Rapporto

Clusit

2019

sulla sicurezza ICT
in Italia

SECURITY
SUMMIT

Indice

ASTREA Via Copernico, 38 - 20125 Milano

Prefazione

Il rapporto CLUSIT che leggerete è il frutto del lavoro di un pool di esperti che ha analizzato e confrontato una serie di fonti e che non può che farci giungere a una sola conclusione: il 2018 è stato un anno di nuovo caratterizzato da criticità importantissime sotto il profilo della sicurezza informatica.

Se da un lato il 2018 è stato l'anno del Regolamento Europeo, che ha determinato investimenti importanti in compliance e in sicurezza, se si è assistiti ad alcuni casi importantissimi in cui il tema "dati personali" ha avuto un riflesso incredibile sui mercati azionari (si pensi al crollo di Facebook e al "non data breach" in merito alla notizia della malattia e poi della morte di Sergio Marchionne dove il titolo FCA è sceso violentemente lasciando intuire quelle che potrebbero essere le conseguenze se notizie di questo livello uscissero sulla stampa senza controllo), sotto altro profilo non vi è dubbio però che il trend da noi individuato dal 2011 a oggi non lascia dubbi. Nel 2018 gli attacchi con impatto significativo sono aumentati a livello globale del 38% con una media di 129 al mese. Poco più di quattro al giorno, e si tratta solo di quelli gravi e conosciuti.

Come ormai da anni, il cybercrime è ovviamente la principale causa di attacchi. Interessante che ormai quattro quinti degli attacchi effettuati sotto questo profilo (il 79%) sono effettuati per ottenere denaro o per sottrarre informazioni allo scopo di monetizzare le informazioni stesse.
Preoccupante, ma non sorprendente visto il trend ormai consolidato da anni, è anche l'aumento dei casi di spionaggio cyber (+57%) a testimonianza di un sempre crescente interesse dei criminali per queste tipologie di attività. Le finalità tipiche di questi attacchi sono lo spionaggio geopolitico, industriale e il furto di proprietà intellettuale.
Casi quindi numericamente meno rilevanti rispetto al cybercrime ma con impatti e conseguenze sempre estremamente critiche.
Ancora in calo risultano invece i casi di hacktivism anche se talvolta non è semplice distinguerli rispetto allo spionaggio cyber.
Abbiamo già accennato al tema degli impatti che, come si evince dai dati raccolti e analizzati, deve essere tenuto in altissima considerazione: basti pensare che nel 2018 c'è stato un importantissimo aumento della gravità media degli attacchi. Nelle categorie dello spionaggio e dell'information warfare i casi classificati come critici nel 2018 sono stati rispettivamente l'80% e il 70% dei casi analizzati.

Spostando l'attenzione sulle vittime risulta di particolare interesse il fatto che il mondo sanitario sia stato al centro di numerosissimi attacchi se, come risulta, il numero di casi censiti, orientati soprattutto a finalità di cybercrime e di furto di dati personali, è aumentato del 99% rispetto al 2017.

Il settore pubblico è poi sempre al centro dell'attenzione dei criminali (+44%) così come i centri di ricerca e formazione (+55%), fornitori di servizi di cloud computing (+36%) e il mondo finanziario (+33%).
Si tratta di numeri preoccupanti a fronte dei quali gli investimenti in sicurezza, le strategie e le scelte politiche non possono più tardare.
La normativa sta aiutando, basti pensare al GDPR e, a breve, al Cybersecurity ACT, che costringeranno da un lato tutte le imprese e le pubbliche amministrazioni a stanziare budget importanti per la compliance e la sicurezza dei dati e delle informazioni e dall'altro daranno la possibilità di mettere sul mercato prodotti e servizi che potranno essere certificati come sicuri grazie alle certificazioni europee e anche sul fronte mediatico non si sta certo a guardare.
Cominciano a esserci anche casi mediaticamente rilevantissimi (si pensi alla sanzione del CNIL a Google e ai casi sopra citati di Facebook e FCA) che lasciano chiaramente intendere che stiamo andando verso una società che fonda larga parte della Pubblica Amministrazione e dei diversi business del settore privato sui dati personali.
Si parla anche molto di blockchain, intelligenza artificiale, industry 4.0, Internet of Things: tutto splendido, ma tutti ambiti in cui la sicurezza non può in alcun modo essere tralasciata o considerata secondaria.
Insomma, il 2019 sarà un altro anno impegnativo. Vedremo se i DPO in Europa saranno di aiuto nell'aumento ulteriore dell'attenzione sul tema sicurezza informatica e se le aziende e le pubbliche amministrazioni stanzieranno budget adeguati.
Ci aspettiamo ancora una crescita negli investimenti, vedremo in che misura.

E allora buona lettura del Rapporto che avete fra le mani.
Il risultato dello sforzo di un team di altissimo livello che da anni lavora per sensibilizzare il mondo pubblico e privato sui temi della sicurezza informatica.

Ringrazio, a nome di tutti gli Associati e di tutti coloro che lo leggeranno, i Colleghi che hanno dedicato tempo e sforzi alla stesura del Rapporto Clusit 2019 e mi auguro che le elezioni europee che si terranno fra pochi mesi portino al governo del nostro continente una classe politica che, sempre più attenta ai temi della sicurezza informatica, proceda nella direzione degli ultimi anni.

2.500 copie cartacee, oltre 60.000 copie in elettronico e più di 250 articoli pubblicati nel 2018, sono l'evidenza della rilevanza del rapporto CLUSIT ed è quindi importante diffonderlo, leggerlo, farlo conoscere, perché solo dalla consapevolezza può derivare la conoscenza del problema, la capacità di adottare scelte idonee e quindi la sicurezza nostra e di tutti.

Buona lettura

Gabriele Faggioli
Presidente CLUSIT

Introduzione al Rapporto

Il Rapporto CLUSIT 2019, giunto ormai al suo ottavo anno di pubblicazione, inizia con una panoramica degli eventi di cyber-crime più significativi degli ultimi 12 mesi. Possiamo affermare che il 2018 è stato l'anno peggiore di sempre in termini di evoluzione delle minacce "cyber" e dei relativi impatti, non solo dal punto di vista quantitativo ma anche e soprattutto da quello qualitativo, evidenziando un trend di crescita degli attacchi, della loro gravità e dei danni conseguenti mai registrato in precedenza. **Nell'ultimo biennio il tasso di crescita del numero di attacchi gravi è aumentato di 10 volte rispetto al precedente. Non solo, la Severity media di questi attacchi è contestualmente peggiorata, agendo da moltiplicatore dei danni.**

Dal punto di vista numerico, nel 2018 abbiamo raccolto e analizzato 1.552 attacchi gravi (+ 37,7% rispetto all'anno precedente), con una media di 129 attacchi gravi al mese (rispetto ad una media di 94 al mese nel 2017, e di 88 su 8 anni).

Ci siamo avvalsi anche quest'anno dei dati relativi agli attacchi rilevati dal **Security Operations Center (SOC) di FASTWEB**, che ha analizzato la situazione italiana sulla base di oltre 40 milioni di eventi di sicurezza. L'analisi degli attacchi è poi completata da due contributi tecnici: il "Rapporto 2018 sullo stato di Internet – Analisi globale degli **attacchi di DDoS, applicativi e furto di identità**" a cura di Akamai e "**Email security: i trend rilevati in Italia nel corso del 2018**" a cura di Libraesva.
Seguono le rilevazioni e segnalazioni della **Polizia Postale e delle Comunicazioni**, del **Nucleo Speciale Tutela Privacy e Frodi Tecnologiche della Guardia di Finanza** e del **CERT Nazionale**.

Presentiamo a questo punto l'abituale capitolo dedicato al settore FINANCE, con 4 contributi: "Elementi sul **Cyber-crime nel settore finanziario in Europa**" a cura di IBM; "Analisi del **Cyber-crime in Italia in ambito finanziario** nel 2018" a cura di Communication Valley Reply; "**"Sviluppo di un sistema di cyber threat intelligence**" a cura del CERT di **Banca d'Italia**; "**Carding** – Scenario ed evoluzione dei canali di vendita nel 2018" a cura di Lutech.

Il 2018 è stato un anno cruciale per la Data Protection e non solo perché il 25 maggio il GDPR è entrato pienamente in vigore: per la prima volta è emersa con chiarezza, nella consapevolezza della pubblica opinione, la relazione fra la protezione dei dati personali e libertà e diritti degli interessati, così spesso richiamati dagli articoli del GDPR. A distanza di 9 mesi dall'entrata in vigore del nuovo Regolamento abbiamo raccolto in uno "Speciale GDPR", alcuni contributi che ci aiuteranno a capire meglio le cose da fare: "2019: **data protection 4.0**" di Sergio Fumagalli e "**La terza fase del GDPR**" di Alessandro Vallega.
Lo Speciale contiene i risultati di una survey realizzata dall'Osservatorio Sicurezza & Pri-

vacy del Politecnico di Milano sullo **stato di adeguamento al GDPR delle aziende italiane**. Si riporta infine un contributo tecnico su "**Cifratura dei dati personali** e adeguamento al nuovo Regolamento Europeo" di Paola Meroni.

Tra le novità del Rapporto Clusit 2019, un capitolo dedicato all'Intelligenza Artificiale, con tre contributi: "**Intelligenza Artificiale: il Buono, il Brutto, il Cattivo**" di Fabio Roli; "**L'Intelligenza Artificiale è sicura?**" di Battista Biggio; "**L'intelligenza artificiale come strumento "dual use" nella cybersecurity**" a cura di DXC Technology.
Un altro capitolo è dedicato alla Blockchain, con: "**Blockchain & Supply Chain: una catena del valore sicura, distribuita e trasparente**" di Guido Sandonà e Federico Griscioli; "Aspetti di sicurezza legali e tecnici sugli **smart contract**" di Alessio Pennasilico e Piero Bologna; "**Il 2018 dei Crypto Exchange**" di Davide Carboni.

Anche in questa edizione del rapporto, troviamo un'**analisi del mercato italiano** della sicurezza IT, realizzata appositamente da **IDC Italia**.

Seguono infine 6 FOCUS ON: "**Programmi di security awareness**: una necessità non più rimandabile" di Garibaldi Conte; "La sicurezza delle imprese è fatta di persone competenti e consapevoli. Un manifesto per la competenza digitale e la consapevolezza in materia di sicurezza online con focus sulla **Generazione Z**" di Ettore Guarnaccia; "Il panorama delle startup italiane nel settore **cybersecurity e legal-tech**. Stato dell'arte e valutazioni sul trend evolutivo" di Giuseppe Vaciago; "La logica del profitto alla base dell'aumento del **cryptojacking"** a cura di Bitdefender; "Infrastrutture critiche vulnerabili. Sempre più alto il rischio di **attacchi agli impianti idrici ed energetici**" a cura di Trend Micro; "**Attacchi e difese nel Cloud Computing** nel 2018" a cura di Microsoft.

Analisi dei cyber attacchi più significativi del 2018 e tendenze per il 2019

Introduzione all'ottava edizione

Come di consueto in questa prima sezione del Rapporto CLUSIT 2019, giunto ormai al suo ottavo anno di pubblicazione[1], classifichiamo i più gravi cyber attacchi di dominio pubblico avvenuti a livello globale (Italia inclusa) negli ultimi 16 semestri e li confrontiamo con l'analisi degli attacchi noti degli ultimi 12 mesi. A partire da questi dati proviamo a fornire un'interpretazione neutra e ragionata sull'evoluzione delle minacce cibernetiche nel mondo e a delineare le tendenze in atto.
L'analisi è basata sull'attenta valutazione di tutte le informazioni pubblicamente disponibili in merito a un campione di attacchi "notevoli" che, a oggi, è costituito da oltre **8.400** incidenti noti avvenuti tra il gennaio 2011 e il dicembre 2018 (dei quali **1.552** nel 2018), ed è volutamente espressa con un taglio divulgativo, in modo da risultare fruibile al maggior numero possibile di lettori.

Considerazioni metodologiche

Dal punto di vista *metodologico* va sottolineato che le nostre analisi e i relativi commenti si riferiscono a un campione necessariamente *parziale*, per quanto ormai statisticamente significativo, rispetto al numero degli attacchi gravi effettivamente avvenuti nel periodo in esame. Questo accade sia perché *un buon numero* di aggressioni non diventano *mai* di dominio pubblico, oppure lo diventano *ad anni di distanza* (solitamente quanto più gli attacchi sono sofisticati), sia perché in molti casi è interesse delle vittime non pubblicizzare gli attacchi subiti, se non costretti dalle circostanze o da obblighi normativi particolari.
Per inciso, in merito a quest'ultima fonte di *disclosure obbligatoria* dobbiamo rilevare che, nonostante l'entrata in vigore del Regolamento GDPR[2] e della Direttiva NIS[3], nel secondo semestre 2018 non abbiamo rilevato un aumento significativo di attacchi gravi di pubblico dominio in Europa, il che alla luce dell'aumento degli attacchi registrati a livello globale nel 2018 (**+37,7%** rispetto al 2017) appare francamente curioso.
Ad ogni modo la natura delle fonti utilizzate per realizzare questo studio introduce inevitabilmente un *bias* [4] nel campione, all'interno del quale sono certamente meglio rappresentati gli

[1] Ovvero alla quattordicesima edizione, considerando anche gli aggiornamenti semestrali
[2] https://it.wikipedia.org/wiki/Regolamento_generale_sulla_protezione_dei_dati
[3] https://clusit.it/wp-content/uploads/2017/02/direttiva_nis.pdf
[4] https://it.wikipedia.org/wiki/Bias_(statistica)

attacchi realizzati per finalità cyber criminali o di hacktivism rispetto a quelli derivanti da attività di cyber espionage e information warfare, che emergono più difficilmente.
In sintesi, considerato che il nostro campione è realizzato esclusivamente a partire da fonti aperte, e che al loro interno alcune classi di incidenti sono sistematicamente sottorappresentate, è plausibile supporre che questa analisi dipinga uno scenario *meno critico rispetto alla situazione sul campo*.

Origini ed evoluzione di questa analisi

Quando nell'ormai remoto 2012 abbiamo iniziato questa ricerca, poi pubblicata nella prima edizione del Rapporto Clusit, definendo (ingenuamente) il 2011 come "l'Annus Horribilis della sicurezza informatica", gli scenari erano radicalmente diversi e gli impatti geopolitici e socioeconomici delle minacce cibernetiche rappresentavano ancora un problema relativamente minore, suscitando interesse e preoccupazione solo tra pochi esperti di ICT Security. Giova qui ricordare che all'epoca i rischi "cyber" non erano nemmeno considerati all'interno del Global Risk Report del World Economic Forum[5], mentre nel 2019 sono assurti al primo posto per impatto e probabilità di accadimento, insieme ai disastri naturali e agli effetti globali del *climate change*.

Lo scopo originario per il quale è nato questo lavoro era dunque di elevare la consapevolezza e migliorare la comprensione del pubblico italiano rispetto all'evoluzione delle minacce cibernetiche, nell'ipotesi (poi dimostratasi drammaticamente esatta) che il problema sarebbe inevitabilmente degenerato con grande rapidità nei mesi e anni successivi, e che la pressoché totale mancanza di sensibilità in materia fosse *una delle principali ragioni* del peggioramento degli scenari.
Questa finalità rimane ancora oggi assolutamente centrale, ma data la criticità della situazione che si è venuta a creare nel frattempo, e considerati i rischi sistemici, esistenziali che oggi incombono sulla nostra *civiltà digitale* a causa della crescita straordinaria delle minacce cibernetiche, siamo convinti che innalzare l'awareness del pubblico non sia più sufficiente, e che questa analisi debba continuare a evolversi, trasformandosi da una semplice cronaca ragionata degli attacchi in un vero e proprio strumento di lavoro e di supporto decisionale.
Per questa ragione, oltre ad analizzare come di consueto gli attacchi in base alla tipologia degli attaccanti, delle vittime e delle tecniche di attacco utilizzate (con approfondimenti verticali per le categorie maggiormente colpite), anche quest'anno come già nel 2017 presentiamo un *indice della gravità degli attacchi analizzati*, classificandoli in base a tre livelli crescenti di "*Severity*", il che ci consente di realizzare inediti confronti e di offrire interessanti spunti di riflessione a coloro che si occupano di *threat modeling*, di *cyber risk management* e di *cyber strategy*, sia a livello aziendale che istituzionale, grazie a una migliore "fotografia" dei rischi attuali resa possibile da questo ulteriore elemento di valutazione.

[5] https://www.weforum.org/reports/the-global-risks-report-2019

Con l'auspicio che anche quest'anno il Rapporto CLUSIT possa apportare un contributo significativo al dibattito nazionale in merito all'accelerazione crescente delle problematiche globali di sicurezza cibernetica, e alle sue ricadute sul benessere del Paese, auguriamo a tutti una buona lettura.

2018, "due minuti a mezzanotte"

Anticipando alcune delle conclusioni che seguono possiamo affermare che il 2018 è stato l'anno *peggiore di sempre* in termini di evoluzione delle minacce "cyber" e dei relativi impatti, non solo dal punto di vista quantitativo ma anche e soprattutto da quello qualitativo, evidenziando un trend di crescita degli attacchi, della loro gravità e dei danni conseguenti *mai registrato in precedenza* dall'inizio della nostra analisi.
Per sintetizzare la gravità della situazione l'anno scorso abbiamo scritto (non senza attirare qualche sberleffo) che il 2017 aveva rappresentato un "salto quantico" nei livelli di cyber-insicurezza globali.
Quest'anno, essendo rimasti a corto di paragoni adeguati, abbiamo deciso di esprimere il nostro giudizio sulla criticità del momento storico facendo riferimento al famigerato "*Doomsday Clock*"[6], l'orologio metaforico ideato nel 1947 dagli scienziati della rivista *Bulletin of the Atomic Scientists* dell'Università di Chicago, in cui la mezzanotte simboleggia la fine del mondo, e i minuti di distanza da essa la probabilità dell'apocalisse nucleare[7].
Perché affermare che ci troviamo ormai a "due minuti dalla mezzanotte"? In sintesi, perché crediamo che le tendenze che stiamo osservando non possano continuare ancora a lungo senza determinare un qualche genere di discontinuità, di rottura (anche se non abbiamo modo di sapere come questa si concretizzerà) e che lo *stress* ancora sopportabile dal sistema sia limitato.
Osservando la situazione dal punto di vista quantitativo, a parità dei criteri di selezione e classificazione che applichiamo al nostro campione (aggiornati nel 2014 e mantenuti invariati da allora) nel quinquennio 2014 - 2018 la crescita degli attacchi gravi è stata del **+77,8%** (da 873 a 1.552).
Mentre nell'arco del biennio 2017-2018 (con un'accelerazione sensibile nell'ultimo anno) il numero di attacchi gravi è cresciuto del **+37,7%**, la crescita registrata nel biennio 2015-2016 era stata "solo" del +3,8%, ovvero nell'ultimo biennio il tasso di crescita del numero di attacchi gravi *è aumentato di 10 volte rispetto al precedente*. Non solo, la Severity media di questi attacchi (che valutiamo dal 2017) è contestualmente peggiorata, agendo da moltiplicatore dei danni.
Questi dati avvalorano la nostra convinzione che sia avvenuto un vero e proprio *cambiamento di fase* nei livelli globali di cyber-insicurezza, causata dall'evoluzione rapidissima degli attori, delle modalità e delle finalità degli attacchi. Dobbiamo sforzarci di tenere presente che il Cybercrime, l'Espionage e l'Information Warfare del 2018 non sono più quelli del 2014, o anche solo del 2016, anche se continuiamo a utilizzare le stesse espressioni per farvi riferimento.
Come previsto, nel 2018 si sono realizzate appieno le tendenze più pericolose individuate nel 2017, che avevamo descritto come "l'anno del trionfo del malware, degli attacchi indu-

[6] https://it.wikipedia.org/wiki/Orologio_dell%27apocalisse

[7] https://www.focus.it/cultura/storia/apocalisse-doomsday-clock-2019-a-due-minuti-dalla-fine

strializzati realizzati su scala planetaria contro bersagli multipli e della definitiva discesa in campo degli Stati come attori di minaccia", e queste tendenze, consolidandosi, sono diventate il "new normal", mentre scenari che solo 5 anni fa avremmo bollato come fantascienza di serie B sono ormai entrati a far parte della nostra realtà quotidiana.
Per fare un esempio eclatante della *mutazione genetica delle minacce cyber* avvenuta negli ultimi 2 anni, il Cybercrime, pur rappresentando senz'altro un problema enorme dal punto di vista quantitativo e facendo la parte del leone nel nostro campione (per le ragioni esposte nel capitolo precedente), ormai dal punto di vista qualitativo (ovvero della Severity, secondo la nostra analisi) è paradossalmente diventato *un rischio secondario,* nel senso che ormai ci troviamo a fronteggiare *quotidianamente* minacce *ben peggiori,* nei confronti delle quali le contromisure disponibili sono particolarmente inefficaci.

Di seguito proviamo a stilare un elenco, sia pure di alto livello, delle 4 principali "nuove" minacce, ricordando che si tratta di un primo tentativo di sistematizzare dinamiche recentissime.

1. Information Warfare e Cyber Guerrilla

L'aspetto più problematico del "new normal" è la possibilità per gli Stati di far "scivolare" senza troppo clamore la gestione dei propri conflitti sempre più verso il piano "cyber", innalzando continuamente il livello dello scontro senza dover fare ricorso a eserciti e armamenti tradizionali [8].
In un mondo multipolare del quale Internet e l'ICT sono ormai parte integrante (ed insostituibile), questo significa entrare in una fase storica di *cyber-guerriglia permanente*, sempre più feroce, ovviamente non dichiarata e anzi sistematicamente negata (sia dagli attaccanti che, in alcuni casi, addirittura dalle vittime).
Per la natura dei mezzi utilizzati, questa dinamica non provoca particolare allarme o rifiuto da parte delle opinioni pubbliche e dà ai partecipanti la sensazione di poter esercitare forme di pressione sempre maggiori senza doverne rendere conto, dato che il rischio di subire le conseguenze di una loro attribuzione rimane remoto - ritenendo anche in caso di attribuzione di poter comunque evitare ritorsioni troppo costose, il che naturalmente è un *incentivo ad alzare continuamente la posta*.
Basti pensare a ExPetr / NotPetya, il singolo attacco più grave di sempre (costato oltre 10 miliardi di dollari)[9], che ha avuto conseguenze planetarie (pur essendo mirato inizialmente all'Ucraina) ed è stato ufficialmente attribuito alla Russia[10] da Stati Uniti, Regno Unito, Canada, Australia e Nuova Zelanda (c.d. "Five Eyes")[11]. In altri tempi e contesti, una simile provocazione avrebbe causato una risposta militare, oggi invece dopo un fatto del genere

[8] https://www.bbc.com/news/technology-43738953 - UK launched cyber-attack on Islamic State

[9] https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[10] https://www.securityweek.com/us-canada-australia-attribute-notpetya-attack-russia

[11] https://en.wikipedia.org/wiki/Five_Eyes

molti Paesi (inclusi molti considerati minori) invece che protestare lavorano silenziosamente al prossimo NotPetya, trasformando così il mondo intero in un campo di battaglia, con la linea del fronte che passa (non incidentalmente, ma *by design*) dalle case dei cittadini, dagli uffici, dalle fabbriche e dalle infrastrutture critiche di tutto il pianeta.
Va detto senza troppi giri di parole che questi crescenti livelli di cyber-attrito rappresentano ormai un "clear and present danger" per la nostra civiltà digitale e possono *in qualsiasi momento*, per un errore di valutazione o a causa di un'escalation tra due o più parti, determinarne il collasso.

2. Cyber espionage e sabotage

Un secondo elemento di grave preoccupazione è legato alle attività di cyber spionaggio e sabotaggio, che sono in netta crescita e assumono ormai le forme più svariate, dalla ormai costante "guerra della percezione" [12] realizzata tramite fake news amplificate via Social Media[13] all'infiltrazione di infrastrutture critiche[14], aziende e istituzioni[15], al furto sistematico di ogni genere di informazioni per finalità geopolitiche, di predominio economico e tecnologico, di ricognizione e di "preparazione del terreno" in vista di ulteriori attacchi.

Questo genere di minaccia è sempre più diffuso per due ragioni fondamentali: da un lato le vittime non sono assolutamente strutturate per difendersi da questa tipologia di attaccanti, e dall'altro forze dell'ordine e servizi di sicurezza non hanno le risorse sufficienti per presidiare efficacemente questo fronte, anche considerato che la superficie di attacco potenziale è sostanzialmente infinita.

Un ulteriore motivo di preoccupazione legato alle attività di cyber spionaggio e sabotaggio scaturisce dal fatto che per gli attaccanti le "barriere all'ingresso" sono molto basse e il rapporto costi-benefici è molto favorevole, il che tra l'altro ha stimolato la proliferazione di gruppi mercenari state-sponsored che realizzano campagne su commissione come subcontractor di strutture governative, e di un ecosistema globale di fornitori di tecnologie e soluzioni "chiavi in mano" che sviluppano strumenti sempre più potenti e sofisticati, di una qualità ben diversa rispetto a quelli utilizzati dal Cybercrime, a supporto di queste operazioni.
L'affermarsi di questo modello, che potremmo definire di "espionage-as-a-service"[16], aumenta ulteriormente i livelli di rischio complessivi derivanti da questo genere di attività, di per sé già particolarmente dannose, dal momento che questi mercenari sono difficilmente controllabili e spesso si comportano come cybercriminali, in alcuni casi addirittura com-

[12] https://www.rand.org/pubs/research_reports/RR1925z2.html

[13] https://www.nytimes.com/2018/02/16/us/politics/russians-indicted-mueller-election-interference.html

[14] https://techcrunch.com/2018/10/04/uk-says-russias-gru-was-behind-a-spate-of-chaotic-cyber-attacks-between-2015-and-2017

[15] https://uk.reuters.com/article/uk-germany-cyber-russia/russian-hacker-group-breached-german-ministries-took-data-media-idUKKCN1GC2HN

[16] https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf

piendo cyber-rapine[17] per finanziarsi o per aumentare i propri profitti, il che rappresenta un ulteriore moltiplicatore di danno.

3. Machine Learning (AI)

Un'altra causa di grave preoccupazione è rappresentata dalla inevitabile "weaponisation"[18] delle tecniche di Machine Learning, e dalla parallela crescita di tecniche di attacco sviluppate specificamente per colpire queste piattaforme.

Si tratta in effetti di due problemi distinti, entrambi legati alla diffusione di sistemi basati su ML. Da un lato infatti stiamo assistendo alle prime fasi dell'utilizzo di tecniche di Machine Learning per la realizzazione di cyber attacchi[19] con l'obiettivo di renderli sempre più efficaci e meno costosi[20], e dall'altro esiste ormai la concreta possibilità che sistemi basati su AI possano essere silenziosamente alterati e indotti in errore tramite tecniche di "adversarial machine learning"[21] oltre che, più banalmente, attaccati e compromessi con tecniche tradizionali.

Rispetto a questi problemi, e in particolare al secondo, va detto che anche la pur lodevole iniziativa della Commissione Europea per lo sviluppo di una "Trustworthy AI"[22] non pone la cyber security tra i requisiti essenziali di questi sistemi. Nel draft del documento "Ethics Guidelines For Trustworthy AI" si parla solo di "respect for privacy" e, all'interno del requisito di "robustness", di "resilience to attack", criteri che di per sé non coprono tutti gli aspetti di sicurezza necessari, e che così formulati si prestano a interpretazioni troppo vaghe (considerato anche che i produttori implementeranno questi requisiti nella forma tecnicamente più conveniente ed economicamente meno onerosa). È certamente auspicabile che nei prossimi mesi questi requisiti siano rivisti in un'ottica più esplicitamente orientata alla cyber security, senza la quale nessuna AI potrà mai essere davvero "trustworthy". Va anche ricordato che in questo settore la parte del leone (in termini di investimenti, di numero di ricercatori e di brevetti) la fanno Stati Uniti e Cina, che a oggi non sembrano preoccuparsi particolarmente di questi aspetti del problema.

Date queste premesse la nostra realistica previsione è che dal punto di vista della cyber-insicurezza globale e degli impatti conseguenti il Machine Learning rappresenti il "nuovo IoT", ovvero un ulteriore fronte sostanzialmente non presidiato, un Far West tecnologico nel quale la complessità della supply chain e la mancanza di chiare responsabilità da parte di produttori, gestori e utenti finali rendono impossibile non solo l'applicazione di contromisure efficaci, ma anche il monitoraggio e la gestione dei rischi associati.

---

17 https://www.theverge.com/2018/11/8/18075124/north-korea-lazarus-atm-fastcash-hack-millions-dollars-stolen

18 https://dizionari.repubblica.it/Inglese-Italiano/W/weaponization.html

19 https://www.forbes.com/sites/forbestechcouncil/2018/03/22/how-ai-can-be-applied-to-cyberattacks

20 https://www.forbes.com/sites/forbestechcouncil/2018/01/11/seven-ways-cybercriminals-can-use-machine-learning

21 https://en.wikipedia.org/wiki/Adversarial_machine_learning

22 https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_draft_ethics_guidelines_18_december.pdf

Considerata la diffusione prevista per queste piattaforme e la delicatezza dei compiti che dovranno assolvere, accettare anche in questo contesto di "navigare a vista" pur di non interferire con l'innovazione tecnologica sembra essere obiettivamente una *pessima idea*.

4. Surveillance Capitalism

Un quarto aspetto molto problematico e troppo poco discusso del "new normal" è legato all'affermazione di un modello economico globale radicalmente nuovo, sorto dalle ceneri dell'utopia tecno-libertaria degli anni '90 e dei primi anni 2000, recentemente definito da Zuboff e altri come "Surveillance Capitalism"[23].

Richiamarne il concetto all'interno di questo elenco potrebbe far storcere il naso ad alcuni, dal momento che, almeno in principio, non si tratta di una minaccia cibernetica puntuale, quanto piuttosto di un fenomeno socioeconomico che sta alterando modelli di business e relazioni umane, modificando equilibri di potere e perfino alterando il funzionamento delle democrazie liberali[24] *grazie* a una determinata applicazione della tecnologia digitale (che non è certamente l'unica possibile), modellata in base agli interessi economici di poche multinazionali high-tech, peraltro in modi (quasi sempre)[25] leciti.

Per quanto nella nostra analisi vengano raccolti e classificati solo attacchi cyber "tradizionali" (realizzati cioè con tecniche di hacking contro / tramite sistemi digitali), di fronte a questa vera e propria rivoluzione in atto sarebbe opportuno iniziare a considerare anche una nuova classe di cyber attacchi, realizzati (per esempio) grazie allo sfruttamento di lacune normative, alla fumosità dei contratti di servizio oppure con la disinformazione del pubblico e forme sofisticate di lobbying per influenzare i legislatori, al fine di ottenere il controllo pressoché totale delle vite, delle scelte e degli orientamenti (anche politici) di ciascuno. In questo senso abbiamo voluto inserire nel campione di incidenti del 2018 anche la vicenda "Cambridge Analytica", considerandola a tutti gli effetti pratici una forma (nuova) di attacco cibernetico di tipo "corporate".

Non potendo approfondire il tema ulteriormente in questa sede, ci limitiamo a sottolineare il problema della mancanza di *trasparenza*, *accountability* e *social responsibility* di questi soggetti privati, il che, dati gli strumenti e le risorse di cui dispongono, li rende oggettivamente pericolosi[26] *anche* dal punto di vista "cyber", sia perché (come loro stessi affermano) sono ormai "too big to regulate", sia in quanto bersagli "too big to defend" (con tutte le implicazioni del caso) che come nuovi strumenti (diretti o indiretti) di censura, di controllo di massa e di esercizio opaco del potere, a maggior ragione in assenza di meccanismi di "check and balance"[27] adeguati.

---

[23] https://www.theguardian.com/books/2019/feb/02/age-of-surveillance-capitalism-shoshana-zuboff-review

[24] https://www.youtube.com/watch?v=wTQmuTZmDOc - How Surveillance Capitalism Undermines Democracy

[25] https://it.wikipedia.org/wiki/Cambridge_Analytica

[26] https://blogs.scientificamerican.com/observations/can-we-avoid-the-potential-dangers-of-ai-robots-and-big-tech-companies/

[27] http://www.treccani.it/enciclopedia/check-and-balance/

Spunti di riflessione

Fatte salve tutte le considerazioni di dettaglio che svolgeremo più avanti, a nostro avviso siamo giunti a un bivio cruciale, al punto di intersezione di un grande numero di crisi concomitanti, il che nel campo della sicurezza cibernetica implica che le scelte che faremo nei prossimi (pochi) anni decideranno le probabilità di sopravvivenza e la sostenibilità della società digitale così come si è venuta a determinare.
Come nel caso di altri fenomeni molto complessi (e dunque caotici), per esempio gli effetti del climate change sull'ecosistema, fare previsioni a lungo termine è particolarmente difficile, e d'altra parte ci sono già forti evidenze del fatto che la situazione sta rapidamente sfuggendo al controllo e diventando irreversibile, il che prefigura esiti altamente indesiderabili.

Al cuore della questione c'è, come già abbiamo scritto in altre edizioni del Rapporto, non tanto un problema tecnologico (volendo risolvibile) quanto piuttosto culturale e soprattutto economico. Implementando le infrastrutture, i protocolli e i processi che danno corpo alla civiltà digitale non abbiamo tenuto conto in modo corretto dei costi correlati alla sua tutela e difesa, costruendo un modello di business che non li prevede se non in modo residuale e, ove possibile, li evita o li minimizza. Di conseguenza queste risorse non sono disponibili, e oggi nel mondo si investe per la cyber security un decimo di quanto si dovrebbe ragionevolmente spendere.

Tali risorse andrebbero recuperate da qualche altro ambito (per esempio a discapito dell'innovazione, o delle rendite di posizione dei grandi player di mercato), il che oltre a suscitare fortissime resistenze tra l'altro implica che, paradossalmente, più la situazione diventerà grave, meno tenderanno a essere reperibili.
Inoltre il fatto che non vengano dedicate risorse adeguate alla cyber security è sia la causa che la conseguenza del fatto che i costi derivanti dalle minacce cyber crescono molto più velocemente degli investimenti in sicurezza, il che sta determinando un circolo vizioso micidiale, da interrompere al più presto, accompagnato da un pericoloso sentimento di "cyber fatigue"[28].

Riuscirci non è affatto facile. Dovremmo riconoscere che "il Re è nudo" e superare una serie di tabù culturali, tra i quali innanzi tutto l'eccezionalismo del settore ICT (che prima o poi si dovrà trattare come qualsiasi altro settore industriale maturo, introducendo regolamenti, test di qualità e sicurezza obbligatori, responsabilità precise, controlli e sanzioni) e l'idea (del tutto balzana) che il progresso dell'ICT sia magicamente un bene a-priori, a prescindere da qualsiasi altra considerazione.

[28] https://www.cio.com/article/3164471/leadership-management/wake-up-to-the-threat-of-cyber-fatigue.html

Dovremmo poi pretendere che Esecutivi, Parlamenti e organismi sovranazionali, dopo decenni di latitanza, riprendano in mano le redini della questione e definiscano la strada da percorrere per lo sviluppo dell'ICT in base all'interesse dei cittadini, dettando le regole, legiferando opportunamente e vigilando sull'applicazione delle norme così come si fa in qualsiasi altro ambito e mercato, senza lasciare decisioni così critiche in mano ai consigli di amministrazione delle multinazionali high-tech.
Per quanto riguarda l'Italia, bisogna ammettere che si è messa da sola nella condizione di essere il proverbiale "vaso di coccio tra vasi di ferro", essendo mancati fino a oggi una visione, una strategia e un commitment commisurati al contesto.

Il singolare (a questo punto potremmo anche dire protervo) disinteresse della politica e delle parti sociali in materia di cyber security, e la conseguente carenza acuta di investimenti in sicurezza cibernetica nel nostro Paese (sia dal punto di vista della ricerca e sviluppo che da quello dell'implementazione di contromisure attive e difensive) fanno sì che in base al Global Cybersecurity Index dell'ITU (pubblicato nel 2017) ci posizioniamo non solo ultimi tra i paesi europei avanzati, ma anche alle spalle di paesi "emergenti" come Lituania, Malaysia e perfino Mauritius[29].

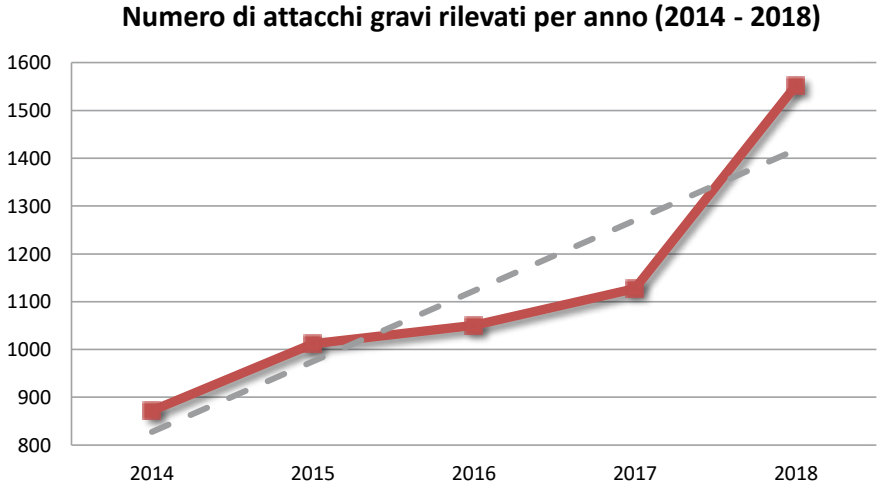
Il fatto di essere un Paese economicamente importante e al tempo stesso una colonia tecnologica, oltretutto dotata di difese particolarmente scarse, ci mette più di altri in balia degli eventi, il che naturalmente indebolisce la nostra sovranità e ci rende interlocutori poco credibili nel mondo, danneggiando la nostra competitività e in ultima analisi il benessere di tutti i cittadini. Cosa aspettiamo a rimediare?

[29] https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

Analisi dei principali cyber attacchi noti a livello globale del 2018

In questa sezione, come di consueto, il Rapporto CLUSIT 2019 propone una dettagliata panoramica degli incidenti di sicurezza più significativi avvenuti a livello globale nell'anno precedente, confrontandoli con i dati raccolti nell'ultimo quinquennio [30].

Lo studio si basa su un campione che al 31 dicembre 2018 è costituito da **8.417** attacchi noti di particolare gravità, ovvero che hanno avuto un impatto significativo per le vittime in termini di perdite economiche, di danni alla reputazione, di diffusione di dati sensibili (personali e non), o che comunque prefigurano scenari particolarmente preoccupanti, avvenuti nel mondo (inclusa quindi l'Italia) dal primo gennaio 2011, di cui **1.552** nel 2018 (**+77,8%** rispetto al 2014, **+ 37,7%** rispetto al 2017) e **5.614** registrati tra il 2014 e il 2018.

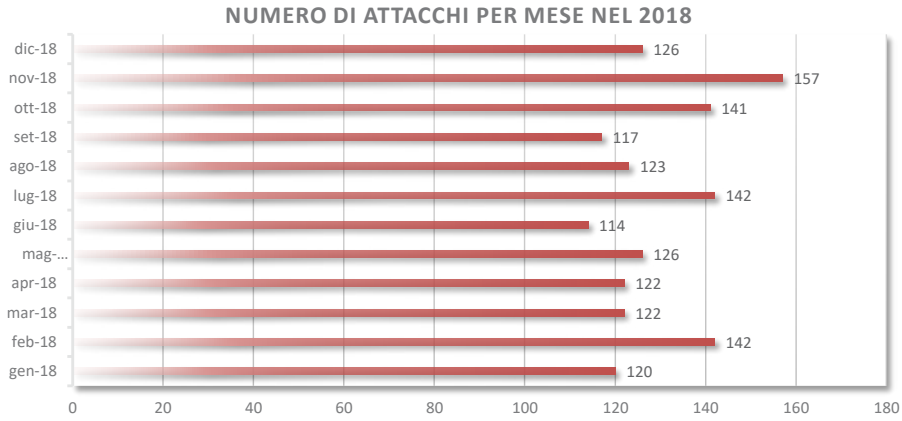


Anche quest'anno, per definire un cyber attacco come "grave" abbiamo impiegato gli stessi criteri di classificazione già applicati ai dati del periodo 2014-2017, più restrittivi rispetto ai criteri che avevamo applicato negli anni 2011-2013, dal momento che nell'arco di questi 96 mesi si è verificata una sensibile evoluzione degli scenari e che alcune categorie di attacchi, che potevano essere ancora considerati "gravi" nel 2011-2013, sono oggi diventati *ordinaria amministrazione* (per esempio, i "defacement" di siti web).

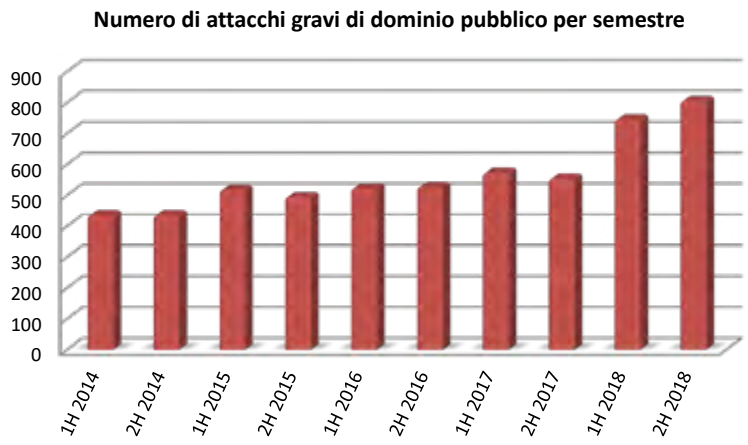
[30] Pur avendo iniziato questa ricerca nel 2011, oggi ha poco senso fare confronti con gli anni precedenti al 2014

A parità di criteri, quest'anno abbiamo classificato come gravi un numero di attacchi superiore rispetto a tutti gli anni analizzati a partire dal 2014, scartando una grande quantità di incidenti "minori" per evitare di confrontare, nell'ambito dello stesso campione, situazioni che hanno causato la perdita di milioni di euro o il furto di milioni di account con, per fare un esempio tra molti, un attacco DDoS di lieve entità verso una banca o un sito web istituzionale. Ciò non significa che questo genere di attacchi a impatto minore non sia a sua volta in rapida crescita.

Dal punto di vista numerico, degli **8.417** attacchi gravi di pubblico dominio che costituiscono il nostro database di incidenti degli ultimi 16 semestri (8 anni), nel 2018 ne abbiamo raccolti e analizzati 1.552, contro i 1.127 del 2017 (+ 37,7%), con una media di **129 attacchi gravi al mese** (rispetto a una media di 94 al mese nel 2017, e di 88 su 8 anni). Il picco massimo di sempre si è avuto nel novembre 2018 (157 attacchi).



Questa la distribuzione degli attacchi registrati nel periodo 2014-2018, suddivisi per semestre:



© Clusit - Rapporto 2019 sulla Sicurezza ICT in Italia

Le tre tabelle seguenti rappresentano una sintesi dei dati che abbiamo raccolto. Come in passato abbiamo evidenziato nella colonna più a destra i trend osservati.

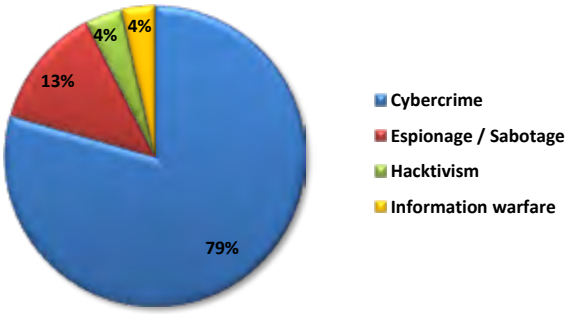
Da qui in avanti, per comodità di consultazione e omogeneità dei criteri di classificazione degli attacchi, presentiamo il confronto solo dei dati dell'ultimo quinquennio, rimandando alle edizioni precedenti del Rapporto Clusit per i dati relativi al triennio 2011-2013.

Distribuzione degli attaccanti per tipologia

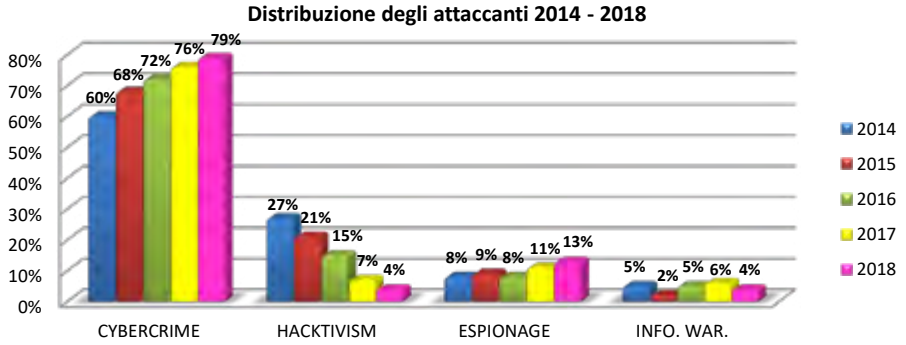
ATTACCANTI PER TIPOLOGIA	2014	2015	2016	2017	2018	2018 su 2017	Trend
Cybercrime	526	684	751	857	1232	43,8%	↑
Hacktivism	236	209	161	79	61	-22,8%	↓
Espionage / Sabotage	69	96	88	129	203	57,4%	↑
Cyber warfare	42	23	50	62	56	-9,7%	↘
Espionage / Sabotage + Cyber Warfare	111	119	138	191	259	35,6%	↑

Complessivamente, rispetto al 2017, il numero di attacchi gravi che abbiamo raccolto da fonti pubbliche per il 2018 cresce del **37,7%**. In termini assoluti, nel 2018 le categorie "Cybercrime" e "Cyber Espionage" fanno registrare il numero di attacchi più elevato degli ultimi 8 anni.
Dal campione emerge chiaramente che, con l'esclusione delle attività riferibili ad attacchi della categoria "**Hacktivism**" che diminuisce ancora sensibilmente (**-22,8%**) rispetto al 2017, nel 2018 sono in aumento gli attacchi gravi compiuti per finalità di "**Cybercrime**" (**+43,8%**), così come quelli riferibili ad attività di "**Cyber Espionage**" (**+57,4%**).
Va sottolineato che, rispetto al passato, oggi risulta più difficile distinguere nettamente tra "Cyber Espionage" e "Information Warfare": sommando gli attacchi di entrambe le categorie, nel 2018 si assiste a un aumento del **35,6%** rispetto all'anno precedente (259 contro 191).

Tipologia e distribuzione degli attaccanti 2018



Già nel 2014 il Cybercrime si era confermato la prima causa di attacchi gravi a livello globale (60%), salendo al 68% dei casi analizzati nel 2015. Nel 2016 tale percentuale era il 72%, salita al 76% nel 2017 e infine al **79%** nel 2018, mostrando un trend inequivocabile. Va sottolineato che già dal 2016 si è assistito alla diffusione ormai endemica di attività cyber criminali "spicciole", che in questo campione di incidenti gravi non sono rappresentate (per esempio le quotidiane campagne di estorsione realizzate tramite phishing e ransomware, che hanno colpito moltissime organizzazioni e cittadini italiani), trend che si è ulteriormente rafforzato nel biennio 2017-2018.



© Clusit - Rapporto 2019 sulla Sicurezza ICT in Italia

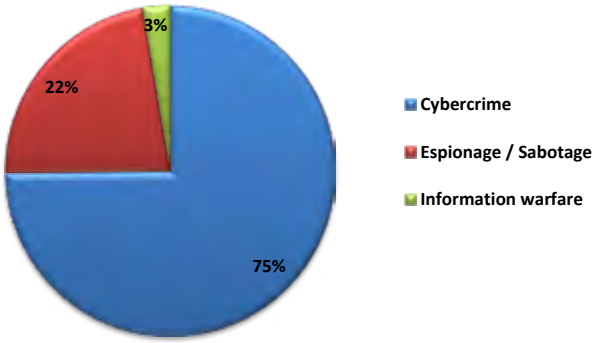
L'Hacktivism diminuisce ulteriormente, passando da quasi un terzo dei casi analizzati nel 2014 al **4%** del 2018.

Per quanto riguarda le attività di Espionage (nonostante la scarsità di informazioni pubbliche in merito) rispetto al 2017 la loro percentuale rispetto al totale degli attacchi rilevati nel 2018 passa dal 11% al **13%**, mentre l'Information Warfare passa dal 6% al **4%**. Come nel 2017, anche nel 2018 queste due categorie sommate valgono il **17%** degli attacchi totali (ricordando però che tale percentuale è calcolata su un numero di attacchi molto maggiore).

Distribuzione degli attaccanti per le categorie più colpite da attacchi

Nel 2018 le categorie più colpite sono state **Multiple Targets** (304 attacchi, +36,9% rispetto al 2017), **Government** (252 attacchi, +40,8%) e **Health** (159 attacchi, +98,8%). Dal punto di vista della distribuzione degli attaccanti che le hanno prese di mira, dalla nostra analisi emergono differenze molto significative tra le diverse categorie.

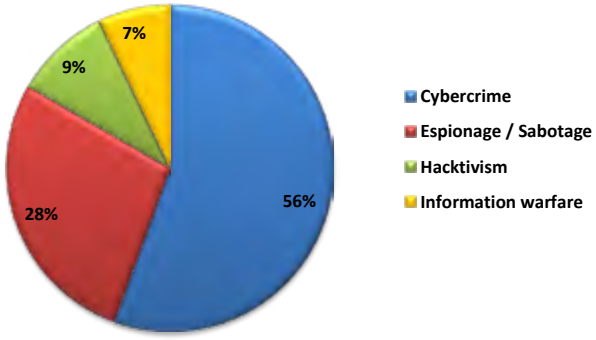
Tipologia e distribuzione degli attaccanti vs Multiple Targets - 2018



© Clusit - Rapporto 2019 sulla Sicurezza ICT in Italia

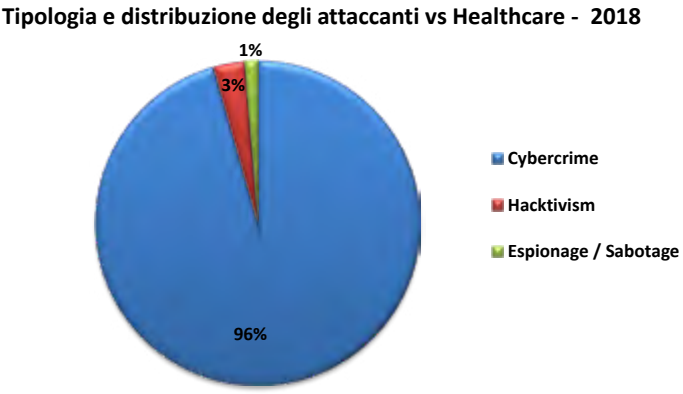
Particolarmente interessante la variazione degli attacchi realizzati contro bersagli multipli con finalità di espionage, che passano dal 16% del 2017 al **22%** del 2018.

Tipologia e distribuzione degli attaccanti vs Gov / Mil / LE - 2018



© Clusit - Rapporto 2019 sulla Sicurezza ICT in Italia

Completamente diversa invece la distribuzione degli attaccanti verso il settore Gov.



© Clusit - Rapporto 2019 sulla Sicurezza ICT in Italia

Ancora diversa la distribuzione degli attaccanti che hanno colpito il settore Healthcare, prevalentemente con finalità cybercriminali (ransomware) e di furto di dati personali.

Distribuzione generale delle vittime per tipologia

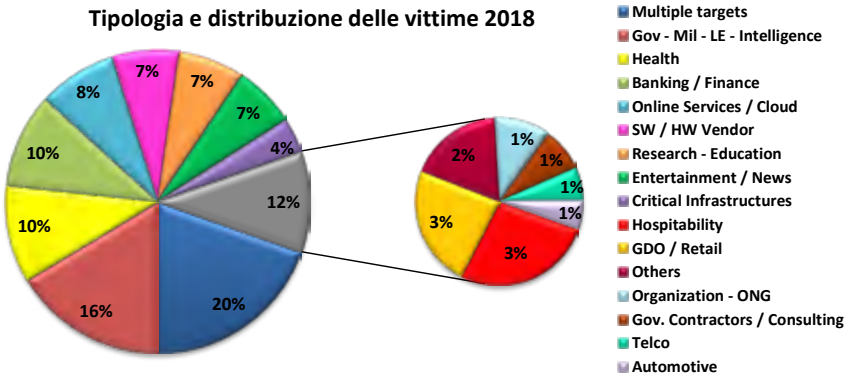
VITTIME PER TIPOLOGIA	2014	2015	2016	2017	2018	2018 su 2017	Trend
Gov - Mil - LEAs – Intel	213	223	220	179	252	40,8%	↗
Multiple targets	-	-	49	222	304	36,9%	↗
Health	32	36	73	80	159	98,8%	↑
Banking / Finance	50	64	105	117	156	33,3%	↗
Online Services / Cloud	103	187	179	95	129	35,8%	↗
Research – Education	54	82	55	71	110	54,9%	↑
Software / Hardware Vendor	44	55	56	68	109	60,3%	↑
Entertainment / News	77	138	131	115	102	-11,3%	↘
Critical Infrastructures	13	33	38	40	57	42,5%	↗
Hospitability	-	39	33	34	45	32,4%	↗
GDO / Retail	20	17	29	24	39	62,5%	↑
Others	172	51	38	40	30	-25,0%	↘
Org / ONG	47	46	13	8	18	125,0%	↑
Gov. Contractors / Consulting	13	8	7	6	14	133,3%	↑
Telco	18	18	14	13	11	-15,4%	↘
Automotive	3	5	4	4	9	125,0%	↑
Security Industry	2	3	0	11	4	-63,6%	↓
Religion	7	5	6	0	3	-	↗
Chemical / Medical	5	2	0	0	1	-	↗
TOTALE / MEDIA VARIAZIONI	873	1012	1050	1127	1552		

Rispetto al 2017, in termini assoluti nel 2018 il numero maggiore di attacchi gravi si osserva verso le categorie “Multiple Targets” (+36,9%), “Gov” (+40,8%) ed “Healthcare” (+98,8%), seguite da “Banking / Finance” (+33,3%), “Online Services / Cloud” (+35,8%) e da “Research / Education” (+54,9%).
Il sensibile calo degli attacchi (-25%) verso la categoria “Others” è principalmente dovuto al fatto che nel 2016 abbiamo introdotto la nuova categoria “Multiple Targets” per rendere

conto del crescente numero di attacchi gravi compiuti in parallelo dallo stesso gruppo di attaccanti contro numerose organizzazioni appartenenti a categorie differenti. Di conseguenza una parte degli attacchi verso organizzazioni appartenenti a tale categoria sono confluiti nella categoria "Multiple Targets".

All'interno della categoria "Multiple Targets", che numericamente costituisce ormai un quinto degli attacchi registrati (causando la maggior parte dei decrementi rilevati per alcune altre categorie, vedi sopra), sono compresi attacchi verso vittime appartenenti a tutte le altre categorie, a dimostrazione del fatto che non solo ormai tutti sono diventati bersagli, ma anche che gli attaccanti sono diventati sempre più aggressivi e conducono operazioni su scala sempre maggiore, con una logica "industriale", che prescinde sia da vincoli territoriali che dalla tipologia dei bersagli, puntando solo a massimizzare il risultato economico (si pensi ai furti di cryptovalute ai danni di grandi Exchange, ad esempio l'attacco cybercriminale a Coincheck[31], o a campagne di spear phishing / espionage su larga scala[32]).

Degna di nota anche la crescita degli attacchi verso le categorie "Critical Infrastructures" (+42,5%), "Software/Hardware vendor" (+60.3%) e "GDO/Retail" (+62,5%).



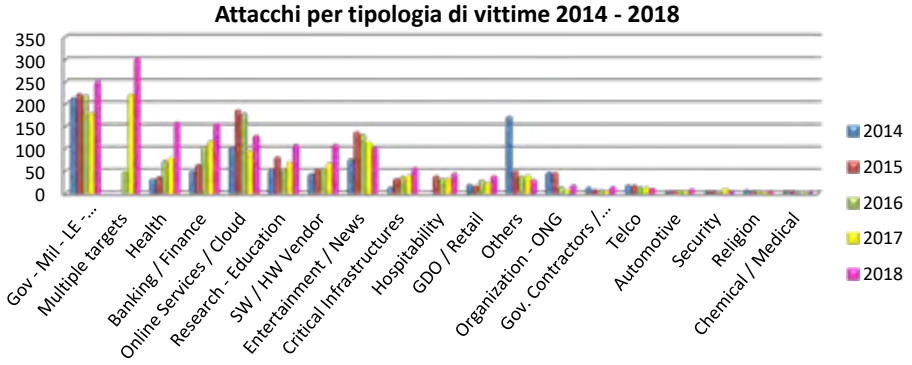
© Clusit - Rapporto 2019 sulla Sicurezza ICT in Italia

Per i motivi sopra illustrati, anche nel 2018 al primo posto assoluto si conferma la categoria "Multiple Targets" (**20%**), superando per il secondo anno di fila il settore "Gov", in diminuzione al **16%**, che dal 2011 al 2016 è sempre stato al primo posto nel nostro studio.
Rispetto al 2017, "Healthcare" sale al terzo posto (**10%**) insieme a "Banking/Finance" (**10%**), seguiti da "Online Services / Cloud" (**8%**) e "SW/HW Vendor" (**7%**).

[31] http://money.cnn.com/2018/01/29/technology/coincheck-cryptocurrency-exchange-hack-japan/index.html

[32] https://www.wired.com/story/iran-cyberattacks-us-universities-indictment/

Al **7%** anche "Research/Education" ed "Entertainment/News", mentre la categoria "Critical Infrastructures" si posiziona al **4%**.



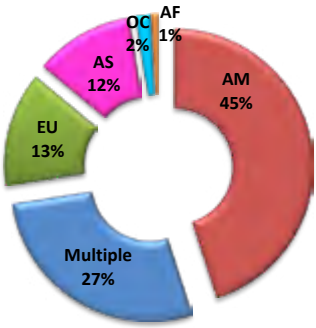
© Clusit - Rapporto 2019 sulla Sicurezza ICT in Italia

Tramite questo grafico si può apprezzare facilmente l'incremento degli attacchi gravi verso bersagli multipli (quindi con impatti potenzialmente sistemici), Gov e Healthcare occorso nel 2018.

Distribuzione generale delle vittime per area geografica

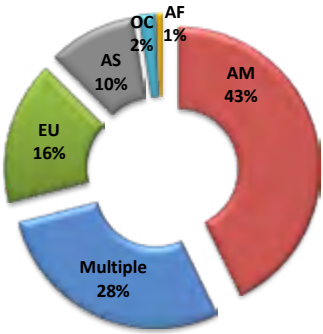
La classificazione delle vittime per nazione di appartenenza viene qui rappresentata su base continentale.
Premesso che rispetto al 2017 le variazioni percentuali sono minime, nel 2018 aumentano le vittime di area americana (dal 43% al **45%**), mentre, in attesa che GDPR e NIS facciano emergere molti attacchi a oggi non noti, gli attacchi noti verso realtà basate in Europa sembrano addirittura diminuire (dal 16% al **13%**) e aumentano quelli rilevati contro organizzazioni asiatiche (dal 10% al **12%**).
Percentualmente rimangono sostanzialmente invariati gli attacchi gravi verso bersagli multipli distribuiti globalmente (categoria "Multiple"), dall'28% del 2017al **27%** del 2018.

Appartenenza geografica delle vittime per continente 2018



© Clusit - Rapporto 2019 sulla Sicurezza ICT in Italia

Appartenenza geografica delle vittime per continente 2017

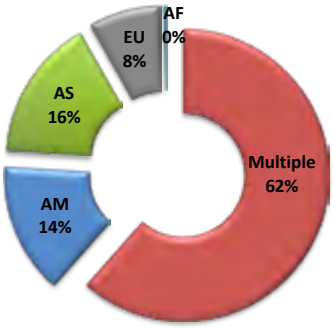


© Clusit - Rapporto 2019 sulla Sicurezza ICT in Italia

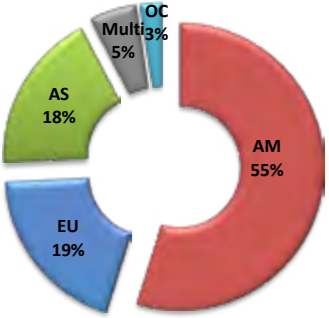
Distribuzione geografica di dettaglio delle vittime appartenenti alle categorie con il maggior numero di attacchi

Anche dal punto di vista della distribuzione geografica delle vittime emergono differenze significative tra le diverse categorie.

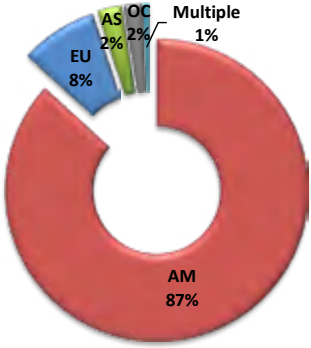
Appartenenza geografica vittime: categoria Multiple Targets - 2018



Appartenenza geografica vittime: categoria Gov / Mil / LE - 2018



Appartenenza geografica vittime: categoria Healthcare - 2018



© Clusit - Rapporto 2019 sulla Sicurezza ICT in Italia

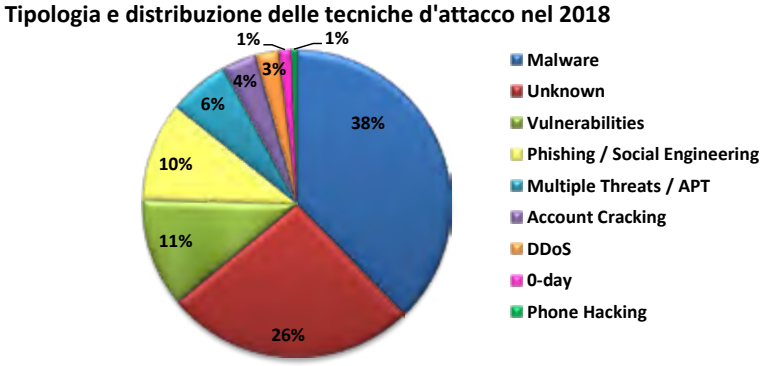
A causa della maturità delle normative USA in materia di data breach, le vittime sembrano concentrarsi negli Stati Uniti. Sorprende molto l'8% di vittime basate in EU, chiaro sintomo che l'implementazione della GDPR procede con lentezza.

Distribuzione delle tecniche di attacco

TECNICHE DI ATTACCO PER TIPOLOGIA	2014	2015	2016	2017	2018	2018 su 2017	Trend
Malware	127	106	229	446	585	31,2%	↗
Unknown	199	232	338	277	408	47,3%	↑
Known Vulnerabilities / Misconfig.	195	184	136	127	177	39,4%	↗
Phishing / Social Engineering	4	6	76	102	160	56,9%	↑
Multiple Techniques / APT	60	104	59	63	98	55,6%	↑
Account Cracking	86	91	46	52	56	7,7%	↗
DDoS	81	101	115	38	38	0,0%	=
0-day	8	3	13	12	20	66,7%	↑
Phone Hacking	3	1	3	3	9	200,0%	↑
SQL Injection	110	184	35	7	1	-85,7%	↓

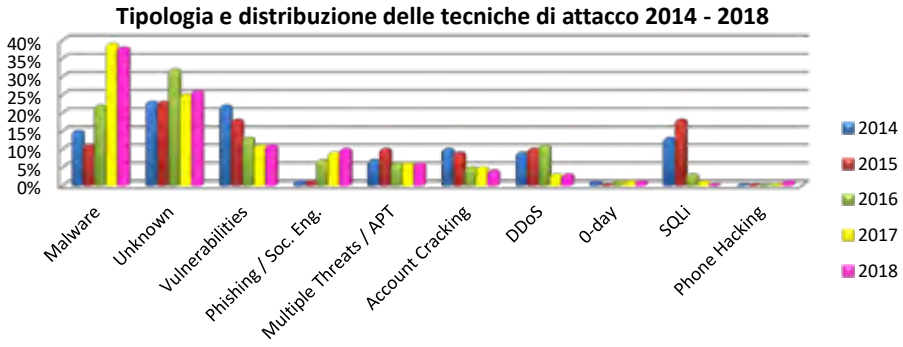
Per la seconda volta dal 2011, nel 2018 le tecniche sconosciute (categoria "Unknown") passano al secondo posto, pur con una crescita del 47,3% rispetto al 2017, superate dalla categoria "Malware" (+31,2%).
A questo dato va sommata la crescita significativa della categoria "Multiple Techniques / APT" (+55,6%), che include attacchi tipicamente con finalità di Espionage, più articolati e sofisticati, per quanto quasi sempre basati anche sull'utilizzo di malware.
I DDoS rimangono sostanzialmente invariati, mentre le SQL injection finalmente crollano all'ultimo posto facendo segnare un -85,7% rispetto al 2017. Lo sfruttamento di vulnerabilità note invece è ancora in crescita (+39,4%), così come l'utilizzo di vulnerabilità "0-day", (+66,7%), per quanto questo dato sia ricavato da un numero di incidenti noti limitato e risulti probabilmente sottostimato. Ritornano a crescere gli attacchi basati su tecniche di "Account Cracking" (+7,7%).

In sostanza gli attaccanti possono fare affidamento sull'efficacia del malware "semplice", prodotto industrialmente a costi decrescenti, e sulle tecniche di Phishing / Social Engineering (+56,9%), per conseguire la gran maggioranza dei loro obiettivi. In generale la distribuzione percentuale ricorda molto quella del 2017, con minime variazioni.



© Clusit - Rapporto 2019 sulla Sicurezza ICT in Italia

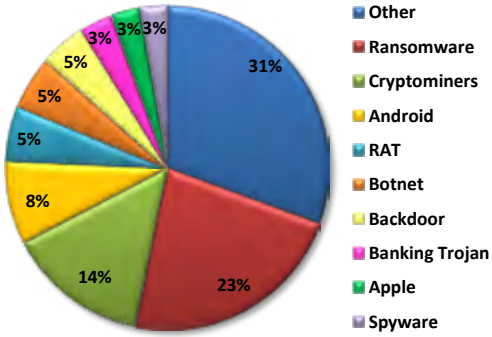
Considerato che stiamo analizzando gli attacchi più gravi del periodo, compiuti contro primarie organizzazioni pubbliche e private, spesso di livello mondiale, il fatto che la somma delle tecniche di attacco più banali (SQLi, DDoS, Vulnerabilità note, Phishing e Malware "semplice") rappresenti ancora il **62%** del totale (era il 68% nel 2017), implica che gli attaccanti *possono realizzare attacchi gravi di successo contro le loro vittime con relativa semplicità e a costi molto bassi, oltretutto decrescenti* – forse una delle considerazioni più gravi tra tutte quelle svolte fin qui.



© Clusit - Rapporto 2019 sulla Sicurezza ICT in Italia

Dato che la categoria "Malware" si conferma per il secondo anno di fila la più numerosa, anche per il 2018 presentiamo anche un'analisi di dettaglio relativa alle tipologie di malware osservate nel nostro campione:

Tipologia e distribuzione Malware 2018

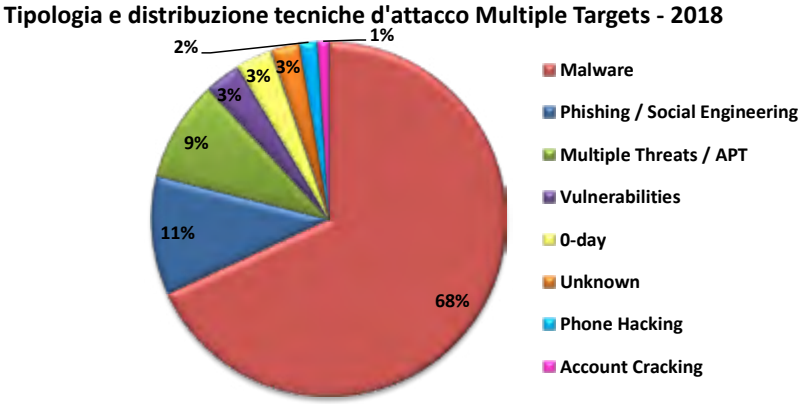


© Clusit - Rapporto 2019 sulla Sicurezza ICT in Italia

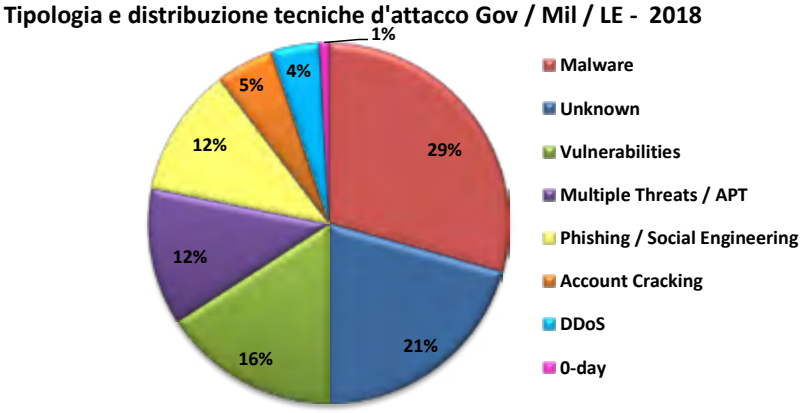
Dal grafico si possono osservare alcuni fenomeni interessanti, tra questi che il malware per le principali piattaforme mobile rappresenta ormai quasi il **12%** del totale, che i Ransomware rappresentano quasi un quarto del malware totale (**23%**), e che i Cryptominers, quasi inesistenti in passato, nel corso del 2018 sono arrivati a rappresentare il **14%** del totale (erano il 7% nel 2017).

Distribuzione delle tecniche utilizzate contro le categorie di vittime oggetto del maggior numero di attacchi

Per analogia con quanto fatto più sopra per la distribuzione degli attaccanti e per quella delle vittime su base geografica, riportiamo di seguito le statistiche relative alla distribuzione delle tecniche di attacco impiegate contro i 3 settori più colpiti da attacchi nel 2018 ("Multiple Targets", "Gov" e "Healthcare").
Anche in questo caso si può osservare chiaramente come la distribuzione delle tecniche di attacco mostri variazioni importanti a seconda della tipologia di bersaglio (il che deriva non solo dal fatto che le vittime sono molto diverse tra loro, ma anche dalla diversa tipologia e dagli obiettivi degli attaccanti).

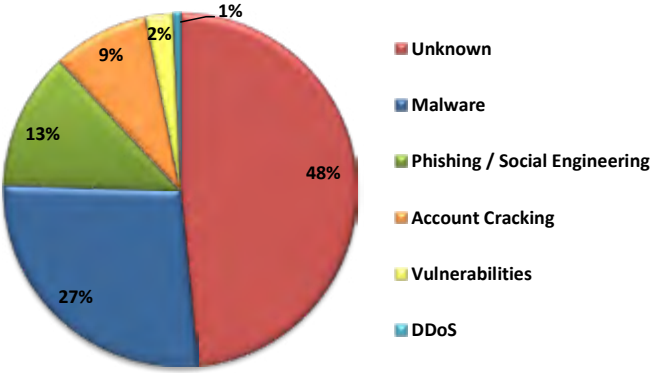


© Clusit - Rapporto 2019 sulla Sicurezza ICT in Italia



© Clusit - Rapporto 2019 sulla Sicurezza ICT in Italia

Tipologia e distribuzione delle tecniche d'attacco Healthcare - 2018

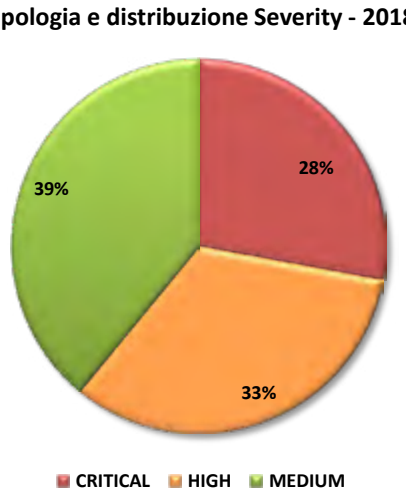


Analisi della "Severity" degli attacchi

Come anticipato nell'introduzione di questa analisi, anche per il 2018 presentiamo una valutazione della Severity degli attacchi analizzati. Tale valutazione ha richiesto da un lato un profondo aggiornamento del nostro approccio nell'analizzare e classificare gli attacchi del nostro campione e dall'altro l'utilizzo di maggiore tempo e risorse.

Abbiamo definito tre categorie o livelli di **impatto** (considerato che stiamo comunque analizzando un campione di attacchi già tutti definiti come "gravi"): Medio, Alto e Critico.
Va premesso che questo genere di analisi si scontra spesso con la scarsità di informazioni dettagliate di dominio pubblico relative ai singoli incidenti, e che pertanto deve considerarsi basata su una stima necessariamente ad alto livello degli impatti.

Le variabili che contribuiscono a comporre la valutazione dell'impatto per ogni singolo attacco analizzato sono molteplici e includono: impatto geopolitico, sociale, economico (diretto e indiretto), di immagine e di costo/opportunità per le vittime.
Per il campione 2018, l'analisi degli impatti stimati ci presenta questo quadro generale:

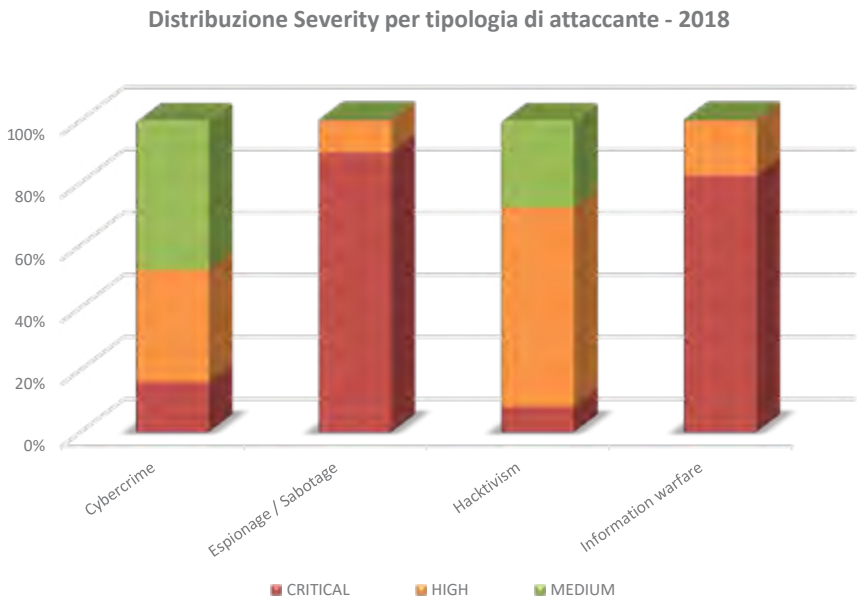


© Clusit - Rapporto 2019 sulla Sicurezza ICT in Italia

Gli attacchi con impatto "Medio" rappresentano il **39%** del totale (erano il 49% nel 2017), quelli di livello "Alto" il **33%** (erano il 31%) e quelli di livello "Critico" quasi un terzo con il **28%** (erano il 21%).

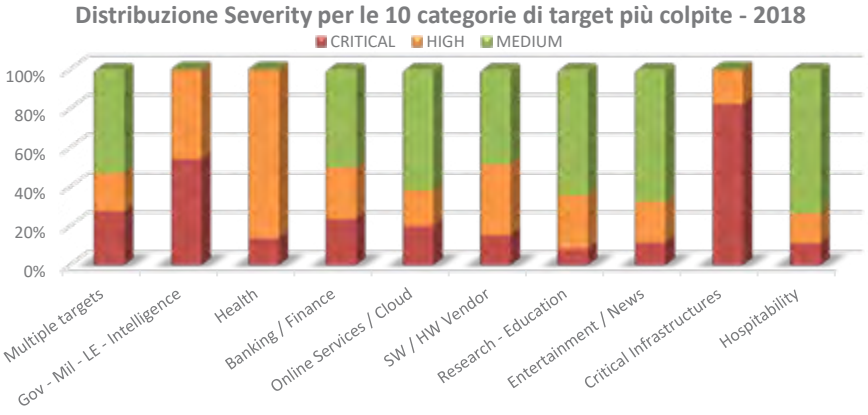
Si osserva pertanto un *apprezzabile aumento della Severity media rispetto al 2017*, il che va considerato come un moltiplicatore dell'aumento puramente numerico degli attacchi osservati per avere un quadro più preciso dei rischi.

Raggruppando le nostre valutazioni di Severity per le consuete categorie (Attaccanti, Vittime e Tecniche di attacco) emergono ulteriori elementi di interesse.



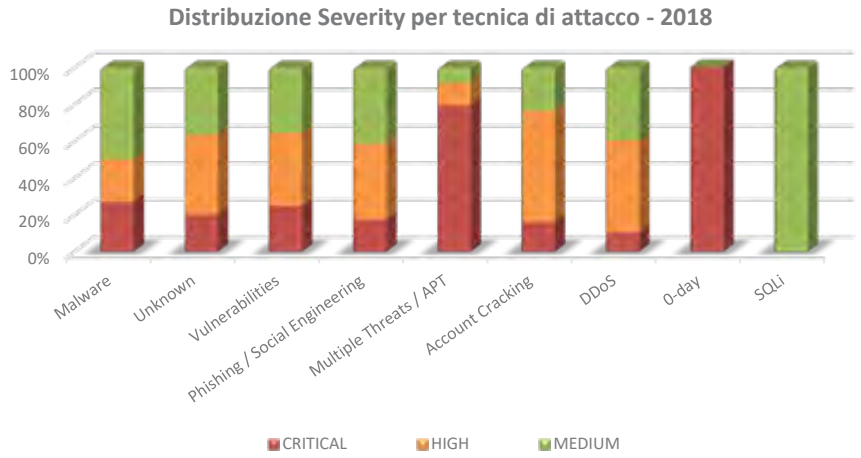
Non sorprende che il maggior numero di attacchi classificati come "Critici" riguardino le categorie Espionage e Information Warfare, mentre la prevalenza di attacchi con impatto di tipo "Medio" e "Alto" riferiti ad attività cybercriminali si spiega con la necessità, per questi soggetti, di rimanere relativamente sottotraccia, guadagnando sui grandi numeri più che sul singolo attacco (tranne casi particolari).

Interessante anche notare come l'Hacktivism, pur in grande diminuzione, presenti un'ampia percentuale di attacchi con impatto di tipo "Alto" e abbia un valore medio della Severity peggiore rispetto alla categoria Cybercrime (pur essendo numericamente molto meno rappresentato nel campione).



© Clusit - Rapporto 2019 sulla Sicurezza ICT in Italia

Si può notare come le categorie "Critical Infrastructures" e "Gov" abbiano subito il maggior numero di attacchi con Severity "Critical", mentre le categorie con il maggior numero di attacchi con impatti di livello "Alto" sono "Healthcare" e "SW/HW Vendor".



© Clusit - Rapporto 2019 sulla Sicurezza ICT in Italia

Gli attacchi con impatto più critico sono quelli realizzati tramite APT e 0-day (quindi più sofisticati e stealth, spesso con motivazioni geopolitiche e finalità di Espionage e Information Warfare).
Molto simili in percentuale gli attacchi con impatto "Critico" realizzati tramite Malware e Vulnerabilità note, mentre prevalgono gli impatti di tipo "Alto" nel caso di attacchi condotti tramite tecniche di Account Cracking, DDoS e Unknown.

Infine presentiamo un confronto tra la Severity media del 2017 e quella del 2018, in base alle categorie di bersagli. Come si evince chiaramente dalla tabella (considerato che nella nostra scala di misurazione 1 è "Critical" e 3 è "Medium"), le medie del 2018 sono praticamente tutte più basse (ovvero peggiori) rispetto a quelle del 2017.

Severity 2018 vs 2017	CRITICAL	HIGH	MEDIUM	TOT	MEDIA 2018	MEDIA 2017	TREND
Multiple targets	84	59	161	304	2,3	2,4	
Gov - Mil - LE - Intelligence	137	115	0	252	1,5	1,4	
Healthcare	22	137	0	159	1,9	2,4	
Banking / Finance	37	41	78	156	2,3	2,0	
Online Services / Cloud	26	23	80	129	2,4	2,7	
SW / HW Vendor	17	40	53	110	2,3	2,4	
Research - Education	9	30	70	109	2,6	2,8	
Entertainment / News	12	21	69	102	2,6	2,7	
Critical Infrastructures	47	10	0	57	1,2	1,7	
Hospitability	5	7	33	45	2,6	2,4	
GDO / Retail	5	7	27	39	2,6	2,9	
Others	4	7	19	30	2,5	2,4	
Organization - ONG	6	6	6	18	2,0	2,4	
Gov. Contractors / Consulting	12	2	0	14	1,1	1,5	
Telco	6	2	3	11	1,7	2,5	
Automotive	2	3	4	9	2,2	2,3	
Religion	1	1	2	4	2,3	0,0	-
Security	0	2	1	3	2,3	2,5	
Chemical / Medical	1	0	0	1	1,0	0,0	-

Questo tipo di analisi consente di evidenziare alcuni fenomeni "nascosti" nei dati del campione.

Per esempio, grazie a questo confronto si evince che i settori "Healthcare" e "Critical Infrastructures", considerando contestualmente il peggioramento della Severity media, il numero (alto) di attacchi subiti e la percentuale (alta) di crescita degli attacchi rispetto al 2017, risultano essere quelli per i quali i rischi cyber sono cresciuti maggiormente nel 2018, mentre le categorie "Gov" e "Multiple targets", pur avendo subito in assoluto un numero di attacchi maggiore, non mostrano peggioramenti significativi in termini di Severity.

Nelle prossime edizioni del Rapporto Clusit raffineremo e dettaglieremo ulteriormente questo nuovo tipo di considerazioni sul campione.

Analisi Fastweb della situazione italiana in materia di cyber-crime e incidenti informatici

Introduzione e visione d'insieme

Il 2018 è stato un anno particolarmente complesso e il panorama delle minacce cyber negli ultimi 12 mesi è evoluto in maniera importante.
Dopo il picco raggiunto nel 2017, gli attacchi di tipo "ransomware" iniziano ad avere una leggera flessione il numero di nuove infezioni si è stabilizzato. Il motivo legato a questo rallentamento è dovuto in parte alla nascita di nuove contromisure a protezione delle macchine, in parte agli attaccanti che hanno spostato la loro attenzione sul crypto-jacking.
Questa nuova generazione di malware che avevamo già iniziato a vedere l'anno scorso, è in grado di utilizzare la capacità di calcolo delle macchine infettate per generare (in gergo mining *"estrarre"*) cryptovalute come Bitcoin, Monero o Ethereum. Tali infezioni possono avvenire o tramite software malevolo direttamente sulla macchina, oppure semplicemente visitando siti web compromessi (javascript mining).

Quest'anno abbiamo anche osservato un'evoluzione legata agli attacchi di tipo APT (Advanced Persistent Threat). Tali attacchi, mirati a soggetti specifici, diventano sempre più evoluti e sofisticati e utilizzano in maniera estensiva tecniche di spear phishing.
La differenza da altri tipi di phishing è che viene preso come obiettivo una persona in particolare o un impiegato di una azienda specifica. Tale modalità fa sì che lo spear phishing diventi ancora più efficace e quindi pericoloso: il cybercrime raccoglie informazioni relative alla vittima in modo tale che questa possa essere ingannata. È infatti molto complesso distinguere un'e-mail di spear phishing ben ideata da una normale, per questo è più facile che le vittime cadano nella trappola.

Ci sono però anche segnali positivi relativamente alla diffusione di nuove tecnologie, sempre più accessibili dal punto di vista economico e che rispondono alle sempre crescenti minacce riuscendo in qualche caso a prevenire i così detti attacchi "zero-days" sfruttando tecniche evolute di machine learning e artificial intelligence.
Nei prossimi capitoli entreremo nel dettaglio dei vari attacchi fornendo un quadro di sintesi di quanto rilevato nel corso del 2018 in relazione alle principali minacce informatiche.

Dati analizzati

Quest'anno abbiamo raccolto oltre 40 milioni di eventi di sicurezza (una base dati del 14% superiore a quella utilizzata per il report 2017). Il dominio di analisi è costituito dai dati ottenuti dal nostro Security Operations Center e relativi agli indirizzi IP appartenenti all'Autonomous System (AS) Fastweb: oltre 6 milioni di indirizzi pubblici su ognuno dei quali possono comunicare decine o anche centinaia di dispositivi e server attivi presso le reti dei Clienti.

I dati raccolti sono stati arricchiti, analizzati e correlati con l'aggiunta di quelli forniti da organizzazioni esterne come ad esempio la Shadowserver Foundation, fonte autorevole e molto dettagliata in merito all'evoluzione delle botnet e dei relativi malware. Inoltre sono stati considerati eventi e segnalazioni dei principali CERT nazionali e internazionali.
I dati sugli attacchi di Distributed Denial of Service, sono stati ricavati da tutte le anomalie DDoS rilevate dalle tecnologie di Fastweb per il contrasto di questo tipo di attacchi. Allo stesso modo le informazioni relative alle principali tipologie di minacce riscontrate sono state raccolte da piattaforme interne utilizzate per attività di Incident Management.
Le indicazioni relative alle frodi sul protocollo VOIP sono invece frutto delle analisi effettuate dal Dipartimento di Fraud Management della Direzione Security di Fastweb.

È importante sottolineare che tutti i dati, prima di essere analizzati, sono stati automaticamente aggregati e anonimizzati per proteggere la privacy e la sicurezza sia dei Clienti sia di Fastweb stessa.

Tipologia di Malware e di Botnet

La composizione dei Malware e Botnet che interessano le macchine appartenenti all'AS di Fastweb si è evoluto rispetto alla precedente rilevazione dell'anno 2017.
Infatti quest'anno sono state individuate 212 famiglie di software malevoli (+10% rispetto all'anno precedente).
Sono state rilevate diverse minacce già presenti lo scorso anno, ma la vera novità riguarda la diffusione massiva di nuovi malware, non ancora classificati e riconducibili a una famiglia nota.
Zeroacces, classificato come "rootkit" è un virus che una volta preso, dirotta il browser web verso pagine che promuovono programmi malware o altro. È anche in grado di veicolare altri tipi di malware specifici e di nascondersi alle scansioni dell'antivirus tradizionale. Infine blocca l'accesso ai siti in cui viene indicato come rimuoverlo in modo che la vittima abbia difficoltà a "chiedere aiuto".
Nei primi posti, troviamo anche quest'anno il noto ransomware Wannacry seguito da Gozi e Ramnit.
Questi ultimi due che insieme coprono il 15% dei malware totali, sono malware specifici per il mercato finanziario e sono in grado intercettare credenziali legate all'home banking trasmettendo quindi agli attaccanti username e la password di accesso alla banca della vittima.
Infine rileviamo un 19% di software malevoli (in aumento dell'11% rispetto al 2017) che non sono ancora stati catalogati di cui non si conoscono tutti i dettagli.

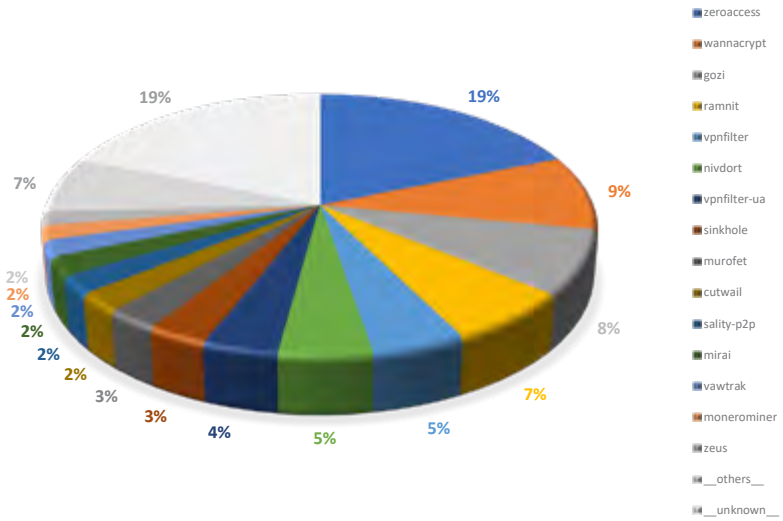


Figura 1 - *Analisi dei Malware rilevati (Dati Fastweb relativi all'anno 2018)*

Andamento temporale

Il grafico di seguito mostra la diffusione temporale degli host infetti e parte di botnet per l'anno 2018. Come si può notare il trend è in calo e in diminuzione anche rispetto all'anno precedente.

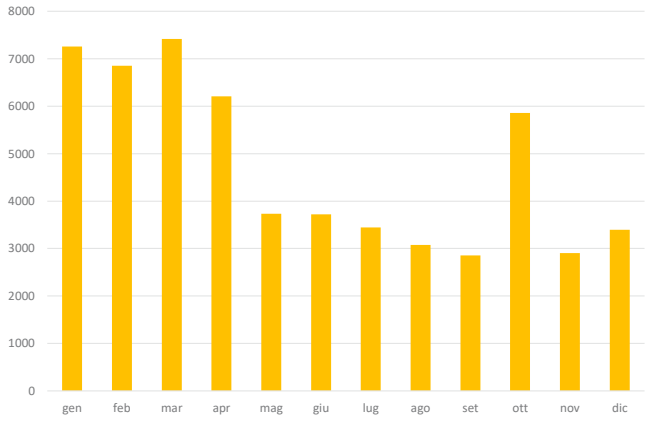


Figura 2 - *Distribuzione temporale del numero di Malware rilevati (Dati Fastweb relativi all'anno 2018)*

Da evidenziare il picco di circa 5900 host infetti durante il mese di ottobre dovuto a una campagna basata sul malware "vpnfilter".
Questo malware, che colpisce i router delle vittime prendendone il pieno controllo, ha iniziato a colpire nel mese di giugno 2018 e ha avuto il suo picco di infezioni proprio nel mese di ottobre.

Principali famiglie di malware e botnet

Analizzando i trend temporali delle varie tipologie di malware si nota una prima metà dell'anno con un trend costante, la seconda metà dell'anno è caratterizzata da una crescita del numero di infezioni da malware con una prevalenza per le infezoni legate a vpnfilter, wannacry e ramnit.
È importante però evidenziare come, nella prima metà dell'anno si siano rilevati eventi (un picco di 8500 nel mese di febbraio) relativi a minacce non immediatamente catalogate e/o riconducibili ad attacchi di tipo mirato. Tali tipologie di attacchi sono più pericolose della media perché non rilevabili da sistemi di protezione tradizionali che necessitano il rilascio di signature per identificarli (ad esempio gli antivirus). Tale trend si è poi ridimensionato nella seconda metà dell'anno dove sono state create "contromisure" efficaci alle campagne malware iniziate a partire dal mese di settembre 2017.

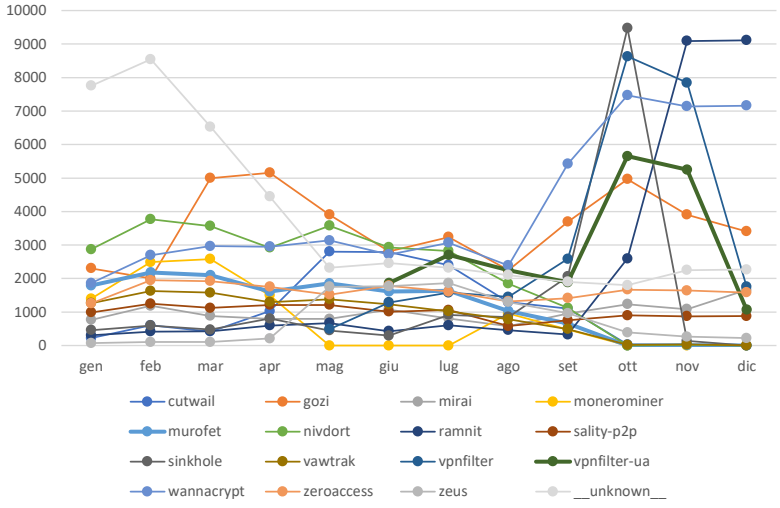


Figura 3 - *Rilevazione mensile dei Malware (Dati Fastweb relativi all'anno 2018)*

Distribuzione geografica dei centri di comando e controllo dei malware

I centri di Command and Control (C&C) rappresentano i sistemi compromessi utilizzati per l'invio dei comandi alle macchine infette da malware (bot) utilizzate per la costruzione delle botnet.

È confermato che anche quest'anno ben oltre la metà dei centri di C&C relativi a macchine infette appartenenti all'AS di Fastweb si trovano negli Stati Uniti (52%). Tale dato è però in calo rispetto all'anno precedente e si nota come i centri C&C stiano crescendo in maniera importante anche in Europa (+24% rispetto all'anno 2017).

È bene sottolineare che molto spesso questi ip sono in realtà dei proxy ponte attraverso il quale i veri attaccanti nascondono il loro effettivo punto di intervento. Soprattutto perché è più semplice operare azioni attraverso macchine ponte che si trovano in cosiddetti "paesi amici".

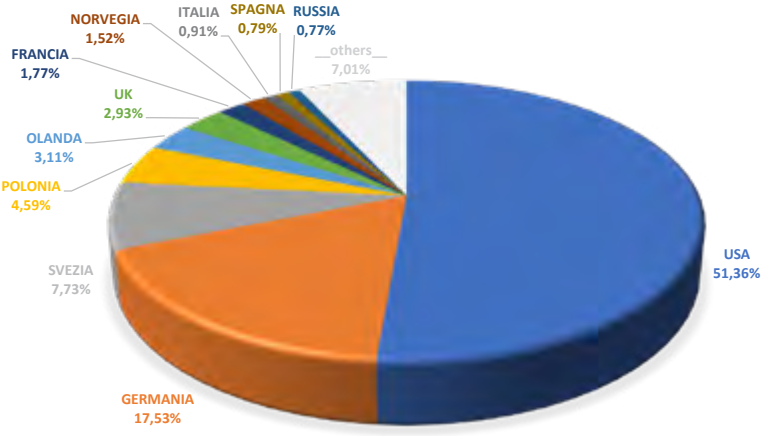


Figura 4 - *Dislocazione dei centri di Comando e Controllo (Dati Fastweb relativi all'anno 2018)*

Attacchi DDOS (Distributed Denial of Service)

Un attacco DoS (Denial of Service) è un attacco volto ad arrestare un computer, una rete o anche solo un particolare servizio.

Alcuni attacchi hanno come target una particolare applicazione o servizio, ad esempio Web, SMTP, FTP, etc., altri invece mirano a mettere fuori uso completamente il server o, addirittura, un'intera rete. Gli attacchi DDoS (Distributed Denial of Service) amplificano la portata di tali minacce.

Un attacco DDoS viene infatti realizzato utilizzando delle botnet, ovvero decine di migliaia di dispositivi (non più solo computer di ignari utenti), in grado di generare richieste verso

uno specifico target con l'obiettivo di saturarne in poco tempo le risorse e di renderlo indisponibile.
Naturalmente gli effetti di un attacco DDoS possono essere devastanti sia a causa della potenza che possono esprimere, ma anche per le difficoltà insite nel poterli mitigare in tempi rapidi (se non attraverso la sottoscrizione di un specifico servizio di mitigation).
Il mercato dei DDoSaaS (DDoS as a Service) è cresciuto e il costo del servizio si aggira sui 5-10$ mese per botnet in grado di erogare un attacco di 5-10 minuti a oltre 100Gbps.

Quanti sono stati gli attacchi DDOS nel 2018?

Nel 2018 sono state rilevate oltre 9.300 anomalie riconducibili a possibili attacchi DDoS diretti verso i Clienti Fastweb (+32% rispetto allo stesso periodo del 2017).

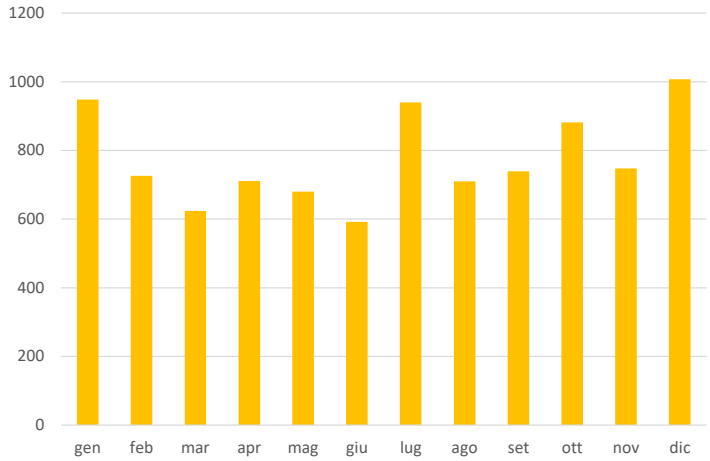


Figura 5 - *Distribuzione mensile delle anomalie DDoS (Dati Fastweb relativi all'anno 2018)*

Quali sono i settori più colpiti

Abbiamo voluto fornire maggiori dettagli in merito alla distribuzione dei target degli attacchi DDoS andando a esplicitare i settori merceologici maggiormente colpiti da questo tipo di attacchi.
Come si evince dal grafico successivo, il fenomeno riguarda senza esclusione un esteso numero di settori tra i quali i più esposti risultano essere le istituzioni governative (soprattutto Ministeri e Pubbliche Amministrazioni centrali) che sono obiettivo nel 30% dei casi, a seguire il mondo dei servizi, quindi i mercati Finance e Insurance.

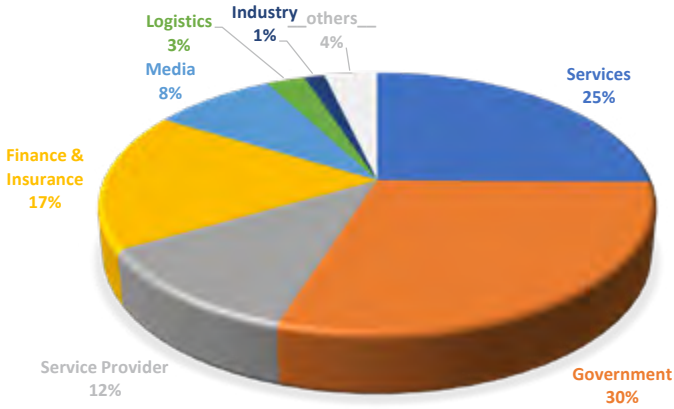


Figura 6 - *Target di possibili attacchi DDoS (Dati Fastweb relativi all'anno 2018)*

Il volume degli attacchi DDoS

Il grafico seguente rappresenta il volume degli attacchi DDOS durante l'anno. La piattaforma di mitigation utilizzata per la protezione dei Clienti, gestisce ogni mese attacchi che occupano una banda variabile tra i 350 Gbps e i 3 Tbps.
Come si può notare il trend è in crescita, soprattutto se si considera la seconda metà dell'anno, con picchi di attacchi a oltre 3 Tbps nel mese di ottobre 2018.

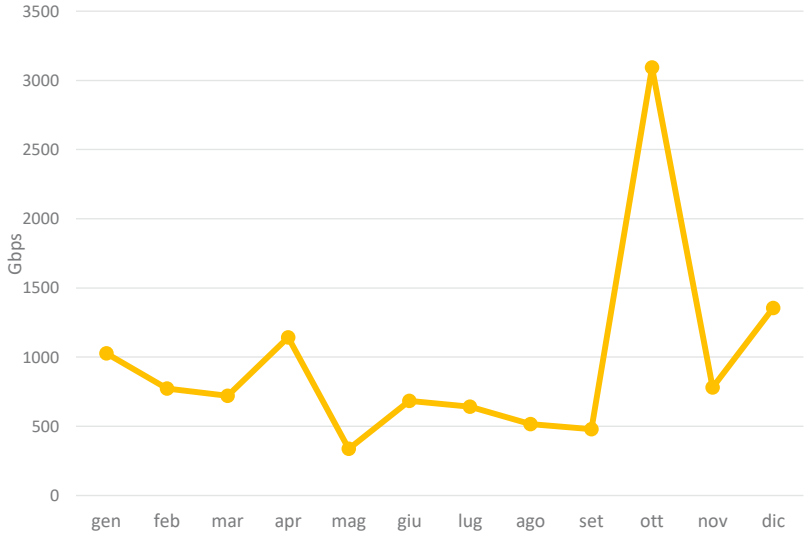
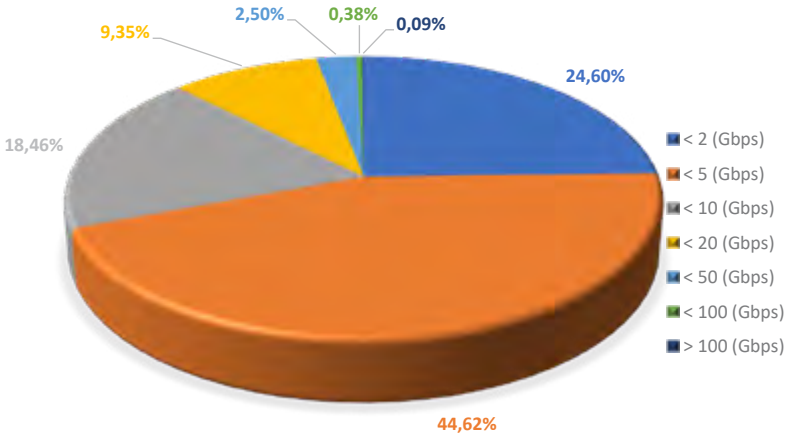


Figura 7 - *Banda totale mensile impegnata negli attacchi DDoS (Dati Fastweb relativi all'anno 2018)*

Di seguito invece riportiamo la distribuzione della banda media di un attacco DDoS nel 2018.



Qual è la durata di un attacco DDOS?

Le tecniche di attacco DDoS e i relativi metodi di mitigazione si evolvono nel tempo. Nel corso degli anni, con il consolidamento delle tecniche di difesa, la durata degli attacchi è mediamente diminuita.

Si è osservato che quest'anno oltre l'95% degli attacchi è durato meno di 3 ore, mentre i rimanenti casi sono principalmente riconducibili a diversi tentativi effettuati in sequenza ravvicinata. È importante però evidenziare che il 2% di questi durino oltre le 24 ore consecutive. Rispetto all'anno precedente si nota quindi un leggero aumento (+3%) di attacchi di piccola durata.

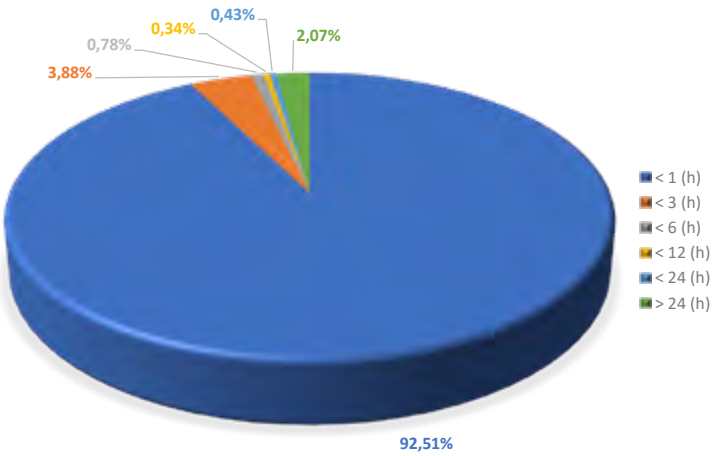


Figura 8 - *Durata dei possibili attacchi DDoS (Dati Fastweb relativi all'anno 2018)*

Tecniche di attacco utilizzate

Le tecniche di attacco utilizzate possono essere diverse, nell'anno 2018 abbiamo rilevato tre principali tipologie ricorrenti con una prevalenza di attacchi di tipo "DNS Amplification". Tale attacco che quest'anno ha registrato il 44% del totale è anche chiamato DNS Reflector attack è un attacco di tipo Distributed Denial of Service (DDoS) che abusa di server DNS open resolver e ricorsivi (recursive) inviando a questi ultimi pacchetti contenenti informazioni falsificate sull'IP di provenienza (IP spoofing).

La seconda tecnica di attacco più utilizzata (25%) è "SNMP Amplification attack" ovvero un tipo di attacco Distributed Denial of Service (DDoS) che richiama le precedenti generazioni di attacchi di amplificazione DNS.
Anziché utilizzare il protocollo Domain Name Server (DNS), gli attacchi SNMP utilizzano l'omonimo protocollo (Simple Network Management Protocol), utilizzato per configurare e raccogliere informazioni da dispositivi di rete come server, hub, switch, router e stampanti.

La terza tecnica di attacco più utilizzata invece è "NTP Amplification" che raggiunge circa il 10% degli attacchi totali.
Un attacco di amplificazione NTP rientra nella famiglia degli attacchi DDoS in cui un utente malintenzionato sfrutta una funzionalità del server Network Time Protocol per saturare una rete o un server con una quantità amplificata di traffico UDP, rendendo l'obiettivo e l'infrastruttura circostante inaccessibile al traffico lecito.
L'8% degli attacchi registrati riguardano invece traffico perfettamente lecito, generato però in maniera massiccia da più bot in modo da esaurire le risorse di banda e computazionali

del server (tipicamente web application). Come si può ben immaginare, quest'ultimi sono molto più complicati da gestire, poiché la discriminazione del traffico malevolo avviene attraverso l'attivazione di contromisure molto più raffinate rispetto a quanto necessario per ripulire tecniche di attacco volumetrico meno elaborate (come quelle descritte prima).

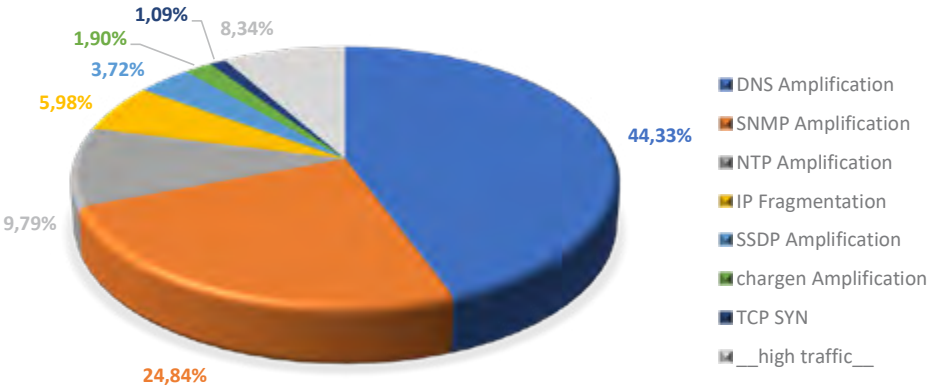


Figura 9 - *Tipologie di attacchi DDoS (Dati Fastweb relativi all'anno 2018)*

Attacchi ai Protocolli VOIP

Le principali minacce

I servizi VOIP (Voice Over Internet Protocol) rappresentano una modalità di trasmissione di voce e traffico multimediale su reti IP dove le comunicazioni vocali vengono convertite, pacchettizzate e trasmesse sotto forma di traffico dati.
In questo modo è possibile abilitare chiamate tra PC e telefoni IP, ma anche verso la rete telefonica classica (tramite una conversione del formato effettuata tipicamente dalla rete dell'operatore).
Il vantaggio maggiore delle comunicazioni VOIP è la sensibile riduzione dei costi che è possibile ottenere dato che può sfruttare le sinergie con la rete dati. D'altra parte questo meccanismo è caratterizzato da possibili vulnerabilità (tipiche di una classica rete IP) e può ampliare la superficie d'attacco alla quale le Aziende sono esposte.
Le particolarità e vulnerabilità dello specifico protocollo possono infatti rappresentare un'ulteriore modo per condurre attacchi mirati e frodi contro aziende e organizzazioni. Le problematiche sono varie: si può trattare di scenari evoluti di Social Engineering e intercettazione fino a possibili interruzioni di servizio (DoS e DDoS) e Service Abuse (dove l'infrastruttura della vittima viene utilizzata per generare traffico verso numerazioni a tariffazione speciale).

I dati Fastweb

Nell'ambito dello studio delle attività illecite condotte sfruttando tali protocolli, anche nel 2018 il Dipartimento di Fraud Management della Direzione Security di Fastweb ha analizzato i trend legati alle piattaforme dei propri Clienti: la maggior parte degli attacchi sono concentrati su piattaforma VOIP, considerando che la quasi totalità di utenti Fastweb utilizza questa piattaforma. L'incidenza degli attacchi su VOIP è tuttavia di molto inferiore rispetto all'incidenza sulla tradizionale tecnologia TDM.

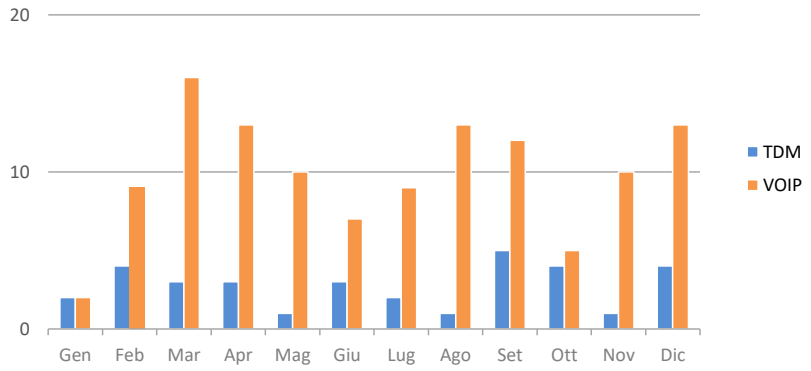


Figura 10 - *Andamento delle frodi durante l'anno (Dati Fastweb relativi all'anno 2018)*

I dati osservati mostrano che circa la metà degli attacchi all'infrastruttura VOIP è diretta verso Clienti di tipo Small Business (piccole imprese): spesso queste aziende non hanno particolari competenze di tipo tecnico e il rischio di utilizzare dispositivi non correttamente configurati né monitorati è più elevato rispetto ad altri segmenti di clientela. Occorre quindi affidarsi a tecnici specializzati, effettuare controlli periodici dei propri dispositivi ed eseguire anche gli aggiornamenti suggeriti dai produttori.

Per ridurre il rischio di intrusione illecita su dispositivi come i centralini digitali, è consigliabile impostare password sicure e aggiornarle periodicamente.

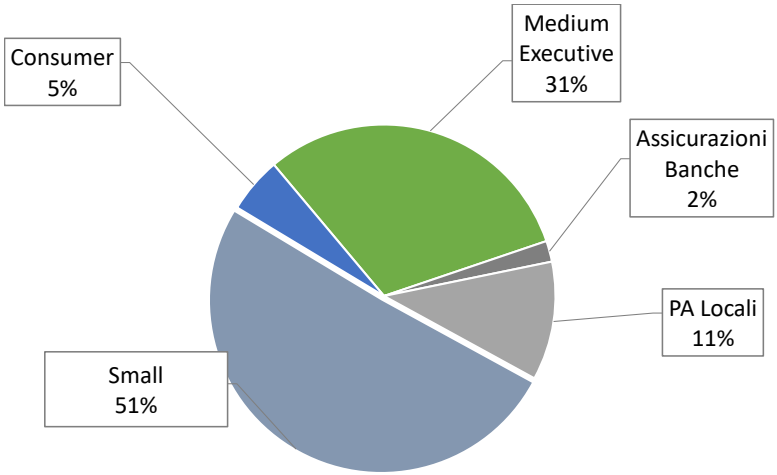


Figura 11- *Vittime di truffe VOIP (Dati Fastweb relativi all'anno 2018)*

La maggior parte delle frodi riscontrate riguarda casi di "Service Abuse", ovvero attacchi volti a generare traffico illecito verso direttrici a tariffazione speciale.

Nel grafico seguente si evidenziano i principali paesi ospitanti le direttrici che hanno generato frodi.

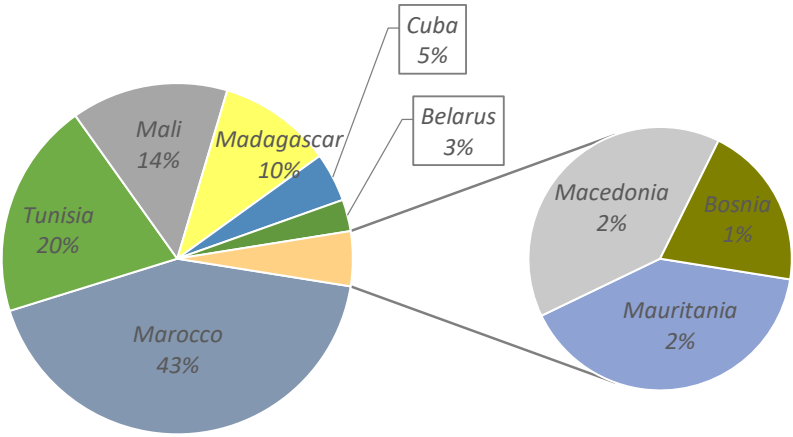


Figura 12 - *Paesi ospitanti le direttrici dei principali attacchi*
(Dati Fastweb relativi all'anno 2018)

Ulteriori vulnerabilità

Servizi critici esposti su Internet

In questo paragrafo viene messo in evidenza il numero di dispositivi che espongono servizi direttamente su Internet privi anche di livelli minimi di protezione. Ciò significa che questi host sono facilmente attaccabili e esposti a rischi elevati di compromissione.
I dati del 2018 riportano circa 58.000 macchine che espongono servizi critici direttamente su Internet anche se si osserva una contrazione del 18% del numero totale di host esposti rispetto al 2017.

Al primo posto troviamo Telnet, protocollo utilizzato per la gestione di host remoti, accessibile da riga di comando, al secondo posto troviamo SMB, utile per la condivisione di file e stampanti nelle reti locali ma che se esposto su internet può essere utilizzato per accedere ai documenti e file condivisi.
Di rilievo è anche la quantità di macchine che espongono RDP, utilizzato per la connessione remota a un PC. Un attaccante potrebbe sfruttare questo protocollo per prendere il controllo completo della macchina.

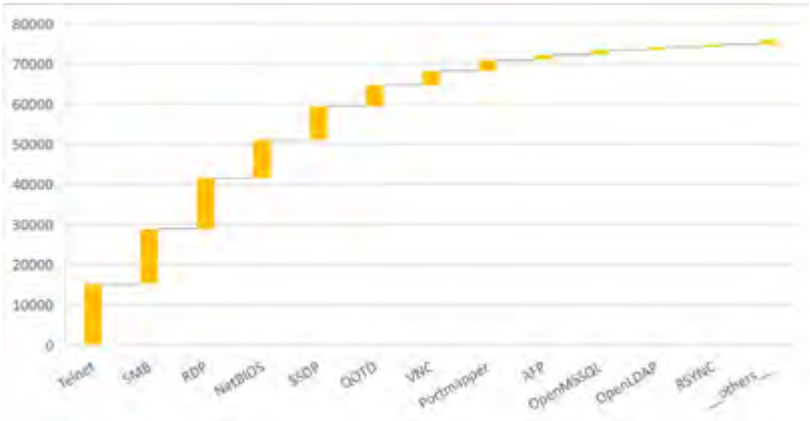


Figura 13 - *Servizi esposti direttamente su Internet (Dati Fastweb relativi all'anno 2018)*

Blacklist

Una blacklist è una lista dove vengono inseriti e catalogati indirizzi IP classificati come fonte di e-mail di SPAM.

Ci sono diversi motivi per cui si può essere inseriti nelle liste nere, di seguito cercheremo di analizzare i principali:

- Invio di e-mail massive dal proprio indirizzo.
- Nel testo o nell'oggetto delle e-mail inviate sono presenti caratteri e simboli in genere utilizzati nelle mail di SPAM.
- Il pc è infetto da virus che invia autonomamente e ciclicamente email infette.

Dalle nostre rilevazioni abbiamo notato che circa 10.500 IP sono stati inseriti almeno una volta nelle blacklist durante il 2018. Il dato è in sensibile calo rispetto al 2017 dove avevamo registrato oltre 40.000 azioni di blacklisting.
Il grafico di seguito rappresenta le città maggiormente colpite.

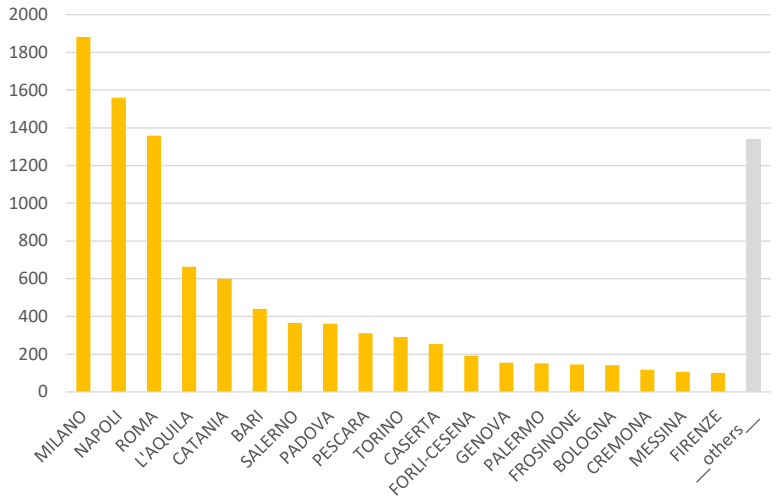


Figura 14 - *Host in Blacklist per città (Dati Fastweb relativi all'anno 2018)*

Rapporto 2018 sullo stato di Internet - Analisi globale degli attacchi di DDoS, applicativi e furto di identità
[a cura di AKAMAI]

"Follow the money!"

Gli attacchi di Distributed Denial of Service (DDoS) sono sempre un ottimo punto di partenza per una analisi annuale, principalmente perché la tendenza in questo ambito è relativamente stabile.
Guardando indietro possiamo notare come i picchi di attacco in termini di banda generata crescano di circa il 9% ogni tre mesi, un raddoppio ogni due anni, statistica curiosamente simile alle legge di Moore (del 1965!) che seppur in ambiti differenti prevedeva un raddoppio ogni 18 mesi.
Si noti che la curva di crescita è irregolare e i nuovi picchi vengono raggiunti quando gli attaccanti scoprono un nuovo metodo per generare attacchi di DDoS come ad esempio l'uso di Memcached di cui parleremo in seguito o della botnet Mirai tanto in voga negli scorsi anni.
Nel tempo che intercorre tra due picchi quello che si può osservare è che il settore IT inizia a lavorare per chiudere la falla appena scoperta. In questo senso, abbiamo nuove release software oppure amministratori di sistema che disabilitano quei servizi non necessari trasformati in veicolo di attacco. Al tempo stesso gli attaccanti iniziano a contendersi le risorse utili per l'attacco. Il risultato finale è che i singoli attacchi diventano più piccoli, pur rimanendo sempre più grandi di quanto sia possibile mitigare "in casa".
Fino alla prossima vulnerabilità, fino al prossimo picco.

Gli attacchi di DDoS, facilmente comprensibili per il grande pubblico, risultano spesso essere efficaci dal punto di vista dell'attaccante ma non particolarmente efficienti. Dopotutto si tratta di una prova di forza che richiede un uso di risorse significative.
Ecco perché, pur senza negare il problema degli attacchi di DDoS, il mercato mostra la necessità di difendersi da differenti tipologie di attacco, meno evidenti e più sottili. Ciò è dovuto al proliferare di differenti attacchi "low and slow" che non richiedono grandi risorse ma hanno come risultato quello di massimizzare l'impatto dell'attaccante. Il solo apparentemente superato attacco Slowloris è un esempio di questa modalità.

Salendo di complessità è dove si incontrano i trend di attacco più interessanti. Come spesso succede, gli attaccanti si spostano alla ricerca di denaro e non deve stupire come uno degli argomenti più caldi dell'anno appena trascorso sia relativo alle credenziali utente che possono essere vendute nel dark web. Il tema in sé non è nuovo, ciò che è nuovo sono attacchi specificamente progettati per ottenere credenziali valide.

Guardando al futuro non possiamo ignorare il crescente interesse del mercato verso il paradigma "Zero Trust" a cui dedichiamo la parte finale della nostra analisi. Il motivo è semplice: il vecchio paradigma di sicurezza, all'interno della rete i buoni e fuori i cattivi, è ampiamente superato. In un mondo iperconnesso, gli utenti, i dati e le applicazioni sono ovunque e il paradigma di sicurezza non può che adeguarsi.

(Riferimenti: #1, #2, #3)

"It's not a bug; it's an undocumented feature!"

#1 - Memcached

Memcached è un software spesso usato sui server web per effettuare caching di dati e per diminuire il traffico sul database o sul backend.
Il server memcached è pensato per non essere esposto direttamente su Internet, per questo nella sua configurazione di default non richiede autenticazione e risponde sia via TCP che via UDP. Si stima che a Febbraio 2018 ci fossero circa 50.000 server memcached esposti pubblicamente su internet, senza autenticazione e con UDP abilitato. Una sorta di bomba a orologeria in attesa di essere scoperta.
Gli attaccanti hanno iniziato a usare questa grande quantità di server per generare traffico di "riflessione" basato su UDP. Il funzionamento di base di questo tipo di attacco si basa sul creare pacchetti di richiesta UDP (generalmente di pochi bytes) riportanti come sorgente l'indirizzo IP dell'obiettivo. Questi pacchetti vengono inviati ai server memcached che in mancanza di autenticazione applicativa e per via della intrinseca natura UDP, rispondono inviando all'indirizzo IP sotto attacco grandi quantità di dati.
Si stima che con questa tipologia sia possibile "amplificare" la potenza di fuoco dell'attaccante di un fattore maggiore di 50.000X.

Fig.1 - *Amplificazione di un attacco*

Proprio per questo motivo il 28 febbraio 2018, si è verificato il più esteso attacco DDoS mai registrato, indirizzato a un cliente Akamai, con un traffico DDoS di riflessione memcached record pari a 1,3 terabit al secondo (Tbps).

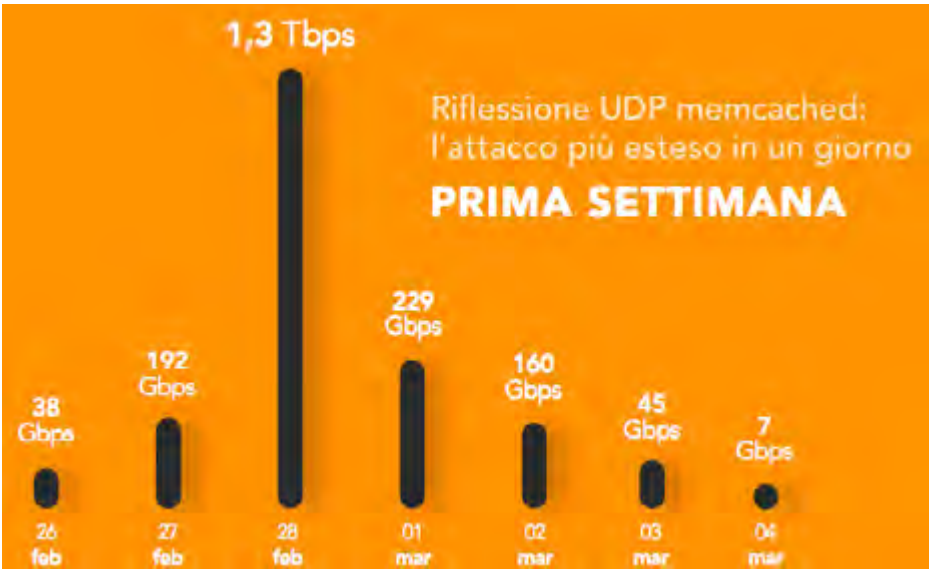


Fig.2 - *Picchi giornalieri di un attacco basato su memcached*

Fig.3 - *Picco di 1,3Tbps di un attacco basato su memcached*

L'attacco ha avuto dimensione doppia rispetto al precedente picco generato da Mirai, nota botnet di IoT (Internet of Things), che nel 2016 aveva destato scalpore.
Questa tipologia e dimensione di attacco è una ulteriore conferma di come sia inadeguato pensare a un meccanismo di difesa incentrato su hardware on premise. Il posizionamento di queste soluzioni non è coerente con i pattern attuali. Per questo motivo anche il mercato riconosce sempre di più la validità di soluzioni di protezione esterne basate su approccio cloud.

Infine, Memcached è stato senza dubbio uno del metodi utilizzati dai vari servizi di booter che, già da alcuni anni rappresentano una minaccia seria per ogni business. Fornito dai booter come "DDoS as a service", l'attacco è banale da lanciare anche per chi non ha conoscenze informatiche. A Dicembre 2018 il Dipartimento di Giustizia americano ha annunciato di aver chiuso circa 60 siti di questo tipo.

(Riferimenti: #4, #5, #6)

"It's not a bug; it's an undocumented feature!"

#2 - Universal Plug and Play

Universal Plug and Play (UPnP) è un protocollo largamente usato in ambito consumer per facilitare la configurazione di apparati e permette a due o più terminali di comunicare tra loro in maniera semplice per condividere un disco, aprire una porta sul router o altro.
Nel caso di un router, è possibile usare UPnP per impostare una regola di NAT o PAT che altrimenti l'utente non sarebbe presumibilmente in grado di configurare. La comunicazione avviene tramite richieste simili a delle chiamate web.
Fin dagli albori del protocollo sono stati trovate bachi implementativi più o meno gravi. Durante le attività di indagine relative a un attacco ricevuto e mitigato da Akamai, è stato scoperto come, nonostante la longevità del protocollo, ci siano molti router vulnerabili a un attacco di NAT Injection.

La modalità di infezione è basata sul fatto che un router vulnerabile è in grado di ricevere un comando di creazione di una regola NAT proveniente dall'esterno anziché dalla rete interna come sarebbe lecito aspettarsi. Il router accetta il comando e lo implementa.

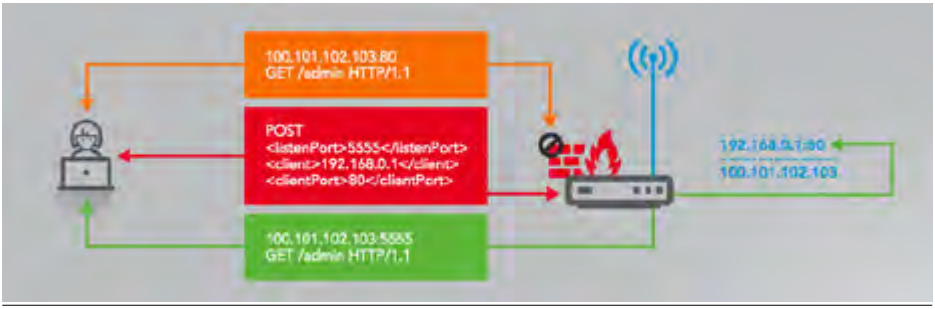


Fig.4 - *Esempio di PAT Injection tramite bug di UPnP*

In questo modo un attaccante è in grado di raggiungere client poco protetti come, per esempio, una macchina Windows non correttamente configurata dall'utente medio, attraverso porte come HTTP/S, FTP o altre ancora più appetibili come 139 e 445 (NetBios e SMB). Ad Aprile 2018 lo scenario era solo ipotetico ma a Novembre 2018 una nuova scansione ha

individuato 45.000 macchine esposte tramite SMB contro cui sfruttare le vulnerabilità di EternalBlue (CVE-2017-0144) o EternalRed (CVE-2017-7494).
Il pericolo di UPnP Proxy è relativo a un difetto implementativo di alcuni modelli di router. Attraverso questo meccanismo si amplia il parco delle potenziali vittime, situazione ideale per un attaccante che in questo modo ha accesso a macchine ottimamente connesse attraverso broadband o fibra ottica. Tale arsenale può essere sfruttato per gli scopi più nefasti come spam e phishing, account takeover (di cui discuteremo in seguito), frodi relative a carte di credito, botnet per fruire di pubblicità, distribuzione di malware, etc. L'elenco, purtroppo non è da considerarsi esaustivo.
Benché manchino indicazioni precise a riguardo, è possibile che la problematica, se non gestita adeguatamente dall'industria IT, sia decisiva per la prossima ondata di attacchi.

(Riferimenti: #7, #8, #9)

Credential Stuffing

Nel cosiddetto "dark web" è possibile comprare diversi tipi di prodotti a prezzi diversi, a volte attraverso vere e proprie aste.
I tempi in cui un hacker con felpa e cappuccio "attaccava", non si è ben capito in che modo, un sito web per ottenere alcuni numeri di carta di credito e usarli per i regali di Natale sono passati. Se mai sono esistiti veramente oramai fanno parte dell'immaginario romantico.
Il mondo hacker segue tecniche e dinamiche simili all'industria, dove domanda e offerta determinano il prezzo di un prodotto.
È possibile comprare: il codice di un exploit non ancora noto, l'elenco di username e password trafugati da non importa dove, singoli numeri di carta di credito garantiti, validi ancora almeno per alcuni giorni etc.
Il fenomeno del Credential Stuffing si basa su due dei nodi più deboli di una intera catena di sicurezza. Il primo sono le persone, il secondo le loro password.
Il concetto di "non usare la stessa password su più siti" è arcinoto. Ce lo sentiamo ripetere spesso e ora anche quando ci registriamo su un nuovo sito. Ma quante persone realmente usano questa accortezza? Ovviamente non stiamo parlando degli addetti ai lavori, che usano un gestore di password o meccanismi simili. Dobbiamo pensare al grande pubblico informaticamente non così evoluto. In questo contesto è molto probabile che venga usata la stessa password su ben più di due siti.
Sfruttando questa vulnerabilità intrinseca, ecco che un attaccante si specializza nella ricerca di combinazioni di username e password valide.

Il primo passo è quello di comprare nel dark web un archivio di username e password trafugate. Con questo database si iniziano a provare tutte le combinazioni su siti diversi alla ricerca di persone che hanno usato più volte la stessa login, spesso un indirizzo email, e la stessa password. Il risultato finale è un distillato di username e password valide su social

media, servizi email, e-commerce il cui valore è molto alto. Ecco quindi che l'uso della stessa password su più siti espone le informazioni personali ben oltre il sito "bucato".
É importante notare che l'attaccante non effettua questo processo di "distillazione" a mano. Piuttosto usa una serie di bot più o meno sofisticati sui quali dividere il lavoro. Di fatto un bot in questo contesto è un software che effettua richieste di login cercando di apparire il più simile possibile a un utente umano. Invia poche richieste usando stringhe di User-Agent simili o uguali a un browser noto e inserendo tutte i parametri tipici di un browser.

Durante il 2018 ci sono stati vari casi di attacchi di questa tipologia ma ne analizzeremo i due più interessanti.
Il primo attacco è stato subito da una banca che riceve la maggior parte dei tentativi di login normalmente attorno all'ora di pranzo. Stiamo parlando di un grande volume di utenti, con picchi di 45 mila login per ora e un totale di oltre 4 milioni di login in una settimana. In una giornata tipo, con volumi di questo tipo, è normale ricevere 800 richieste di login fallite ogni ora. Durante l'attacco il volume di login fallite è cresciuto di un ordine di grandezza. In una settimana intera si sono registrati 315.178 richieste di login, da 19.992 indirizzi IP differenti con 4.382 differenti User-Agent da 1.750 diversi Autonomous System. Come si può notare l'attacco è stato architettato ed eseguito con cura nel tentativo di evadere i meccanismi di riconoscimento, variando la tipologia, frequenza e modalità delle richieste di login.

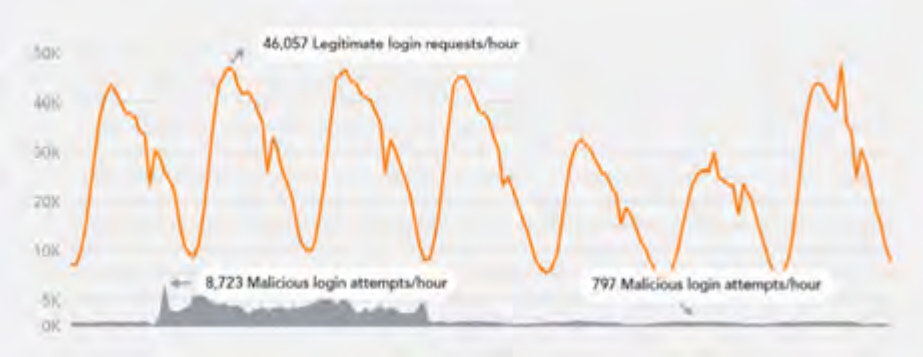


Fig.5 - *Statistiche di traffico durante attacco di credential stuffing (primo caso)*

Fig.6 - *Modalità di generazione del traffico in diverse fasi dell'attacco*

L'attacco appena descritto potrebbe apparire come "rumore di fondo" se non ci fossero meccanismi in essere per riconoscere bot e anomalie sulla pagina di login. In effetti soltanto l'1,5% delle richieste erano parte dell'attacco, una percentuale non nulla ma nemmeno troppo alta.

Nel secondo caso invece l'attaccante, forse per inesperienza o per errore, ha generato un attacco troppo grande per non essere notato. Nel momento di picco sono stati osservati 350.000 tentativi di accesso ogni ora, la maggior parte dei quali falliti, rispetto a un traffico normale di 50.000 accessi ogni ora. In poco tempo l'attacco è stato notato e sono state messe in atto le opportune contromisure. In totale, la botnet protagonista ha generato oltre 8.5 milioni di richieste in due giorni (rispetto alla media di poco più di un milione al giorno) con traffico proveniente da vari stati tra cui Vietnam e Stati Uniti, sfruttando circa 20.000 macchine dislocate in 4.923 Autonomous Systems.

Fig.7 - *Statistiche di traffico durante attacco di credential stuffing (secondo caso)*

Il proliferare dei bot porta a problemi differenti di cui il Credential Stuffing è solo uno degli esempi. Per mitigare tali tipi di attacchi decisamente sottili e pericolosi occorre applicare tecnologie di riconoscimento di bot e della loro gestioni. Si noti l'utilizzo della parola "gestione" in questo contesto rispetto a "blocco" o "mitigazione". Infatti è buona norma cercare di non bloccare i bot (perchè questo sarebbe un messaggio per l'attaccante che andrebbe a cambiare il comportamento del bot generando una corsa del gatto e del topo) ma piuttosto di gestirne il traffico - ad esempio generando messaggi di login fallita anche quando la login è corretta - in modo da scoraggiare l'attaccante e spingerlo verso un altro obiettivo.

Fig.8 - *Dettagli sulle modalità di generazione del traffico per User-Agent, distribuzione IP e paesi*

In parallelo - e speriamo che il presente report possa essere di aiuto - occorre incentivare negli utenti finali l'uso di meccanismi di gestione evoluta delle password (molti sono gratuiti) e far crescere la cultura sull'uso corretto di password e strong authentication.

(Riferimenti: #10, #11, #12)

Uno sguardo al futuro

I temi trattati finora saranno sicuramente di interesse anche per il 2019 in quanto nessuno di essi è esaurito o risolto. Gli attacchi di DDoS continueranno ad esistere, gli utenti a usare le stesse password, gli attaccanti a cercare metodi più efficaci per fare soldi.
Un tema futuro ma che sta ponendo le basi già da qualche anno è relativo a un cambio di approccio alla sicurezza aziendale in generale.
La vecchia visione era ed a volte è tuttora basata sul concetto che vede i buoni dentro la rete aziendale e i cattivi fuori.
I trend di mercato degli ultimi anni relativi all'uso dei servizi cloud e degli utenti in mobilità, tuttavia, hanno portato a fenomeni che non possono più essere gestiti con il vecchio paradigma. Se ci pensiamo bene, i dati aziendali si stanno spesso spostando fuori, nel cloud. Così come gli utenti, sempre meno in numero a lavorare solo dall'ufficio e non dal loro cellulare o in mobilità, le applicazioni e la loro modalità di fruizione. Chi e cosa rimane all'interno dei confini aziendali?
In questo nuovo contesto il paradigma di "Zero Trust" prende sempre più piede e sarà sicuramente trainante nei prossimi anni.
I principi fondamentali sono: si assuma che l'ambiente sia ostile, non si distingua tra utenti interni ed esterni, non si assuma "trust" (da cui il nome), si eroghino applicazioni solo a device e utenti riconosciuti e autenticati, si effettuino analisi dei log e dei comportamenti utente.
In pratica occorre trattare tutti gli utenti nello stesso modo, utenti della stessa azienda o esterni, che siano nel perimetro della rete aziendale o meno, che i dati a cui vogliono accedere siano dentro l'azienda o da qualche parte nel cloud.
Il rovesciamento del paradigma è forte e richiederà anni per la sua completa adozione che prevede meccanismi di autenticazione, autorizzazione e controllo che non sempre sono già implementati. Ma sarebbe un errore non iniziare fin da subito a conoscere l'argomento e iniziare le opportune valutazioni.

(Riferimenti: #13, #14, #15)

Riferimenti

1. https://blogs.akamai.com/sitr/state-of-the-internet/
2. https://blogs.akamai.com/sitr/2018/12/a-year-of-research.html
3. https://blogs.akamai.com/2018/06/summer-soti---ddos-by-the-numbers.html
4. https://blogs.akamai.com/sitr/2018/03/memcached-fueled-13-tbps-attacks.html
5. https://www.akamai.com/it/it/about/our-thinking/threat-advisories/ddos-reflection-attack-memcached-udp.jsp
6. https://www.akamai.com/it/it/multimedia/documents/brochure/memcached-reflection-attacks-launch-a-new-era-for-ddos-brochure.pdf
7. https://blogs.akamai.com/sitr/2018/04/universal-plug-and-play-upnp-what-you-need-to-know.html
8. https://www.akamai.com/it/it/multimedia/documents/white-paper/upnproxy-blackhat-proxies-via-nat-injections-white-paper.pdf
9. https://blogs.akamai.com/sitr/2018/11/upnproxy-eternalsilence.html
10. https://blogs.akamai.com/sitr/2018/09/state-of-the-internet-security---credential-stuffing.html
11. https://blogs.akamai.com/2018/12/defending-credentials-from-automated-attack-tools.html
12. https://www.akamai.com/us/en/solutions/bot-management-and-credential-stuffing.jsp
13. https://www.akamai.com/it/it/solutions/zero-trust-security-model.jsp
14. https://blogs.akamai.com/2018/10/why-traditional-security-isnt-enough.html
15. https://blogs.akamai.com/2018/09/accelerating-your-zero-trust-security-transformation-with-enterprise-threat-protector.html

Email security: i trend rilevati in Italia nel corso del 2018
[A cura di Libraesva]

Introduzione

Immaginiamo di trovarci improvvisamente senza posta elettronica. Quale sarebbe l'impatto sulla nostra vita, sulle nostre aziende e sull'economia del paese?
La posta elettronica è un protocollo antico, nato prima ancora di Internet. Al pari di tanti altri strumenti che utilizziamo continuamente e che diamo per scontati, raramente ci soffermiamo a soppesarne l'importanza. Eppure oggi le nostre aziende, la nostra economia, la nostra produttività dipendono in modo assolutamente determinante dalle comunicazioni di posta elettronica.
Essendo il principale canale di comunicazione per le nostre organizzazioni, non sorprende che l'email sia il vettore principale di attacchi informatici.
In questa analisi della email security del 2018 in Italia ci concentreremo su aspetti concreti, offriremo spunti di riflessione costruttivi senza scendere troppo nel tecnico, accompagneremo ai numeri l'analisi dei nostri specialisti che si occupano a tempo pieno di sicurezza della posta elettronica.

Il panorama italiano di email security nel 2018

Per questo report abbiamo analizzato un campione di 10 miliardi di email ricevute in Italia nel 2018, un campione selezionato per essere rappresentativo del traffico email del paese: traffico consumer, aziende di ogni dimensione, service provider, istituzioni e università.
Oltre il 70% del campione è classificabile come posta indesiderata: spam, malware, phishing ed altri attacchi. Questo valore è più basso rispetto a quello che avevamo registrato lo scorso anno (84%) ma si tratta di un indice che è naturalmente soggetto ad oscillazioni, anche significative, nel corso del tempo.
Nel corso dell'anno lo abbiamo visto variare su base mensile tra il 59% e il 94%, si tratta di oscillazioni fisiologiche legate alle dinamiche delle organizzazioni dedite alla distribuzione del malware, ai grandi operatori dello spam e all'evoluzione e la diffusione delle botnet.

Percentuale di posta indesiderata nel 2018, fonte: Libraesva

Botnet

Le botnet, appunto, restano uno dei canali principali di distribuzione di attacchi di malware e phishing ed è ormai consolidata la transizione verso l'abuso di dispositivi IoT (Internet of Things), in particolare i router.

Questi dispositivi "zombizzati" consegnano grandi quantità di email malevole e lo fanno prevalentemente abusando account di posta legittimi, ovvero autenticandosi con credenziali di utenti legittimi e inviando email a loro nome. Le credenziali sono fornite dal centro di comando e controllo che gestisce la botnet stessa e provengono dai tanti database leak (per via dell'ancora diffusa pratica di utilizzare la stessa password per più servizi) oppure da attacchi di forza bruta (che scoprono password a bassa entropia o presenti in dizionari) oppure da campagne di phishing. Le mail malevole vengono quindi inviate prevalentemente da account di posta legittimi sempre diversi, riducendo il numero di segnali utili a classificarle come malevole.

A titolo di esempio la botnet "Necurs", che si stima sia composta da oltre un milione di dispositivi, è una delle principali responsabili delle massive campagne email di estorsione a cui abbiamo assistito in Italia nell'ultimo trimestre. In queste campagne la vittima viene indotta a credere di essere stata spiata durante la visione di filmati per adulti. Varianti di queste campagne si sono protratte per molte settimane, decisamente più a lungo del solito, e sono state diffuse in almeno otto lingue diverse (tra cui l'italiano). Tutto lascia intendere che si trattasse di un inganno particolarmente efficace e remunerativo.

Nel tempo abbiamo monitorato diverse "ondate" di questa truffa che implementavano tecniche variabili per cercare di superare i filtri antispam, come ad esempio l'utilizzo mirato di errori ortografici, l'adozione di frasi volutamente sgrammaticate o l'utilizzo di omoglifi e caratteri invisibili o zero-width-space, al fine di ingannare l'analisi semantica e il machine learning.

Per meglio comprendere l'entità di un fenomeno interessante dal punto di vista tecnico (una campagna interamente basata sull'ingegneria sociale che sembrava avere un particolare successo) i nostri ricercatori hanno seguito le transazioni verso alcuni wallet bitcoin pubblicati in queste mail. È pratica comune effettuare numerosi trasferimenti di wallet in wallet per far perdere le tracce dell'origine dei fondi, abbiamo seguito le numerose transazioni e dopo alcuni passaggi siamo approdati ad un wallet contenente 224 bitcoin, ovvero circa 1,4 milioni di dollari al cambio corrente. Sebbene non si possa affermare che questa cifra sia interamente attribuibile a questa campagna, è probabile che sia attribuibile allo stesso gruppo ed è una indicazione del giro d'affari legato all'uso malevolo della email.
Ulteriori dettagli sono stati pubblicati sul "security blog" di Libraesva.

I numeri del ricatto sessuale, Fonte: libraesva

Gli stessi dispositivi arruolati nelle botnet si occupano di eseguire con continuità ed in modo coordinato attacchi a forza bruta sulle credenziali di posta elettronica. In questo campo una vasta botnet coordinata da un unico centro di comando e controllo consente di eludere le difese tradizionali. L'esecuzione coordinata distribuisce i tentativi di accesso tra migliaia di dispositivi, lo stesso dispositivo tenta una sola volta di accedere ad una determinata casella e il tentativo successivo verrà fatto da un altro dispositivo con un diverso indirizzo IP. Questo vanifica l'efficacia dei sistemi di rilevamento degli abusi basati sul rate-limiting. Le credenziali di posta acquisite in questo modo si aggiungono a quelle provenienti da

attacchi di phishing e a quelle ricavate dai database leak, fornendo sempre nuovi indirizzi legittimi da utilizzare per l'invio delle successive campagne di malware e phishing.
Per il lettore resta valido il consiglio di non riutilizzare la stessa password su servizi diversi e di utilizzare password ad alta entropia non presenti in dizionari, il che significa rassegnarsi ad utilizzare un password manager.

Spam

Per quanto riguarda lo spam "puro", quello che pubblicizza prodotti più o meno miracolosi, le dinamiche sono per lo più legate alla nascita, alla crescita e all'evoluzione delle organizzazioni dedite allo spam. Queste organizzazioni utilizzano tipicamente intere classi di indirizzi IP (dai 256 in su) che affittano in blocco per poi abbandonarle dopo qualche settimana, quando ormai la reputazione di tali classi di indirizzi è compromessa. I domini utilizzati per l'invio sono numerosi e vengono variati molto frequentemente, con una logica "usa e getta". Queste mail rispettano tutti gli standard tecnici esistenti e le variazioni di domini e classi di IP puntano a vanificare i sistemi di protezioni basati sulla reputazione.

Efficacia ed evoluzione dei sistemi di protezione della posta

Da quanto detto sopra deduciamo come l'attività di classificazione e filtraggio della posta possa contare sempre meno su segnali di ordine tecnico avendo a che fare con email che dal punto di vista tecnico sono assolutamente corrette o che addirittura sono originate da account individuali legittimi.
Di anno in anno diventano sempre più importanti gli strumenti di analisi del contenuto, i quali ricadono parzialmente all'interno di categorie che sono diventate delle "buzzword" del marketing come "machine learning", "semantic analysis", "artifical intelligence", "data mining", eccetera.
Chi lavora nel settore utilizza questi strumenti (magari con nomi diversi) fin dagli anni '90, non si tratta quindi di reali novità ma di strumenti che hanno certamente visto una evoluzione in virtù della loro crescente importanza nel tempo. Altri strumenti, come quelli basati su approcci a "signature" o "pattern", storicamente caratteristici dei sistemi antivirus, continuano a perdere di efficacia.
I sistemi di filtraggio della posta si comportano in modo piuttosto uniforme finché la lingua dei messaggi è l'inglese, quando la campagna di spam/malware/phishing è in italiano l'efficacia dei sistemi di protezione mostra una maggiore variabilità legata al livello di attenzione che il vendor dedica al nostro paese.

Malware

Si conferma la crescita nel numero di varianti sempre diverse al fine di superare i controlli a "signature" e "pattern". Aumentano anche i malware capaci di evadere la rilevazione da parte dei sistemi di sandboxing basati su virtualizzazione.
Lo scorso anno parlavamo di un nuovo tipo di sandbox proattiva, in grado di rimuovere dai documenti il codice che abilita alla realizzazione di malware e dropper. L'efficacia di questo

approccio è confermata dal fatto che nel corso dell'intero anno non abbiamo registrato una singola infezione su sistemi protetti da questo tipo di sandbox degli allegati.

Sanitizzazione di codice nei documenti, Fonte: Libraesva

Si tratta di adottare un approccio "firewall" al codice contenuto nei documenti. Il codice che fa operazioni di accesso a internet e/o al filesystem e/o di esecuzione di comandi non viene lasciato passare anche se il file non viene riconosciuto come malevolo. Il sistema è in grado di rimuovere il codice dal documento consegnando un documento Office o PDF "inerte", senza più macro e quindi non più in grado di nuocere. Questo previene infezioni da varianti di malware ancora ignote.

Percentuale documenti bloccati, Fonte: Libraesva

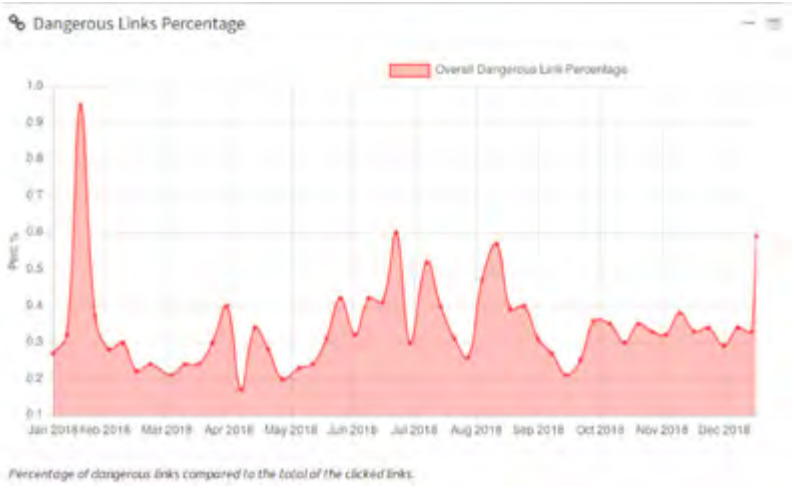
Restando in tema di allegati malevoli, il formato più utilizzato (47%) è il documento word binario (.doc), seguito (17%) dal documento excel binario (.xls). I formati binari dei documenti Office offrono una maggiore versatilità per gli autori del malware rendendo più facile nascondervi codice malevolo e per questo sono più usati, mentre i documenti malevoli di tipo .docx e .xlsx (formato openxml) sono ciascuno al 2,7%.
Gli allegati html malevoli sono il 3,6% mentre il pdf è poco sopra all'1%, questo formato è usato più per veicolare link a siti malevoli che per veicolare malware in se.
Per quanto riguarda gli archivi, quelli di tipo .iso sono malevoli nel 96% dei casi, gli .arj nell'89% dei casi, i .tar nel 78%, i .rar nel 63% seguono .ace (50%), .zip (17%), .gz (7%).
Ci sono poi alcuni allegati meno frequenti ma che risultano essere malevoli nella quasi totalità dei casi, le estensioni di questi file sono .vbe, .jse, .cmd, .reg, .cpl, .vbs, .exe, .jar, .scr, .lnk, .com, .iqy e i vari archivi winrar con esensione .rXX dove al posto di X abbiamo un numero.
Quali sono invece i file legittimi più inviati in allegato ad una mail? I pdf vincono con il 37% mentre i documenti word (qualunque formato) sono il 4,5%, stessa percentuale per i documenti excel.

Link malevoli

Circa il 10% delle mail contiene un link, il link malevolo resta un efficace sistema di attacco, in crescita rispetto all'anno precedente. Rispetto all'invio del malware in allegato offre maggiori possibilità di evasione dei sistemi di email security, soprattutto quando la mail è inviata da un account legittimo (abusato) e il link punta ad un sito legittimo che è appena stato compromesso.

Geolocalizzazione del malware sul web, Fonte: Libraesva

Per i sistemi di email security può essere difficile classificare come malevola una mail di questo tipo per la mancanza di "segnali" di ordine tecnico, questo è il motivo per cui è ormai indispensabile un sistema di URL sandboxing in grado di analizzare il contenuto del link visitandolo prima dell'utente. Questa analisi deve essere necessariamente fatta quando l'utente clicca sul link e per farlo il link viene riscritto puntando ad un servizio di analisi che si occuperà di analizzare la pagina finale e impedire all'utente di visitarla se malevola.



Percentuale link malevoli nel 2018, Fonte: Libraesva

Sul nostro campione di 10 miliardi di email sono circa 30 milioni i link malevoli che sono stati bloccati dal servizio di URL sandboxing. Dal punto di vista percentuale è solo lo 0,3% ma si tratta di link malevoli contenuti in email che, per i motivi appena illustrati, riescono a superare i sistemi di sicurezza e raggiungono la inbox dell'utente. Senza questa ulteriore linea di difesa rappresentata dal sandboxing delle URL ci sarebbero stati 30 milioni di click su link malevoli che non sarebbero stati intercettati. Ognuno di questi click è potenzialmente una infezione della propria organizzazione.

Phishing

Il phishing è una delle fonti di credenziali fresche da utilizzare per l'invio di nuove campagne malevole.
Rileviamo regolari tentativi di phishing nei confronti di organizzazioni universitarie con portali ingannevoli costruiti ad hoc.

Phishing credenziali mirato all'Università di Milano, Fonte: Libraesva

Tra i numerosi toolkit di phishing che consentono di realizzare velocemente delle pagine di raccolta delle credenziali ci sono quelli che emulano un portale di webmail dell'organizzazione a cui viene inviata la mail malevola.

Phishing webmail confindustria, Fonte: Libraesva

La pagina che richiede le credenziali cerca di apparire come un portale di webmail dell'organizzazione mostrando in modo dinamico nel titolo il nome del dominio dell'indirizzo email della vittima.

Phishing webmail Prada, Fonte: Libraesva

Lo strumento di sandboxing dei link, analizzando la pagina, individua i toolkit utilizzati per la realizzazione della pagina di phishing e blocca la navigazione dell'utente avvertendolo del pericolo.

Attacchi mirati alle organizzazioni

Sono in decisa crescita, confermando la tendenza registrata lo scorso anno, gli attacchi mirati. I cosiddetti attacchi di "Business Email Compromise" (BEC) detti anche "Whaling" sono rappresentati principalmente dal tentativo di impersonare un dirigente C-level tentando di indurre persone interne all'organizzazione a fare bonifici ai truffatori o fornire informazioni confidenziali.


Da: Francesca <ceo.phonen@gmail.com>
A: paola
Oggetto: Pagamento!
Data: Wed, 10 Oct 2018 10:54:29 +0100 (10/10/2018 11:54:29)

Ciao Paola,

Sei qui? Ho bisogno che tu faccia un pagamento SEPA o un bonifico internazionale. quando puoi farlo?

Cordiali saluti,

Francesca

Tentativo di attacco BEC, Fonte: Libraesva

Da questo punto di vista si registrano due distinte tendenze.
La prima è una sorta di "serializzazione" di questi attacchi che passano dal puntare ad una specifica vittima con un messaggio costruito su misura (l'approccio tradizionale) al mirare contemporaneamente a più destinatari all'interno dell'organizzazione con messaggi tutti uguali e meno sofisticati.
La seconda tendenza va in direzione opposta, ovvero una maggiore specializzazione degli attacchi mirati. In un caso abbiamo monitorato un tentativo di truffa in cui l'attaccante si era trasformato in un man-in-the-middle nelle comunicazioni email tra una importante S.p.A. italiana e un suo fornitore straniero. L'attacco è stato fatto acquisendo due domini di posta elettronica visivamente simili a quelli delle due aziende. Utilizzando questi domini l'attaccante si spacciava per il fornitore nei confronti della SPA e impersonava la SPA nei confronti del fornitore. Dopo una prima email inviata ad entrambi per "avviare" la conversazione, l'attaccante non faceva altro che girare all'uno la mail ricevuta dall'altro modificando i codici IBAN dei documenti allegati.

Al di là dei casi più sofisticati come quello di questo esempio, gli attacchi BEC sono in aumento e riguardano ormai aziende di ogni dimensione, non solo le più grandi. La "serializzazione" di questi attacchi consente di contenere l'effort dell'attaccante e portare l'attacco verso un numero di aziende maggiore di dimensioni sempre minori.
Gli engine specifici contro gli attacchi BEC riducono significativamente la probabilità di incorrere in questo tipo di inganno.

Conclusioni

Per i sistemi di email security è sempre più importante l'analisi di contenuto in quanto le mail malevole sono sempre più indistinguibili da quelle legittime nelle modalità di trasporto e consegna. Questo porta ad una crescente differenziazione dell'efficacia dei sistemi di sicurezza, in particolare nei paesi non anglofoni.

I sistemi di sandboxing dei file basati sul disarmo del codice sospetto contenuto nei documenti hanno provato sul campo la loro efficacia e sono molto meno vulnerabili a tecniche di evasione rispetto ai tradizionali sistemi di sandboxing basati su virtualizzazione.

Il sandboxing delle URL è diventato uno strumento pressoché indispensabile come ultima linea di difesa nei confronti di email contenenti link malevoli non intercettate dai sistemi di protezione.

Quello degli attacchi mirati, fenomeno emergente nel 2017, si conferma in crescita nel 2018 ed è prevedibile una diffusione sempre più capillare nel 2019. Si tratta di attacchi a bassa frequenza ma ad alto impatto potenziale e per questo ogni strumento atto a ridurre la superficie d'attacco è auspicabile, dagli engine specifici contro il BEC alla revisione delle procedure aziendali (ad esempio prevedendo un canale di conferma aggiuntivo per autorizzare le transazioni).

Attività e segnalazioni della Polizia Postale e delle Comunicazioni nel 2018

In uno scenario nel quale la continua evoluzione tecnologica influenza ogni azione del nostro vivere quotidiano, lo sforzo della Polizia Postale e delle Comunicazioni nell'anno 2018 è stato costantemente indirizzato alla prevenzione e al contrasto della criminalità informatica in generale, con particolare riferimento ai reati di precipua competenza di questa Specialità.

CNCPO- Centro Nazionale per il Contrasto alla Pedopornografia Online

Nell'ambito della **pedopornografia online,** nell'anno in corso, sono stati eseguiti **43** arresti e denunciate **547** persone; tra le operazioni più significative, coordinate dal Centro Nazionale per il Contrasto alla pedopornografia Online del Servizio Polizia Postale e delle Comunicazioni, si segnala l'operazione "Ontario" che ha consentito l'esecuzione di **22** perquisizioni, **4** persone tratte in arresto e **18** persone denunciate in stato di libertà; nell'ambito dell'operazione "Safe Friend" sono state eseguite **15** perquisizioni che hanno consentito di arrestare **3** persone e denunciarne **12.**

Le indagini svolte anche in modalità sotto copertura nell'Operazione "Good Fellas" hanno consentito di eseguire **14** perquisizioni, portando all'arresto di **4** persone, nonché di denunciare in stato di libertà altri **12** indagati. L'Operazione denominata "*Showcase*" si è conclusa con l'esecuzione di **12** perquisizioni, la denuncia di **11** persone e l'arresto di un altro indagato.

Dalle complesse attività di prevenzione, è scaturita una assidua attività di monitoraggio della rete che ha visto coinvolti ben **33086** siti internet, di cui **2182** inseriti in black list.

Le indagini relative al fenomeno dell'adescamento di minori online hanno portato all'arresto di **3** persone e alla denuncia di **139** indagati.

Fondamentale importanza assume la collaborazione con organismi internazionali dalla quale prendono avvio importanti e complesse attività investigative nei vari scenari della Rete.

Il Centro rivolge massima attenzione al contrasto di fenomeni emergenti che scaturiscono da fragilità psico-emotiva dei minori tra i quali emergono episodi di istigazione all'autolesionismo e al suicidio, strutturati anche in modalità di sfida o di gioco. In particolare, dal 2017, il Centro ha avviato un'attività di monitoraggio della rete finalizzata a contrastare il fenomeno noto come "Blue Whale", attività rivolta a individuare le vittime e i "curatori" e che ha fatto registrare circa **700** segnalazioni, delle quali **270** confluite in comunicazioni di notizie di reato alle Procure.

L'aumento del numero degli adolescenti presenti sul web ha determinato una crescita costante del numero di minorenni vittime di reati commessi dagli stessi minori autori di reato: dai 236 casi registrati nel 2016 si è passati a 325 nel 2017 e 346 casi trattati nel 2018.

Sezione Operativa

Nell'ambito dei reati contro la persona perpetrati sul web, il **ricatto on line** è un fenomeno in continua crescita con **948** casi trattati dall'inizio dell'anno, atteso che il dato emerso è parziale e fortemente ridotto rispetto alla reale entità del fenomeno. Sono 20 le persone denunciate e 2 le persone arrestate in Italia nel 2018. Anche grazie a una complessa attività di collaborazione internazionale ed in particolare con la Gendarmerie Royale del Marocco, tramite gli organi di coordinamento istituzionali, sono stati arrestati da quella Forza di Polizia 23 cittadini marocchini destinatari delle transazioni finanziarie provento di estorsioni a sfondo sessuale. Dal mese di gennaio ad oggi, sono state denunciate **955** persone e **8** persone sono state tratte in arresto, per aver commesso estorsioni a sfondo sessuale, stalking, molestie sui social network, minacce e trattamento illecito di dati personali. Tra i reati contro la persona, in costante aumento sono le **diffamazioni on line,** soprattutto ai danni di persone che ricoprono incarichi istituzionali o che sono note. In questo ambito, nel 2018, sono state denunciate **697** persone. Si registra inoltre una continua evoluzione nella tipologia dei reati commessi. L'ultima modalità della violenza sulle donne è il fenomeno dei c.d. stupri virtuali: all'interno di gruppi chiusi i partecipanti di sesso maschile condividono foto, ricercate sui social o copiate da contatti whatsapp, di donne ignare, ritratte nella loro vita quotidiana, dando poi sfogo a fantasie violente e comportamenti offensivi.

Di rilievo è l'attività condotta dal Servizio Polizia Postale e delle Comunicazioni nel contrasto ai reati d'incitamento all'odio, svolgendo il prezioso ruolo di punto di contatto nazionale per il **contrasto all'hate speech on line**. Sono oltre **5000** gli spazi virtuali monitorati nel 2018 per condotte discriminatorie di genere, antisemite, xenofobe e di estrema destra.
Le **truffe on line** sono in continua crescita: nel 2018 la Specialità ha denunciato **3383** persone, ne ha arrestato **43**, ha sequestrato **22.687** spazi virtuali, ha ricevuto e trattato circa **160.000** segnalazioni di truffe o tentate truffe. Significativa l'attività svolta sulle cosiddette frodi delle assicurazioni. Questa tipologia di truffa viene commessa attraverso la commercializzazione di polizze assicurative mediante la creazione di portali, in taluni casi con riproduzioni di pagine web di compagnie note, sulle quali sono promosse polizze assicurative temporanee false, esercitando in tal modo l'attività di intermediazione assicurativa in difetto di iscrizione al registro degli intermediari assicurativi.

CNAIPIC

Di evidente incremento è l'attività di contrasto alla minaccia cyber svolta dal Centro Nazionale Anticrimine per la Protezione delle Infrastrutture Critiche (C.N.A.I.P.I.C.), attestata dal rilevante aumento del numero di alert diramati alle infrastrutture critiche nazionali che, rispetto al 2017, si è quasi raddoppiato sino a raggiungere **60777**.
La tempestiva condivisione dei c.d. "indicatori di compromissione" dei sistemi informatici con i fornitori di servizi pubblici essenziali ha consentito di rafforzare gli strumenti volti alla protezione della sicurezza informatica, garantita anche da una costante attività di monitoraggio.

In tale ambito, il Centro ha ulteriormente gestito monitoraggi della rete che hanno riguardato strutture sensibili di rilievo nazionale.
Inoltre in particolare la Sala Operativa del Centro ha gestito:

- **459** attacchi informatici nei confronti di servizi internet relativi a siti istituzionali e infrastrutture critiche informatizzate di interesse nazionale;
- **108** richieste di cooperazione nell'ambito del circuito "High Tech Crime Emergency".

Tra le attività investigative condotte, in tale ambito, si segnalano **74** indagini avviate nel **2018** per un totale di **14** persone denunciate e l'arresto di **1.**
Tra le attività più significative si segnala un'operazione, frutto di una proficua attività di collaborazione internazionale intrapresa con la polizia olandese, che ha ricevuto il supporto di Europol per il tramite dell'European Cyber Crime Centre della Joint Cybercrime Action Taskforce. Il Centro**,** con l'ausilio della Sezione Polizia Postale di Cosenza ed il supporto logistico della Stazione dei Carabinieri di San Giorgio Albanese (CS) ha eseguito una perquisizione locale e personale nei confronti di un ventottenne italiano residente nella provincia di Cosenza resosi responsabile del reato di "intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche" (Art. 617 quater C.P.).
Nel corso della perquisizione sono stati sequestrati computer e supporti informatici utilizzati per portare a compimento l'attività illecita**.**
Nell'ottica di un'efficace condivisione operativa, il Centro ha proseguito la stipula di specifici Protocolli a tutela delle infrastrutture critiche nazionali: al riguardo, nel 2018 sono state sottoscritte 8 nuove convenzioni con le società WindTre, Sky Italia, Fincantieri, MM S.p.A., Monte dei Paschi di Siena, Consip S.p.A., Nexi S.p.A. e BT Italia, oltre al rinnovo delle convenzioni in essere con Sogei, ATM, ENI, RAI, ENAV e TERNA.
Si rappresenta, altresì, che analoghe forme di collaborazione sono state avviate dagli uffici territoriali della Specialità con strutture sensibili di rilevanza locale, sia pubbliche che private, al fine di garantire un sistema di sicurezza informatica capillare e coordinato.

Con riferimento al **financial cybercrime,** le sempre più evolute tecniche di *hackeraggio,* attraverso l'utilizzo di *malware* inoculati mediante tecniche di phishing, ampliano a dismisura i soggetti attaccati, soprattutto nell'ambito dei rapporti commerciali. Infatti lo scopo delle organizzazioni criminali è quello di intromettersi nei rapporti commerciali tra aziende dirottando le somme verso conti correnti nella disponibilità dei malviventi. Il BEC (business e-mail compromise) fraud o CEO (Chief Exeutive Officer) fraud sono la moderna applicazione della tecnica di attacco denominata "man in the middle".
Nonostante la difficoltà operativa di bloccare e recuperare le somme frodate, soprattutto perché inviate verso paesi extraeuropei (Cina, Taiwan, Hong Kong), grazie alla versatilità della piattaforma **OF2CEN** (On line Fraud Cyber Centre and Expert Network) per l'analisi e il contrasto avanzato delle frodi del settore, nell'anno 2018, la Specialità ha potuto bloccare e recuperare alla fonte su una movimentazione in frode di **38.400.000,00 €** ha potuto già recuperare e restituire circa **9.000.000,00 €** mentre sono in corso attività di

cooperazione internazionale finalizzate al recupero delle restanti somme. La piattaforma in questione frutto di specifiche convenzioni intercorse mediante ABI con gran parte del mondo bancario, consente di intervenire in tempo quasi reale sulla segnalazione bloccando la somma prima che venga polverizzata in vari rivoli di prestanome.

Al riguardo, di rilievo è la recente operazione internazionale denominata "Emma4", coordinata dal Servizio Polizia Postale con la collaborazione di **30 Paesi** Europei e di Europol, volta a identificare i c.d. "money mules", primi destinatari delle somme provenienti da frodi informatiche e campagne di phishing, che offrono la propria identità per l'apertura di conti correnti e/o carte di credito sui quali vengono poi accreditate le somme illecitamente acquisite.
L'operazione in parola ha consentito sul territorio nazionale di identificare **101** money mules di cui **50 arrestati e 13 denunciati.**
Le transazioni fraudolente sono state **320**, per un totale di circa **34 milioni di euro,** di cui **circa 20 milioni euro** sono stati bloccati e/o recuperati grazie alla piattaforma per la condivisione delle informazioni denominata "OF2CEN", realizzata appositamente al fine di prevenire e contrastare le aggressioni criminali ai servizi di home banking e monetica.

Sezione Cyber Terrorismo

La recente direttiva del Sig. Ministro dell'Interno sui comparti di specialità ha confermato in capo alla Polizia Postale e delle Comunicazioni, sia a livello centrale che territoriale, le competenze in materia di contrasto al fenomeno del terrorismo di matrice jihadista in rete, con particolare riferimento al monitoraggio del web, quale principale strumento di strategia mediatica del Daesh, già espletato da personale della Polizia Postale e delle Comunicazioni, affiancato da un qualificato, supporto di mediazione linguistica e culturale.
Tale rinnovato, rafforzato, impegno della Polizia Postale e delle Comunicazioni in tale ambito ha reso necessario implementare le attività in argomento, ampliando il coinvolgimento di un maggior numero di Compartimenti nel summenzionato monitoraggio, nonché un potenziamento del numero dei mediatori linguistici e culturali, il cui prezioso apporto, per la peculiarità della materia e dei relativi contenuti multimediali presenti nella rete, risulta assolutamente indispensabile.

Nell'ambito della prevenzione e contrasto al terrorismo internazionale di matrice jihadista e, in particolare, ai fenomeni di radicalizzazione, la Polizia Postale e delle Comunicazioni ha svolto attività sia di iniziativa, che su specifica segnalazione, al fine di individuare i contenuti di eventuale rilevanza penale all'interno degli spazi e servizi di comunicazione on line, siti o spazi web, weblog, forum, portali di social network e i cosiddetti "gruppi chiusi", anche a seguito di informazioni pervenute dai cittadini tramite il Commissariato di P.S. Online.
L'attività, funzionale a contrastare il proselitismo e prevenire fenomeni di radicalizzazione, ha portato a monitorare circa **36.000** spazi web e alla rimozione di diversi contenuti (**250**).
Nel corso di tale attività di monitoraggio, si è inoltre riscontrato un effettivo incremento

dell'azione da parte dei maggiori fornitori di servizi Internet (*Facebook, Google, Twitter, etc.*) volta alla rimozione di contenuti illeciti presenti sulle proprie piattaforme, grazie anche alla richiesta di maggiore collaborazione elaborata in numerose sedi istituzionali nell'ambito di progetti internazionali (es. *EU Internet Forum*), ai quali ha preso parte anche la Specialità.
A seguito di tale strategia, si è rilevato un repentino passaggio dei fenomeni di diffusione e divulgazione dei contenuti riconducibili al radicalismo islamico su piattaforme di comunicazione *social* ritenute più sicure (*Telegram, WhatsApp*), in quanto garantiscono maggiore riservatezza. Inoltre, fornendo ai propri utenti un grado di anonimato più elevato, come da *policies* aziendali, di fatto finiscono per attrarre la quasi totalità delle attività di diffusione di contenuti illeciti o comunque di propaganda poste in essere da soggetti contigui ad ambienti filo-jihadisti e agli stessi membri delle organizzazioni terroristiche.
Nell'ultimo anno, in concomitanza con le recenti perdite territoriali da parte del c.d. Stato Islamico, si è riscontrato un significativo decremento dell'attività mediatica del Daesh, in particolare per quanto concerne la diffusione di nuovi contenuti di proselitismo nel web, sia in termini quantitativi, che qualitativi. Infatti, si è notato che i pochi filmati e le info-grafiche emanati hanno standard qualitativi palesemente inferiori a quelli precedenti, segno, verosimilmente, che il Califfato è in fase di riorganizzazione/trasformazione e sta ristrutturando il suo network interno e ridelineando la propria strategia. In particolare, si sta passando da forme di comunicazione di massa, ben strutturate, alla diffusione di materiale autoprodotto attraverso l'utilizzo di mezzi più semplici, quali smartphones, ma che comunque trovano diffusione attraverso canali sommersi e forme di comunicazione compartimentate.

L'attività preventiva e informativa della Polizia Postale e delle Comunicazioni ha visto, inoltre, momenti di collaborazione con la Direzione Centrale della Polizia di Prevenzione e le locali Digos, anche per il supporto in caso di necessari approfondimenti tecnici in relazione a posizioni emergenti o monitorate sul territorio nazionale.
Infatti, la Polizia Postale e delle Comunicazioni concorre con altri organi di Polizia e di *intelligence* alla prevenzione e al contrasto dei fenomeni di proselitismo on line e di radicalizzazione, sia a livello nazionale che internazionale, posti in essere attraverso l'utilizzo di strumenti informatici e di comunicazione telematica. La sinergia tra i diversi comparti in tale ambito è divenuta sempre più incisiva, sia nell'ambito del raccordo info-investigativo che di quello tecnico-operativo.

Per quanto concerne, invece, l'attività di contrasto, la Polizia Postale e delle Comunicazioni si avvale di profili sotto copertura creati *ad hoc* e gestiti dagli operatori, con l'affiancamento dei mediatori linguistici e culturali.
L'utilizzo di uno di tali account fittizi, nel tempo fatto "maturare" dagli investigatori nel corso delle diverse, quotidiane, attività di monitoraggio informativo e, dunque, accreditato all'interno dei canali e gruppi frequentati dagli internauti sostenitori dello Stato Islamico, ha permesso di condurre diverse, complesse, attività tecnico-investigative.
A titolo esemplificativo, si evidenziano, in particolare, tre significativi risultati investigativi.

Il primo ha condotto all'arresto dei componenti di una cellula terroristica che, su Facebook, svolgeva attività di propaganda jihadista e di reclutamento.
Sulla base degli esiti investigativi, il Tribunale di Perugia ha emesso 4 ordinanze di custodia cautelare in carcere e 3 perquisizioni a carico di altrettanti indagati, nei cui confronti il Ministro dell'Interno ha disposto l'espulsione dal territorio nazionale per motivi di sicurezza dello Stato.
Uno dei tre espulsi, è stato successivamente tratto in arresto in Tunisia, per i suoi legami con la jihad.

Nell'ambito del monitoraggio informativo della rete svolto da personale della Polizia Postale e delle Comunicazioni, sono stati individuati diversi utenti Facebook ritenuti meritevoli di approfondimenti investigativi e nei cui confronti è stata svolta una mirata attività sotto copertura, che ha consentito, unitamente a servizi di intercettazioni telematiche, telefoniche e di osservazione, controllo e pedinamento al fine della loro puntuale identificazione, nonché di delineare le diverse responsabilità ascrivibili ai singoli componenti della cellula, i quali, tutti di nazionalità marocchina e tunisina, gravitavano tra Perugia, Milano e la Germania.
Uno di questi, in particolare, ha assunto, nel tempo, la qualità di indottrinatore e formatore della cellula in argomento, con una attività costante nel fornire notizie e commenti sullo Stato Islamico ai propri sodali, tesi ad esaltarne le vittorie militari e i traguardi civili raggiunti, dando anche indicazioni sul modo corretto di comportarsi di un buon musulmano, arrivando a inneggiare al martirio in nome di Allah e all'annientamento dei miscredenti cristiani e degli apostati sciiti. Non è stato semplice identificarlo, in quanto lo stesso utilizzava diversi profili contemporaneamente, collegandosi a reti wireless "aperte" che ne assicurassero l'anonimato.
Gli altri appartenenti alla cellula sono risultati, sebbene con ruoli diversi, strettamente legati al predetto, con il quale hanno condiviso l'adesione alla jihad tramite frequenti contatti sul web e con assidue frequentazioni reali.
Il secondo risultato investigativo ha portato all'individuazione di un minore italiano di origine algerina, il quale, attraverso la rete, svolgeva un'intensa campagna di proselitismo di matrice jihadista su Telegram, istigando altri utenti a commettere delitti di terrorismo, fatti aggravati in quanto le azioni venivano compiute attraverso strumenti informatici e telematici. All'interno del canale Telegram, frequentato da circa 200 utenti e considerato tra i principali veicoli della narrativa dell'IS, venivano pubblicati messaggi testuali, immagini, video, infografiche e audio di propaganda del Daesh, tradotti in lingua italiana e rivolti in particolare ai c.d. "lupi solitari" presenti sul territorio nazionale.
Considerata l'impossibilità di acquisire elementi investigativi utili all'identificazione dell'amministratore del canale attraverso vie ufficiali dirette, il Servizio Polizia Postale ha attivato una mirata attività tecnico-investigativa che ha permesso di orientare le indagini finalizzate a individuarne l'amministratore, la cui identificazione è risultata complicata, in quanto il minore si è dimostrato particolarmente abile e competente a livello informatico, poiché utilizzava tecniche di anonimizzazione evolute (connessioni attraverso servizi di VPN e nodi TOR).

È stato possibile raggiungere il risultato sperato soltanto a seguito di una difficile e articolata attività tecnica svolta da personale del Servizio Polizia Postale anche attraverso l'utilizzo di software sviluppati ad hoc e rivelatisi di particolare efficacia.
Le successive attività d'indagine, svolte attraverso l'attivazione di servizi di intercettazione delle comunicazioni telematiche, telefoniche e ambientali, nonché riscontrate da servizi di diretta osservazione, hanno consentito di acquisire concreti elementi di prova a carico di un cittadino italiano minorenne di "seconda generazione", nato in Italia da genitori di origine algerina, che è stato indagato per aver compiuto attività di proselitismo a favore dell'IS mediante diffusione e traduzione di contenuti di propaganda on line.
Nonostante la giovane età, il minore risultava in possesso di elevate capacità tecnico-informatiche, padronanza linguistica non comune e approfondita conoscenza dei principali testi sacri dell'Islam, proponendosi quale punto di riferimento per tutti coloro che intendevano contribuire attivamente alla causa jihadista.
L'attività investigativa ha consentito di riscontrare e raccogliere elementi in ordine al percorso di autoradicalizzazione del minore, intrapreso esclusivamente in rete e sfociato in una successiva diffusione on line del proselitismo di matrice jihadista.
Infatti, nella vita reale il ragazzo non frequentava la moschea, né ambienti contigui all'estremismo islamico. Anche il contesto familiare, sebbene musulmano, risultava di impostazione musulmana, ma non integralista.
Oltre ai risultati operativi conseguiti, tale indagine ha presentato anche profili di rilevanza giudiziaria e sociale, in quanto è stata riconosciuta la pericolosità reale delle iniziative adottate dell'indagato, le quali, lungi da esaurire i propri effetti nella "dimensione virtuale", sono risultate concretamente rilevanti.
Il puntuale intervento della Procura dei minori e della Polizia di Stato ha consentito di superare la mera fase accertativa della responsabilità penale del minore, avviando un dedicato percorso di recupero e deradicalizzazione, reso possibile dallo "scollegamento" del giovane dalla rete della c.d. *"cyber jihad"*.
Come noto, infatti, ormai il web assurge a un ruolo fondamentale quale strumento strategico di propaganda dell'ideologia del Daesh, di reclutamento di nuovi combattenti, di finanziamento, di scambio di comunicazioni riservate nella pianificazione degli attentati e di rivendicazione degli stessi.

Infine, il terzo, recente risultato investigativo è consistito nell'arresto di un cittadino egiziano di 22 anni, irregolare sul territorio nazionale, per associazione con finalità di terrorismo internazionale e istigazione e apologia per delitti di terrorismo.
Le indagini, avviate nel 2017 con intercettazioni telefoniche, ambientali, telematiche e specifici servizi di osservazione e pedinamento h24.
Il giovane arrestato è un appartenente all'ISIS, indottrinatosi con il materiale di propaganda di DAESH reperito on line. Gli elementi raccolti hanno evidenziato che il predetto ascoltava in continuazione, in una sorta di "***brain washing***", files audio di Imam radicali e della rivista "Dabiq" inneggianti all'odio per l'occidente, alla jihad e a sostegno degli atti di martirio.

Dalle intercettazioni telematiche e accertamenti tecnici svolti dalla Polizia Postale e delle Comunicazioni, è emerso che il giovane è altresì organico anche alla macchina della propaganda del sedicente stato islamico.
Infatti, gestiva gruppi e canali chiusi su Telegram, nei quali venivano diffuse le notizie delle attività dello Stato Islamico, tramite le agenzie mediatiche del Califfato.
In particolare, era in assiduo contatto con due connazionali, anch'essi radicalizzati, con i quali scambiava video e audio Jihadisti e inneggianti l'Islam radicale.
Nei loro confronti il Ministro dell'Interno ha emesso il decreto di espulsione dal territorio italiano.
Trattandosi di un fenomeno a carattere transnazionale, sia per la natura internazionale del fenomeno, che per la stessa connaturata struttura della rete, risulta imprescindibile l'attivazione efficiente degli strumenti della cooperazione sovranazionale, sia ordinari che "nuovi", soprattutto per la condivisione di informazioni che, collegate a situazioni peculiari interne, riescono ad apportare indiscusso valore aggiunto alle attività di prevenzione messe in atto dalle diverse forze di polizia nazionali.
In ambito europeo, il Servizio Polizia Postale e delle Comunicazioni è il punto di contatto nazionale dell'Internet Referral Unit (IRU) di Europol, Unità preposta a ricevere dai Paesi Membri le segnalazioni relative ai contenuti di propaganda jihadista diffusi in rete e di orientarne l'attività. Lo scambio delle informazioni tra Paesi Membri viene effettuato attraverso l'utilizzo di specifiche piattaforme tecnologiche, tra cui *Check-the-Web* (CTW) e *SIRIUS*, appositamente create in ambito IRU a supporto del monitoraggio e delle indagini nell'ambito di terrorismo in Internet.

Parallelamente all'incremento dell'uso di strumenti telematici, sono cresciute le aspettative di sicurezza da parte del cittadino.

La Polizia Postale e delle Comunicazioni è impegnata, ormai da diversi anni, in campagne di sensibilizzazione e prevenzione sui rischi e pericoli connessi all'utilizzo della rete internet, rivolte soprattutto alle giovani generazioni.

Nello specifico si evidenzia la campagna itinerante della Polizia Postale e delle Comunicazioni "Una Vita da Social", grazie alla quale sino ad oggi sono stati incontrati oltre **1 milione e 700 mila studenti**, **180.000 genitori, 100.000 insegnanti** per un totale di **15.000 Istituti scolastici** e **250** città italiane.
Un progetto dinamico, innovativo e decisamente al passo con i tempi, che si avvicina alle nuove generazioni evidenziando sia le opportunità del web che i rischi di cadere nelle tante trappole dei predatori della rete, confezionando un vero e proprio "manuale d'uso", finalizzato ad evitare il dilagante fenomeno del cyberbullismo e tutte quelle forme di uso distorto della rete in generale e dei social network.
A disposizione degli utenti è presente la pagina **facebook e twitter** di "Una vita da social", gestita direttamente dalla Polizia Postale e delle Comunicazioni, dove vengono pubblicati

gli appuntamenti, le attività, i contributi e dove i giovani internauti possono "*postare*" direttamente le loro impressioni ad ogni appuntamento.

Grande consenso ha riscosso la campagna **#cuoriconnessi**, che ha coinvolto 30.000 studenti, attraverso la proiezione di un docufilm e le testimonianze dirette dei minori vittime di prevaricazioni, vessazioni e violenze online.

Inoltre nel corso dell'anno sono stati realizzati incontri educativi su tutto il territorio nazionale raggiungendo oltre **300 mila studenti** e circa **3000 Istituti scolastici** per i quali è stata messa a disposizione anche un'email dedicata: progettoscuola.poliziapostale@interno.it.

Il portale del Commissariato di P.S. online è divenuto il punto di riferimento specializzato per chi cerca informazioni, consigli, suggerimenti di carattere generale, o vuole scaricare modulistica e presentare denunce.
Uno strumento agevole che consente al cittadino, da casa, dal posto di lavoro o da qualsiasi luogo si desideri, di entrare nel portale ed usufruire dei medesimi servizi di segnalazione, informazione e collaborazione che la Polizia Postale e delle Comunicazioni quotidianamente ed ininterrottamente offre agli utenti del web.

Di particolare importanza le denunce e le segnalazioni giunte anche sul sito del Commissariato di P.S. on-line per i reati di cyberbullismo, perpetrati soprattutto in ambito scolastico da parte di studenti nei confronti di compagni e perpetrati attraverso i social media, con atti denigratori e diffamatori nei confronti delle giovani vittime. Alcune attività sono sfociate nell'emissione da parte dei Questori di provvedimenti di ammonimento anche al fine di responsabilizzare minori autori del reato.

Attività del Commissariato di PS online

Richieste di informazioni evase	**20.432**
Segnalazioni ricevute dai cittadini	**20.047**
Denunce presentate dagli utenti	**11.245**

Il Nucleo Speciale Tutela Privacy e Frodi Tecnologiche della Guardia di Finanza

Il Nucleo Speciale Tutela Privacy e Frodi Tecnologiche è il reparto della Guardia di Finanza che garantisce un costante presidio di polizia economico-finanziaria in Rete. Il Nucleo, con sede in Roma, anche in ragione dell'extra-territorialità del web, ha competenza sull'intero territorio nazionale. L'attuale configurazione, cui si è giunti a seguito di una serie di revisioni ordinative dei Reparti Speciali della Guardia di Finanza operate dall'Organo di vertice del Corpo, ha visto, recentemente, assorbire sia il personale sia le competenze attribuite al soppresso Nucleo Speciale Privacy.

Il Comando Generale del Corpo, sin dal 2001, aveva avvertito l'esigenza di istituire un reparto che quotidianamente fosse impegnato in prima fila in un contesto operativo in esponenziale sviluppo tecnologico, dove gli interessi delle organizzazioni criminali avevano individuato un florido ambiente per perseguire i propri obiettivi in danno del settore economico-finanziario. Nel tempo, la consapevolezza di un maggiore impegno nel crescente settore degli illeciti di natura economico-finanziaria perpetrati in Rete ha portato, nel corso del 2004 all'elevazione dell'allora Gruppo Anticrimine Tecnologico a Nucleo Speciale Anticrimine Tecnologico. Nel corso del 2012 il Nucleo assumeva la denominazione di Nucleo Speciale Frodi Tecnologiche e, al fine di rendere maggiormente incisiva l'azione preventiva e repressiva del reparto, ne veniva, contestualmente, potenziata la struttura ordinativa, prevedendo la creazione al suo interno di quattro Gruppi operativi che sviluppano attività di polizia giudiziaria nel cyber-crime, nel dark-web ed effettua un monitoraggio costante della Rete finalizzato all'individuazione di fenomeni di riciclaggio e di finanziamento al terrorismo internazionale. Viene, altresì, attenzionato il settore delle criptovalute, che, atteso l'elevato grado di anonimità garantito dal loro utilizzo, sono spesso impiegate per effettuare transazioni a carattere illecito.

Il Nucleo Speciale Tutela Privacy e Frodi Tecnologiche oltre a costituire un'eccellenza nell'ambito dei Reparti Speciali con specifico riferimento al contrasto degli illeciti economico-finanziari sulla Rete, garantisce un'attività di ausilio agli altri reparti del Corpo in tutti quei settori d'interesse istituzionale nei quali le violazioni sono commesse ricorrendo ad Internet ovvero alle cosiddette "nuove tecnologie". In tale ambito, il Nucleo è Polo Tecnologico per tutta la Guardia di Finanza ed è incaricato di assumere un ruolo di centralità nella gestione delle tecnologie e nello sviluppo di sistemi informatici di ausilio alle indagini di polizia, nell'appoggio specifico alle unità territoriali nel settore del "Computer Forensics and Data Analysis", nonché nell'interscambio di esperienze con Enti istituzionali esterni, al fine di avviare specifiche iniziative di collaborazione che consentano di migliorare le professionalità e l'aggiornamento del personale impiegato in tali specifici ambiti di servizio. Il Nucleo Speciale ha, nella circostanza, stipulato appositi protocolli d'intesa con il Garante della Privacy per le attività ispettive in materia di sicurezza informatica e protezione dei dati

personali, con la Federazione Italiana Tabaccai per l'individuazione in Rete di reati di contrabbando di tabacchi e con l'Agenzia per l'Italia Digitale per l'attività di controllo in materia di sicurezza dei pagamenti elettronici della Pubblica Amministrazione.

Nel corso del 2018, tra le diverse attività di servizio condotte dal Nucleo, ha assunto particolare rilievo l'operazione "Darknet Money". Le indagini sono scaturite dall'analisi di diversi portali, raggiungibili esclusivamente tramite rete Tor, dediti alla vendita di merce illegale e sui quali risultavano attivi soggetti potenzialmente italiani. Dall'analisi del forum Italian Darknet Community (IDC) è stato individuato, tra gli altri, il venditore contraddistinto dallo pseudonimo Benz99, dedito al commercio di banconote false, oro contraffatto, documenti falsi, SIM telefoniche e carte Postepay Evolution intestate a terzi. Per essere contattato tramite messaggi a contenuto cifrato, il venditore ha condiviso alcune informazioni personali. Analizzando questi elementi, è stato possibile risalire a un indirizzo di posta elettronica in uso al venditore, al quale è stato successivamente abbinato anche un profilo social.

Dall'analisi dei log di consultazione di queste risorse, (email e social), sono stati ottenuti diversi indirizzi IP, gestiti dai provider di telefonia. Innanzitutto erano presenti diversi indirizzi IP riferibili a connessioni di linea fissa che però risultava venire erogata a un indirizzo con civico inesistente. Erano inoltre presenti molteplici connessioni mobili di tipo NAT, ovvero connessioni in cui diverse utenze condividono il medesimo indirizzo IP pubblico nello stesso lasso di tempo. Questa circostanza ha richiesto una minuziosa analisi di una grande quantità di dati, grazie alla quale è stato possibile venire a conoscenza di diverse utenze mobili e di diversi identificativi IMEI relativi a dispositivi in uso al venditore.

Dalle indagini tecniche condotte sul territorio è stato possibile individuare l'indirizzo di erogazione di una linea telefonica fissa. Interrogando nuovamente i fornitori di telefonia mobile non virtuali, sono stati ottenuti i dati di tutte le utenze mobili le cui schede SIM sono state inserite nei dispositivi associati al venditore. Tra queste utenze, due sono risultate intestate all'indagato, residente e domiciliato nella stessa via dove, a un civico inesistente, risultava erogata la linea citata di telefonia fissa. Grazie a tali attività sono stati raccolti elementi utili a confermare la coincidenza dell'identità dell'indagato principale con il soggetto celato dietro il nickname Benz99 ed altri due responsabili (sottoposti a misure cautelari) e sono stati ottenuti elementi in merito ad ulteriori condotte criminose poste in essere dal soggetto, tra cui l'autoriciclaggio di somme ottenute tramite l'acquisto on-line di codici di carte di credito illegalmente carpiti ed utilizzati per effettuare acquisti in frode.

Il Nucleo, inoltre, ha partecipato, unitamente al Servizio Centrale Investigazioni Criminalità Organizzata, ad un'operazione sul contrasto al finanziamento, anche attraverso il circuito dei money transfer, del terrorismo internazionale legato ai "foreign fighters". Dall'attività di analisi effettuata sui flussi finanziari intercorsi con i paesi a rischio tramite la rete nazionale dei money transfer, venivano individuati alcuni soggetti. Il Nucleo mediante un'attenta e

minuziosa azione di monitoraggio del web ha analizzato i profili social dei soggetti coinvolti, inoltre attraverso l'esecuzione di una delicata attività di analisi forense sul materiale informatico acquisito nel corso delle indagini ha individuato le connessioni esistenti tra i medesimi. I successivi sviluppi investigativi hanno consentito di raccogliere una ingente quantità di elementi di prova tali da consentire l'emissione ed esecuzione di nr. 10 ordinanze di custodia cautelare in carcere nei confronti di altrettanti soggetti di origine siriana facenti parte di un'associazione a delinquere aggravata, a carattere transnazionale, dedita ai reati di riciclaggio, autoriciclaggio ed abusiva attività di prestazione di servizi di pagamento, condotte finalizzate al finanziamento di gruppi terroristici di matrice islamica.

Attività e segnalazioni del CERT Nazionale

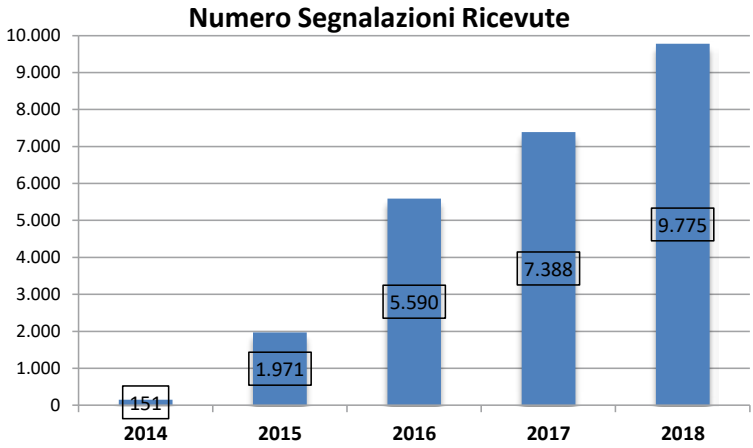
Introduzione

Il 2018 ha visto un consolidamento delle attività che il CERT Nazionale (https://www.certnazionale.it) svolge nei confronti della propria "constituency" sia a livello nazionale che internazionale.

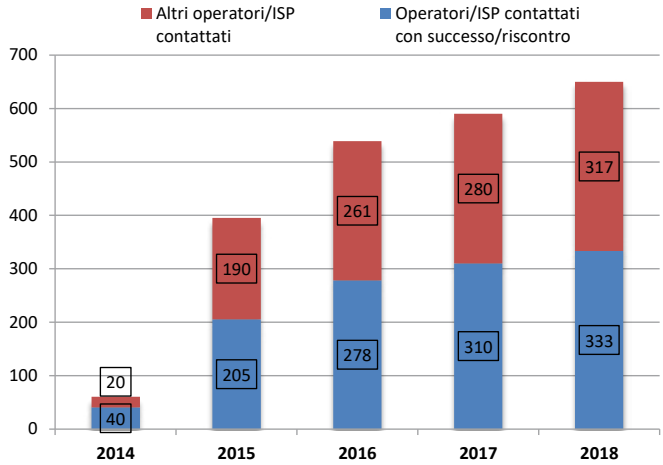
In attesa dell'attuazione del D.Lgs. del 18 maggio 2018, n.65, che stabilisce la costituzione di un CSIRT unico presso la Presidenza del Consiglio dei Ministri, il CERT Nazionale ha intensificato le attività svolte in collaborazione con il CERT-PA, tra le quali si segnala la partecipazione congiunta all'esercitazione "Cyber Europe 2018".

Le attività

Il CERT Nazionale opera principalmente come "*facilitatore*" per la soluzione di incidenti informatici a livello nazionale e transnazionale e riceve giornalmente segnalazioni relative ad incidenti, o semplici minacce, riferibili a reti italiane. Le segnalazioni provengono da una molteplicità di soggetti, da ricercatori di sicurezza ad omologhi CERT internazionali, da CERT o SOC di Aziende italiane o estere, a semplici cittadini o soggetti privati.



Il numero di segnalazioni ricevute, aumentate del 30% rispetto al 2017, conferma la sempre crescente attività del CERT Nazionale come punto di riferimento, sia a livello nazionale che a livello internazionale, per lo scambio di informazioni relative a minacce, incidenti e vulnerabilità riscontrate in rete.

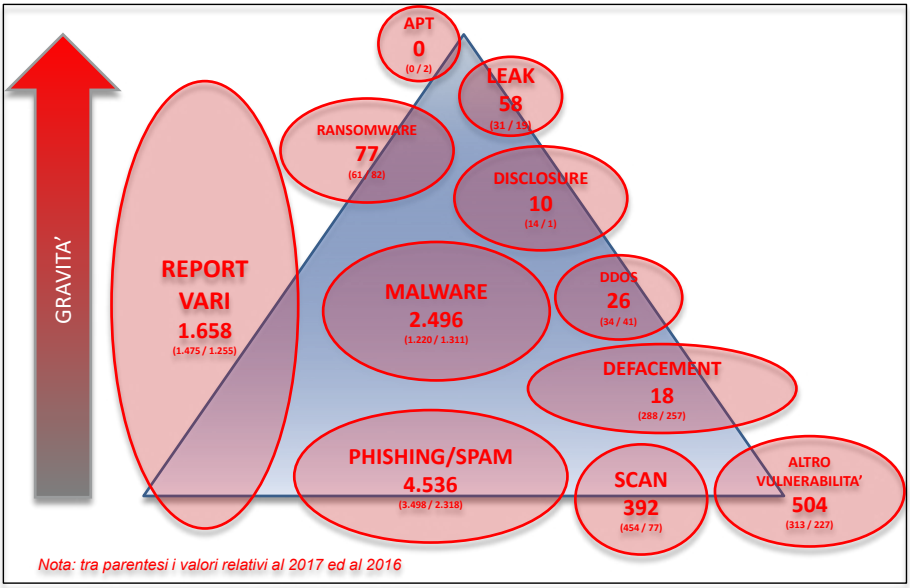


Anche il numero di soggetti nazionali, Operatori ed Internet Service Provider, con i quali il CERT si è interfacciato nel corso del tempo, è in costante crescita. Ormai sono circa 650 gli Operatori con i quali il CERT Nazionale ha scambiato e condiviso informazioni volte a mitigare o a prevenire incidenti informatici che ne abbiano coinvolto le rispettive reti.
Con la maggior parte degli Operatori si è instaurato un contatto proficuo, improntato alla reciproca fiducia, che ha consentito la risoluzione delle problematiche riscontrate.
Anche il numero il numero di omologhi CERT a livello internazionale con i quali il CERT Nazionale italiano è entrato in contatto è in costante crescita con un numero che sfiora i 60 soggetti di altrettanti Paesi europei ed extra-europei.

Le segnalazioni

Le tipologie di segnalazioni che giungono quotidianamente al CERT Nazionale sono di vario genere e si riferiscono sia a compromissioni acclarate, a seguito di attacchi o incidenti, sia a minacce legate a vulnerabilità riscontrate in rete.
Il 2018 ha continuato a registrare un notevole peso delle segnalazioni legate a pagine di *phishing* ospitate su reti italiane (+30% rispetto al 2017) che, pur rappresentando un vettore di attacco ormai datato e ben conosciuto, riesce ancora a colpire diverse vittime anche attraverso tecniche sempre più raffinate.
Si sono continuate a registrare campagne di diffusione di *malware*, principalmente, ma non solo, volto alla compromissione delle credenziali di posta elettronica o di accesso a servizi bancari. Da questo punto di vista la diffusione di *malware* estorsivo (*ransomware*) pur proseguendo sulla falsariga dell'anno precedente, non ha registrato fenomeni mediatici comparabili a quelli del 2017, come *WannaCry* o *notPetya*.
Si è invece avuto un incremento, anche a livello mediatico, dei fenomeni di *data breach*, ovvero della compromissione di portali più o meno grandi, con conseguente pubblicazione e rivendita, principalmente nel *dark web*, di credenziali di accesso di centinaia di migliaia

di ignari clienti. Per capire la dimensione del fenomeno il solo sito *haveibeenpwned*, che rappresenta il più conosciuto tra quelli che consentono di verificare se il proprio account risulti tra quelli appartenenti ai *data breach* noti, contiene oltre 6 miliardi di record. A parte la completa compromissione dei dati presenti nei portali coinvolti, il rischio maggiore resta quello del *password-reuse*, soprattutto nel caso in cui le credenziali di accesso consentano una facile individuazione del soggetto fisico coinvolto, anche se, in alcuni casi le credenziali "rubate" sono state a loro volta utilizzate nell'ambito di campagne estorsive alternative al *ransomware* (tipicamente di tipo "*sextortion*") come ulteriore fattore di pressione psicologica nei confronti delle vittime, che vedendosi indicare dai criminali una *password* in qualche modo realmente utilizzata, sono portati più facilmente a cadere nella truffa.



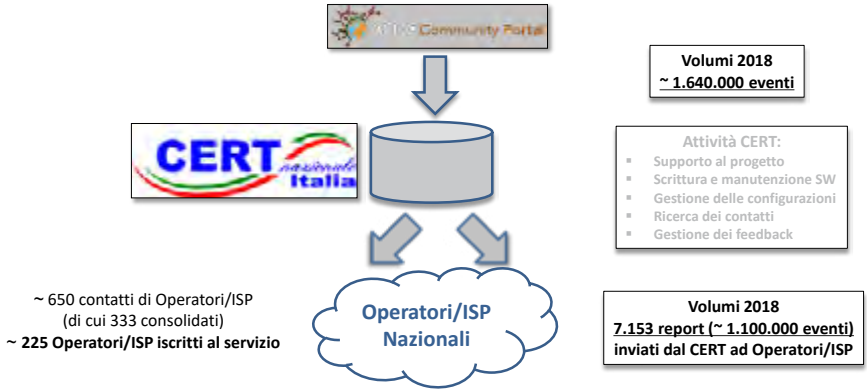
Vengono riassunte in figura le segnalazioni giunte al CERT Nazionale nel corso del 2018. La rappresentazione riportata non è chiaramente esemplificativa dello stato dell'arte globale, ma una vista di quanto pervenuto al CERT.

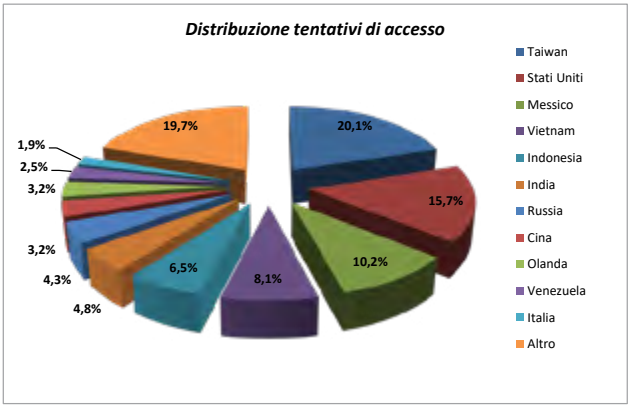
La reportistica periodica sulla quale il CERT Nazionale può contare rappresenta una fonte informativa estremamente interessante. I dati provengono sia da fonti interne, nella fattispecie le *honeypot* predisposte nell'ambito del progetto europeo ACDC (*Advanced Cyber Defence Center*), sia da fonti esterne. Le fonti esterne sono generalmente di tipo *semi-aperto*, ovvero fonti potenzialmente aperte ma per le quali il CERT Nazionale può contare su viste complessive dell'intero spazio di indirizzamento italiano, ma anche di tipo *chiuso*, tipicamente report provenienti da aziende di sicurezza o, più frequentemente, da omologhi

CERT internazionali a fronte di attività specifiche di contrasto alla diffusione di *malware* e/o *botnet* o di eventi specifici rilevati in rete.

Le *honeypot*

Nel corso del 2018 è proseguita l'attività di diffusione agli Operatori coinvolti delle segnalazioni fornite dalla rete *anti-botnet* del progetto europeo ACDC, terminato nel corso del 2015, ma i cui risultati vengono ancora utilmente sfruttati.
L'informatizzazione della procedura di ricezione ed invio delle segnalazioni ha consentito di inviare oltre 7.000 report nel corso del solo 2018 ai 225 Operatori iscritti al servizio.

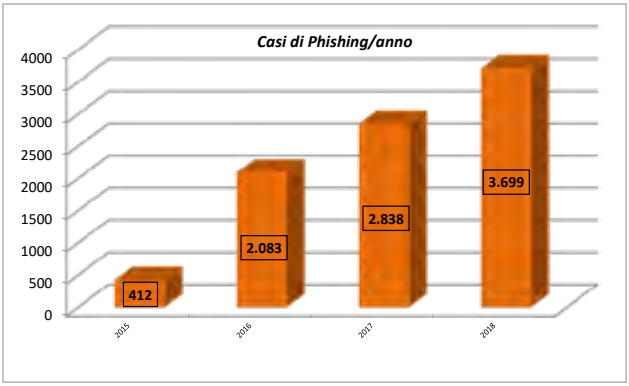




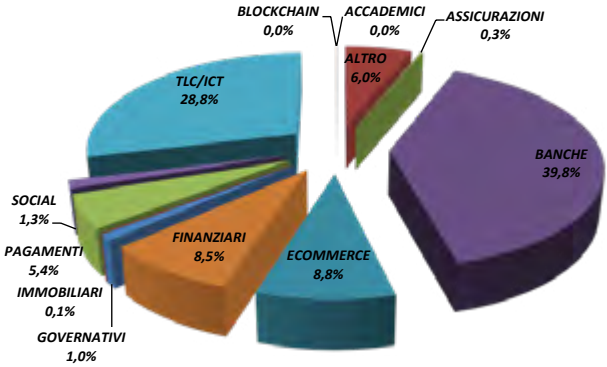
La ree di *honeypot* predisposta nell'ambito del progetto, ovvero di macchine dedicate a "*catturare*" tentativi di attacco dall'esterno, continua a raccogliere un notevole numero di eventi, tra tentativi di connessioni malevole e tentativi di scaricamento di *malware*, consentendo anche di avere una ricca base dati sulla provenienza, a livello mondiale, di determinati tipi di attacco.

Il *phishing*

Nel corso del 2018 si sono registrate numerose campagne di *malspam*, *phishing* e *spear-phishing*, che restano i principali vettori di diffusione di *malware* oltre a classici strumenti per la compromissione di credenziali.
In particolare diverse sono state le segnalazioni di tentativi di *spear-phishing* diretti a figure apicali di organizzazioni appartenenti a diversi settori merceologici, tra cui energia e trasporti.



Le segnalazioni di pagine di *phishing* ospitate su server italiani compromessi e pervenute al CERT Nazionale sono notevolmente cresciute nel corso degli anni, passando dalle circa 400 del 2015 alle 3.700 del 2018.
Generalmente questo tipo di segnalazioni giungono al CERT Nazionale solo dopo precedenti tentativi di contattare gli amministratori o di risolvere in altro modo l'incidente ed il numero rappresenta pertanto solo una parte del fenomeno, sebbene statisticamente rilevante.



Circa il 40% delle segnalazioni ha riguardato falsi siti di banche, italiane ed estere, mentre una quota consistente (circa il 30%) è stata quella relativa ad attacchi che hanno preso di mira grandi Operatori OTT (*Over The Top*) o del settore ICT volti alla compromissione delle credenziali di accesso (tipicamente a profili *social* o *Email*).
Non trascurabili anche attacchi ai danni di clienti di servizi finanziari (tra cui quelli legati a *criptovalute*) o di portali di E-commerce.
I siti utilizzati a scopo malevolo sono spesso riconducibili a domini registrati ad-hoc o, in gran parte dei casi, alla compromissione di siti legittimi, spesso grazie allo sfruttamento di vulnerabilità dei CMS (*Content Management System*) utilizzati e non aggiornati.

Minacce e incidenti

Se il 2017 era stato caratterizzato dall'attacco "*WannaCry*", *ransomware* capace di colpire diversi soggetti a livello mondiale (anche se, fortunatamente, in Italia l'impatto fu decisamente limitato se confrontato con quanto accaduto in altri Paesi), nel 2018 non ci sono stati casi che abbiano avuto una risonanza mediatica confrontabile, se non, periodicamente, quella legata ad alcuni importanti *data breach*, soprattutto quando tra gli account compromessi risultavano quelli di qualche soggetto istituzionale.

Il CERT Nazionale, grazie alla propria rete di *infosharing* a livello nazionale ed internazionale riceve giornalmente report relativi a minacce e compromissioni. Tali segnalazioni possono avere carattere periodico o *una tantum* e legate ad un particolare evento e, generalmente, si compongono di liste di macchine compromesse e dei relativi indirizzi IP. La compromissione è spesso rilevata da terze parti attraverso analisi di traffico specifiche (per esempio connessioni a *sinkhole* predisposti *ad hoc*) o di macchine a loro volta compromesse (per esempio C&C analizzati dopo la dismissione di infrastrutture fraudolente). Tali segnalazioni, opportunamente analizzate, vengono inoltrate agli Operatori/ISP coinvolti per la parte di propria competenza e per tutte le azioni di verifica e bonifica che si rendano necessarie.
Nel corso dell'anno sono state predisposte oltre 20 campagne informative, contenenti ol-

tre 20.000 macchine afferenti a reti italiane, inviate agli oltre 300 Operatori e Provider coinvolti relative a diversi attacchi registrati nel corso del tempo. Tra questi si ricordano le campagne di diffusione del *malware Ursnif* e la compromissione di diversi siti per lo sfruttamento di una vulnerabilità del CMS *Drupal*, note come "*Drupalgeddon*" e "*Drupalgeddon 2*", attivamente sfruttata dai criminali informatici per compromettere siti web ed installare dei *cryptominer*.

Anche a livello di prevenzione, il CERT Nazionale ha proseguito con l'attività di predisposizione di campagne informative e di sensibilizzazione relative a macchine configurate non correttamente o a protocolli pericolosamente "aperti" in rete, al fine di prevenirne l'utilizzo da parte di criminali informatici per attacchi, tipicamente *DDoS* (*Distributed Denial of Service*), a danni di terze parti.
A titolo di esempio, a fine febbraio 2018 sono stati rilevati a livello internazionale attacchi *DDoS* estremamente pesanti (fino a raggiungere la banda record di 1,7 TB) che avrebbero utilizzato istanze di *Memcached* (un sistema per il *webcaching* ad oggetti distribuiti progettato per diminuire il tempo di caricamento delle pagine dei siti web dinamici) aperte ed accessibili dall'esterno. In particolare l'apertura all'esterno al protocollo UDP avrebbe reso possibile raggiugere altissimi fattori di amplificazione (fino a 50.000), tali da rendere particolarmente appetibile ai criminali informatici l'utilizzo delle macchine esposte per attacchi ai danni di terze parti. A seguito degli eventi rilevati, il CERT Nazionale ha provveduto ad emettere alcuni approfondimenti sul sito web ed alla predisposizione di alcune campagne informative nei confronti degli Operatori di rete italiani all'interno delle quali risultavano macchine con il servizio aperto ed accessibile dall'esterno. A seguito della campagna è stato riscontrata una sensibile diminuzione del numero di macchine esposte a livello italiano.

Come nell'anno precedente, anche nel 2018 si sono registrati alcuni casi che hanno visto il ricorso al CERT Nazionale, da parte di diversi soggetti, a volte privati cittadini, a volte ricercatori di sicurezza, per segnalazioni di vulnerabilità di varia gravità in modalità "*responsabile*". Le segnalazioni giunte nel corso dell'anno, talvolta relative a problematiche che avrebbero messo seriamente a rischio la sicurezza dei dati, hanno consentito al CERT Nazionale di raggiungere direttamente le strutture tecniche delle Aziende interessate per la messa in sicurezza dei rispettivi sistemi. Il CERT Nazionale si è impegnato nella verifica della correttezza e della affidabilità delle segnalazioni e, una volta accertata la presenza della falla di sicurezza ha proceduto all'invio dell'informativa alle funzioni tecniche preposte. L'attività ha richiesto anche una attenta ricerca e valutazione dei soggetti ai quali inviare la segnalazione, riscontrando sempre la massima collaborazione per la risoluzione delle problematiche rilevate in tempi estremamente ridotti.
Una decina i casi più seri che mettevano a repentaglio informazioni personali, documentazione o credenziali. Le segnalazioni hanno riguardato diversi settori merceologici: dai trasporti alle banche, dalla telefonia all'editoria.
La fonte informativa proveniente da soggetti privati non malintenzionati si è confermata

essere una preziosa risorsa per la prevenzione di incidenti potenzialmente gravi che avrebbero potuto concretizzarsi con il furto di informazioni, siano esse informazioni personali piuttosto che credenziali di accesso, o con la *disruption* di interi sistemi.

Il sito web

Il sito web del CERT Nazionale (*https://www.certnazionale.it*) si rivolge a cittadini ed imprese con **notizie** di interesse generale legate alla sicurezza informatica, **bollettini** tecnici e **linee guida** di comportamento.
L'obiettivo è quello di trattare argomenti tecnici con la necessaria precisione, ma cercando di renderne i contenuti utili e comprensibili anche a chi non necessariamente ha conoscenze tecniche professionali.

Le statistiche di accesso al sito web confermano un trend di crescita, stimabile in un +30% rispetto all'anno precedente, del numero di consultazioni.

Nel corso del 2018, in particolare, sono state pubblicate:

- **338 notizie** a valenza informativa di vasto interesse a copertura degli eventi di sicurezza rilevati: dalla diffusione di *malware* all'utilizzo di nuove tecniche, dalla pubblicazione di aggiornamenti di sicurezza da parte dei *vendor* alla scoperta di nuove vulnerabilità;

- **12 bollettini** tecnici specialistici, relativi a specifiche vulnerabilità di sistemi diffusi e considerate ad alto rischio di sicurezza per gli utilizzatori.

Le **notizie** (***news***), pubblicate con cadenza giornaliera, rappresentano un giusto compromesso tra una trattazione tecnica specialistica ed una informativa generale relativa alle problematiche di sicurezza del momento.
Le pubblicazioni contengono informazioni utili per tutti gli utilizzatori di sistemi informatici, indipendentemente dal loro livello di conoscenza tecnica, a partire dalla descrizione delle problematiche di sicurezza rilevate in rete, alla disponibilità di aggiornamenti di sicurezza, a suggerimenti generali o particolari, per la protezione dei propri dati. In particolare la disponibilità di aggiornamenti di sicurezza per le principali piattaforme di vasto utilizzo è messa sempre in grande evidenza al fine di sensibilizzare l'utenza ad una loro veloce applicazione sui propri sistemi.
Nel corso del 2018 si è inoltre continuato a riservare molto spazio alle campagne di diffusione del *malware* (compreso il *ransomware*, in tutte le sue nuove versioni), al fine di fornire una informazione precisa e tempestiva sulle tecniche utilizzate e sui relativi rischi per gli utilizzatori della rete.
Oltre a fornire elementi tecnici utili, tra i quali precisi indicatori di compromissione o indicazioni di massima sulla prevenzione o su possibili soluzioni del problema, l'obiettivo dei comunicati resta quello di riassumere le azioni necessarie per evitare di diventare vittime di criminali informatici, spesso legate al buon senso più che a conoscenze tecniche particolarmente approfondite.
I **bollettini** rappresentano invece un approfondimento tecnico specialistico, dedicato ai soggetti più esperti del settore, su argomenti di particolare importanza, tipicamente vulnerabilità riscontrate su piattaforme o sistemi di vasta diffusione e con impatti potenzialmente molto estesi.

Elementi sul cybercrime nel settore finanziario in Europa

[A cura di Pier Luigi Rotondo e Domenico Raguseo, IBM]

Introduzione

Il cybercrime finanziario ha visto importarti sviluppi nel 2018, con numerose evoluzioni sia dei malware usati che del modus operandi dei gruppi cyber criminali. Il fenomeno dei malware per frodi finanziarie è ormai territorio di gruppi criminali internazionali, ben organizzati e strutturati.

Nell'analisi che segue, presentiamo e commentiamo i risultati delle rilevazioni sul cybercrime nel settore finanziario in Europa nel corso del 2018. Questo lavoro è stato possibile anche grazie ai contributi del team di ricerca IBM Security, IBM X-Force, le analisi di IBM Trusteer, e al lavoro quotidiano di molti IBMers che gli autori desiderano ringraziare.

Le fonti sono elencate nella bibliografia al termine del capitolo.

Un anno di cybercrime finanziario

La storia sembra ripetersi quando si tratta di malware. Anche nel 2018, proprio come era avvenuto l'anno precedente, **Marcher** è il primo malware a festeggiare il nuovo anno.

Marcher è un malware per Android usato per rubare numeri e dati di carte di credito, apparso alla fine del 2013, e offerto in vendita sui siti underground in lingua russa. Marcher ebbe il suo periodo d'oro durante il 2016, con attacchi a banche in Francia, Polonia, e Austria. Nei suoi primi utilizzi documentati Marcher usava una schermata di overlay all'accesso a Play Store per catturare l'inserimento del numero di carta di credito, la data di scadenza e il codice CVV2. Nel Rapporto CLUSIT 2018 [1] avevamo già descritto un'importante campagna verso gli utenti di banche francesi, con un picco ai primi di Gennaio 2017. In occasione di questa campagna, gli autori avevano sviluppato un modulo per catturare anche l'SMS inviato dalla banca come secondo fattore di autenticazione.

La campagna di inizio 2017 partiva da mail di phishing che invitavano gli utenti a un aggiornamento urgente di Flash Player, con istruzioni dettagliate e un link, ovviamente da un sito non ufficiale. L'aggiornamento trojan chiedeva, tra le altre, anche l'autorizzazione ad accedere agli SMS, proprio per attivare modulo di SMS hijacking. Una autorizzazione insolita per un lettore multimediale, ma ignorata da molti incauti utenti. La frode poteva avere inizio.

La campagna Marcher del 2018 si sviluppa nelle prime due settimane di **Gennaio** e colpisce utenti di banche in **Turchia**. Questa volta il malware è inserito all'interno di giochi Android in lingua turca, caricati su Play Store e sfuggiti ai controlli automatizzati dello store. Dopo l'infezione iniziale, il trojan monitora l'attività dell'utente, pronto ad attivarsi appena la vittima accede ad una delle app di banking configurata.

A questo punto Marcher, con una schermata di overlay copre la applicazione legittima e invita l'utente a inserire le credenziali di login, per poi inviarle all'esterno attraverso la sua infrastruttura di Command and Control (C&C).
Ancora a Gennaio, una campagna **GootKit v2** prende di mira utenti di banche online, servizi di pagamento nel **Regno Unito**, e due piattaforme di cambio per cripto valute. Gli operatori di GootKit sembrano tornati indietro [2], con una mossa a sorpresa, dai redirection attack che hanno spopolato nel 2017, ai più tradizionali webinjects. La campagna GootKit di Gennaio 2018 si diffonde attraverso email con allegati Word che guidano l'utente ad attivare l'esecuzione delle macro. Di fatto le macro sfruttano la vulnerabilità CVE-2017-11882, una Memory Corruption presente in alcune versioni di Office, per scaricare ed eseguire GootKit sul computer della vittima. Microsoft, ben prima dell'attacco, aveva già fornito indicazioni su come disabilitare l'Equation Editor affetto dalla vulnerabilità, e poi a fine Novembre 2017 una Service Pack correttiva. Il malware fa tuttavia incetta di utenti poco attenti agli aggiornamenti di software. Per tutto il 2017, e la parte iniziale del 2018 gli operatori di GootKit hanno estensivamente usato documenti Microsoft, proprio per la loro popolarità in ambienti di lavoro, che ne rende delicato il filtraggio.

Nella prima parte del 2018 si intensifica un fenomeno già osservato nei mesi precedenti, la deriva del malware **TrickBot** verso le piattaforme a supporto delle cripto-valute. L'attacco TrickBot analizzato [3] si concentra su una piattaforma che consente di acquistare bitcoin con la propria carta di credito e addebitarli sul proprio wallet. Questo particolare attacco si sviluppa tutto nella fase di acquisto della cripto valuta. Dopo il login, la vittima inserisce l'indirizzo del proprio wallet bitcoin, per poi essere ridiretto su un sistema esterno di pagamento con la carta di credito. È proprio a questo punto che attraverso webinjects le coordinate del wallet su cui accreditare i bitcoin vengono sostituite con quelle dei cyber criminali. L'importo corretto viene addebitato alla carta di credito della vittima, che riceve anche conferma dalla società emettitrice della carta di credito, ed + quindi convinto che la transazione abbia avuto successo. In realtà la somma ha iniziato il suo viaggio verso il wallet dei cyber criminali.
Un nuovo banking trojan fa la comparsa nel mese di **Marzo**. Si tratta di **BackSwap**, usato dapprima verso alcune banche in **Polonia** [4], e poi in campagne decisamente più importanti ad Agosto, contro sei banche spagnole.
Ad **Aprile** alcune campagne di spam [5] [6] che si presentano come contenenti modelli F24 oppure fatture, veicolano in **Italia** il malware **Zeus Panda** all'interno di allegati Office. Per queste campagne il malware cattura le credenziali di login ad un lungo elenco di banche online e istituti finanziari italiane. I file Office contengono script VBA che si avviano dopo aver aperto il documento, e dopo aver ignorato il messaggio di sicurezza di Office, attivando di fatto l'esecuzione delle macro.
Tra **Giugno** e **Luglio** una serie di campagne di attacco basate su **TrickBot** prendono di mira banche e piattaforme di pagamento principalmente nel **Regno Unito**, e in misura inferiore in **Germania**, **Austria**, **Irlanda**, **Francia**, **Norvegia**, oltre alcune piattaforme

di cambio per cripto valuta. TrickBot, che in passato aveva usato come veicolo la botnet Necurs, nel 2018 si sposta verso più tradizionale spamming di documenti Office contenenti macro.
Nelle campagne 2018 TrickBot usa, in egual misura, sia redirection attack che webinject. La tecnica dei redirection attack, cresciuta enormemente del corso del 2017 e di cui avevamo parlato nel rapporto CLUSIT 2018 [1], si è rivelata difficile da gestire, e segna un rallentamento nel corso del 2018. Continua invece il tentativo di offuscare le comunicazioni tra gli endpoint infetti e la rete di Command-and-Control. Gli sviluppatori di TrickBot integrano, a Luglio 2018, un plugin che sfrutta il modulo Tor di Nginx, offuscando le comunicazioni tra endpoint infetto e le altri componenti dell'infrastruttura di supporto, rendendo decisamente più complessa l'analisi e il blocco dell'attacco. Ancora, tra **Giugno** e **Luglio**, alcune campagne di spamming attaccano enti pubblici e utenti privati in **Italia** con il malware **Ursnif** (alias **Gozi**) [7] [8].
La mail che veicola il malware sembra provenire da un'utenza PEC, ma questo è solo un trucco. Il messaggio è in realtà una semplice email generata con tecniche di spoofing, in grado di raggiungere qualsiasi casella di posta elettronica, e il riferimento alla PEC nell'indirizzo serve solo a rendere più credibile il mittente. Ancora una volta le email veicolano un documento Word contenente macro, disabilitate alla prima apertura del documento, ma con un messaggio che inganna abilmente l'utente mimando la veste grafica di Office.
Il messaggio sembra essere una normale notifica di Office, e indica che il file è stato creato con una versione precedente di Word, e che per aprirlo è necessario abilitare l'esecuzione delle macro. Un messaggio ingannevole che consente il download e l'istallazione del malware sul computer della vittima, e la conseguente compromissione. Nei sistemi compromessi analizzati, Ursnif cattura credenziali di posta elettronica, di piattaforme cloud, e di siti di e-commerce.
La cattura delle credenziali per accedere alla posta elettronica è un'attività apparentemente anomala per un banking trojan. Più tardi nell'anno capiremo che alcune campagne, utilizzando le credenziali rubate, inseriscono il malware all'interno di scambi di email realmente avvenuti, con il sottile fine di aumentare il successo della campagna di spamming.
Sempre a **Luglio**, una campagna basata sul malware bancario **Kronos** [9] colpisce utenti di almeno cinque istituti finanziari in **Germania**. La campagna di spamming veicola documenti Word che si presentano come un aggiornamento delle condizioni contrattuali, apparentemente inviati dagli stessi istituti. Il documento Word contiene però, al suo interno, delle macro che se abilitate scaricano una copia di Kronos, infettando il computer.
Kronos è un malware bancario che usa webinject per modificare ciò che la vittima vede sullo schermo e perpetrare un attacco del tipo man-in-the-browser, con l'obiettivo ultimo di catturare le credenziali per l'accesso ai siti bancari. La novità di questa campagna è l'uso di server di Command-and-Control attestati sulla rete Tor.
Ad **Agosto** una nuova campagna basata sul malware **Ramnit** prende di mira banche e istituti di carte di credito nel **Regno Unito**, e contemporaneamente siti per la ricerca di personale sia nel Regno Unito che in **Francia**.

La ricerca di credenziali di accesso a siti per la ricerca di personale, alquanto apparentemente bizzarra, trova una possibile interpretazione nella necessità di arruolare continuamente *money mule*, gli spalloni digitali disposti a far transitare sui loro conti bancari le somme frodate, dopo aver trattenuto una parte della somma come compenso. Il mercato armonizzato dei pagamenti nell'area Euro apre le frontiere anche alle frodi. Gli importi frodati in un attacco sono spesso inviati verso beneficiari compiacevoli in altri paesi europei prima di saltare al di fuori delle barriere esterne dell'Unione Europea e rendere più complesso il tracciamento e il recupero.
La campagna Ramnit di Agosto prende di mira account bancari personali. Le coordinate bancarie del beneficiario vengono sostituite, con webinject che manipolano ciò che compare nel browser, in modo da indurre la vittima ad autorizzare inconsapevolmente una transazione verso il conto di un money mule, piuttosto che del legittimo destinatario. Dal punto di vista della banca, la transazione si presenta come assolutamente legittima, quindi difficile da individuare come fraudolenta al momento dell'esecuzione.

Nel corso del 2017 Ramnit era stato responsabile di circa una infezione su quattro, attestandosi come uno dei malware finanziari più attivi. La stessa tendenza è continuata nel 2018, con **Ramnit** nella lista dei *Top* 5 malware che si sono contesi il mercato delle frodi finanziarie, assieme a **TrickBot**, **Ursnif/Gozi**, **IcedID** e **Zeus Panda**.
Il nuovo banking trojan **BackSwap**, dopo attacchi blandi verso banche polacche nel mese di Marzo [4], si presenta in modo decisamente più aggressivo in una campagna verso sei banche in **Spagna** [10]. Secondo l'analisi di X-Force, BackSwap si basa su funzionalità che esistevano già all'interno di **Tinba**, ipotizzando un collegamento tra gli operatori due malware. BackSwap implementa in maniera estremamente innovativa i webinject, inserendo del codice JavaScript all'interno della URL iniettata nella barra indirizzi del browser, raggirando così alcune protezioni antimalware e del browser che si limitano ad analizzare il contenuto della pagina da visualizzare. Il malware tiene costantemente sotto controllo la navigazione utente, e quando la vittima approda a specifiche pagine bancarie pre-configurate, come ad esempio la sezione del sito di banking per effettuare un bonifico, il malware sostituisce le coordinate bancarie del destinatario con quelle del mule.
Anche una nuova campagna **GootKit v2** sfrutta webinject, alla quale aggiunge la funzionalità di video cattura di porzioni selezionate della transazione, che viene poi inviata all'esterno. La video cattura semplifica il lavoro agli operatori di GootKit che possono studiare dal vivo l'interfaccia del sito bancario senza la necessità di dover fare login e senza lasciare alcuna traccia. Le nuove configurazioni di **Settembre** prendono di mira banche e società emettitrici di carte di credito in **Italia**, **Regno Unito**, **Francia**, **Olanda** e **Belgio**.
In passato altri malware avevano catturato screenshot di passaggi critici della transazione bancaria. Lo stesso GootKit aveva iniziato ad aggiungere alcune funzionalità di video cattura già nel 2016. Questa è però la prima implementazione su larga scala di registrazioni video che permette di seguire nel dettaglio tutti i passaggi e le tempistiche di eventuali secondi fattori di autenticazione, sia al login che all'autorizzazione della transazione.

Individuato per la prima volta nel 2014, GootKit è considerato uno dei più avanzati banking trojan attivi ed è stato usato principalmente in Europa. Di Gootkit avevamo già parlato nel rapporto CLUSIT del 2017 [11] in quanto era stato uno dei banking trojan a dominare lo scenario del 2016, e ancora nel rapporto CLUSIT del 2018 [1] per temutissimi redirection attack verso banche di Regno Unito e Italia.
A **Novembre** una nuova campagna **BackSwap** prende di mira alcune banche nella **Repubblica Ceca**. BackSwap si presenta da subito molto aggressivo. Dopo una prima campagna verso banche polacche [4], BackSwap raccoglie molto più successo con una campagna verso utenti di banche spagnole [10]. Adesso nella target list di BackSwap ci sono anche banche nella Repubblica Ceca. BackSwap si caratterizza per inserire codice JavaScript all'interno barra indirizzi del browser, raggirando così alcune protezioni antimalware e del browser. BackSwap implementa frodi man-in-the-browser automatizzate. Il malware segue la transazione dell'utente e si attiva all'inserimento del beneficiario, sostituendo il reale beneficiario con le coordinate bancarie di un mule. Il malware lascia passare inalterati eventuali fattori 2FA che quindi contribuiscono ad autorizzare la transazione. Webinjects continuano a far vedere alla vittima le coordinate bancarie desiderate, anche se la transazione avviene verso un altro soggetto.

Una campagna di spamming a Novembre [12] verso vittime in **Italia** veicola allegati malevoli, che se aperti, infettano il computer con malware **Danabot** [13]. Danabot perpetra attacchi man-in-the-browser, ed è ingegnerizzato per il furto delle credenziali di sistema, quelle memorizzate nel browser, e le credenziali di accesso a client email. Inoltre, consente l'accesso remoto al sistema infetto via VNC e RDP. Il malware si diffonde attraverso un'e-mail ingannevole che si presenta come una fattura commerciale, con allegato un archivio rar. Una volta scompattato, l'archivio rar contiene un file VBScript che se aperto darà il via all'infezione.
L'**Italia** è colpita anche da una campagna di spamming che veicola il malware **Ursnif** (alias **Gozi**) [14]. Questa campagna è particolarmente insidiosa anche per l'utente attento in quanto, sfruttando precedenti compromissioni di account email, invia il malware all'interno di scambi di mail già intercorsi tra la vittima e l'account email compromesso [16]. Le mail di spamming contengono un file Word con all'interno una macro malevola. Ancora una volta l'utente viene indotto ad abilitare l'esecuzione delle macro, simulando una notifica di sistema che spiega che il file è stato creato con una versione precedente di Word e che per l'apertura è necessario abilitare il contenuto, cosa che consente l'esecuzione della macro. Il documento Word, una volta aperto, apre una command shell di Windows in modalità nascosta, che invoca la PowerShell per scaricare da un sito Internet esterno il malware vero e proprio (payload) sotto forma di file eseguibile exe.
Il 2018 si conclude per l'**Italia** con una fantasiosa campagna di spamming **Gootkit** [17] che raggira l'analisi automatica in sandbox incrementando la propria dimensione, una volta scompattato, fino ad oltre 450MB, rendendo di fatto impossibile l'upload su sistemi e piattaforme di analisi degli allegati per la ricerca del malware.

Questa release di GootKit implementa inoltre molti controlli per verificare l'esecuzione in modalità debug o dentro macchine virtuali, segno evidente di un'analisi dell'eseguibile, automatizzata oppure assistita dall'operatore.
La tecnica usata per rendere il file di grandi dimensioni dopo l'estrazione è sorprendentemente semplice. All'interno del file sono state inserite numerosissime aree vuote, che hanno un tasso di compressione altissima, e quindi ad un file compresso di dimensioni esigue, facilmente allegabile ad un email. Una volta estratto sulla macchina vittima, l'attachment ricrea il file originario, di dimensioni molto grandi.

Compartecipazione della vittima

L'elemento che ha contribuito al successo delle principali campagne di malware dell'anno è stata la compartecipazione della vittima, che spesso ha aperto ed eseguito gli allegati malevoli ricevuti via mail. Questo nella noncuranza delle più elementari norme di precauzione, e dei messaggi di avvertimento generati dalle versioni più recenti dei prodotti di produttività, come Office.
Tra queste campagne annoveriamo GootKit nel Regno Unito a Gennaio, Zeus Panda in Italia ad Aprile [5] [6], TrickBot a Giugno-Luglio, Ursnif/Gozi a Luglio [7] [8], Kronos in Germania a Luglio [9], Danabot a Novembre [12] verso vittime in Italia, e ancora Ursnif a Novembre. [14]
Il fenomeno è più grave di quanto si possa immaginare. All'atto pratico, non solo la vittima ha aperto per curiosità una mail che nella maggior parte dei casi non attendeva, ma si è anche fidato delle informazioni fallaci che ha visto a schermo, ed ha collaborato attivamente con l'attaccante abilitando l'esecuzione delle macro all'interno dei documenti o dei file.
Le macro consentono di automatizzare alcune attività all'interno di un documento Office, e sono generalmente scritte in Visual Basic Application Edition (VBA), da cui spesso il nome di VBScript. Le macro sono un ottimo strumento di produttività, tuttavia possono costituire un potenziale rischio di sicurezza in quanto un attaccante può inserire macro malevole all'interno di un documento Office per scaricare il malware e infettare il computer. Quando si apre un documento Office contenente macro, o un documento creato da altri, vengono visualizzati avvisi di sicurezza ben evidenti, con un pulsante che consente di abilitare il contenuto. A causa della loro potenziale pericolosità, le macro vanno attivate solo se si è certi della loro effettiva necessità, e dell'origine del documento.

You have new mail waiting

In molti casi analizzati, i malware sono stati inseriti come allegati all'interno di conversazioni realmente avvenute tra la vittima e un interlocutore noto. All'atto pratico, la vittima riceve una risposta ad un messaggio già scambiato, oppure un nuovo messaggio da una controparte nota, e il messaggio contiene un allegato malevolo. Questo modus operandi mira ad aumentare la fiducia della vittima nei confronti dell'allegato ricevuto, inducendolo ad aprire il file senza porsi troppe domande. Le campagne che hanno diffuso il malware Ursnif [14] [16] hanno fatto largo uso di tale espediente.

Il nuovo modus operandi è da mettere probabilmente in relazione con le numerose campagne di attacco che oltre a credenziali di siti bancari hanno ricercato credenziali di accesso a sistemi di posta elettronica, un'attività apparentemente anomala per un banking trojan. Tra queste ricordiamo due campagne Ursnif/Gozi, una a Luglio [7] [8] e una a Novembre [14] [16], entrambi verso utenti italiani, DanaBot a Novembre verso vittime in Italia [12], e infine quella GootKit a Dicembre.
La pubblicazione a Gennaio 2019 di #Collection1, una raccolta con oltre 700 milioni di indirizzi email e decine di milioni di password, non può che accrescere questo fenomeno, con evoluzioni negative anche nel dominio degli attacchi *BEC*, o Business Email Compromise. [18] [19]

Anno nuovo, modus operandi nuovo

Una nuova tattica è emersa nella seconda parte del 2018. In almeno due campagne studiate da IBM Security, i malware sono stati usati per seguire e osservare le attività online della vittima senza alcun intervento, lasciandogli effettuare il login e la navigazione all'interno del sito bancario, intervenendo però con webinject al momento dell'effettiva operazione dispositiva, sostituendo le coordinate bancarie del beneficiario.
I webinject permettono di alterare ciò che viene visualizzato all'interno del browser. In questo modus operandi i webinject mostrano a video le coordinate bancarie del destinatario, ma all'invio della transazione passano al sito bancario altre coordinate bancarie. La frode diventa trasparente nei confronti della banca, e difficile da individuare per l'utente non attento. La vittima inserisce anche il secondo fattore di autenticazione (solitamente inviato via SMS), e riceve poi segnalazione della avvenuta transazione con l'importo effettivamente immesso, che vede tra le operazioni effettuate. Quello che un occhio attento non nota però è che le coordinate del beneficiario sono state sostituite con altre coordinate di pagamento, spesso appartenenti ad un money mule, oppure a conti controllati dagli attaccanti e usati per far transitare le somme.
Hanno operato così dapprima TrickBot nella campagna di Febbraio [3] che colpisce una piattaforma a supporto delle cripto-valute. Poi è la volta della campagna Ramnit che ad Agosto ha colpito utenti nel Regno Unito. Infine troviamo le stesse modalità operative anche nelle campagne di BackSwap a Settembre in Spagna [10] e a Novembre in Repubblica Ceca. In tutti i casi analizzati, webinject manipolano il contenuto dello schermo per mostrare il beneficiario desiderato dalla vittima, per poi passare al server della banca coordinate di pagamento diverse.

Ritorno ai webinject

Se il 2017 era stato, anche per l'Italia, l'anno dei temuti redirection attacks di cui avevamo parlato nel rapporto CLUSIT 2018 [1], nel 2018 abbiamo visto un passo indietro da parte di molti malware ai webinject.
Lidea alla base dei redirection attack è di dirottare il traffico della vittima verso siti replica, attraverso questi catturare le credenziali di accesso, per poi riutilizzarle per accedere al vero

sito di banking, attraverso un'altra sessione parallela controllata dai cyber criminali. In questo secondo accesso, da parte dei cyber criminali, la precisione è chirurgica, con una percentuale di successo molto alta. Durante l'intera sessione la vittima è tenuta appositamente lontana dal sito della banca, per portare la vittima a rivelare tutte le informazioni critiche per il log in senza che la banca si accorga che l'account del suo cliente è stato compromesso. Per preparare un tale attacco i cyber criminali creano dapprima un sito replica, molto fedele, della banca. Quando il sito replica è pronto, il trojan dirotta tutte le richieste HTTP al nuovo indirizzo, senza che l'utente noti nulla di anomalo all'interno del suo browser. L'indirizzo che compare sulla barra del browser è quello corretto del sito di eBanking, ma la connessione sta avvenendo con il sito replica, non quello originale.
La tecnica dei redirection attack, sviluppatasi del corso del 2017, si è rivelata complessa da gestire, ed ha mostrato un apparente rallentamento nel corso del 2018.
Il malware TrickBot ha alternato tecniche di redirection attack a webinject nelle campagne 2018. GootKit è stato il primo malware a fare uso di questa tecnica in Italia, con una campagna contro sei banche italiane [20] nel 2017. Tuttavia, la campagna GootKit di Gennaio 2018 [2] torna ai webinject. Ancora, a Settembre la campagna GootKit verso Italia, Regno Unito, Francia, Olanda e Belgio si basa esclusivamente su webinject.

Sfruttamento della PowerShell di Windows

Per tutti gli amministratori di sistema la PowerShell è uno strumento incredibilmente versatile ed efficace per accedere a molte funzionalità di Windows. Parimenti, è uno strumento potente anche nelle mani dei cyber criminali.
I ricercatori di IRIS (IBM X-Force Incident Response and Intelligence Services) evidenziano un trend in ascesa nell'uso fraudolento della PowerShell [21], sulla scorta dei successi nell'utilizzo della PowerShell per iniettare il malware all'interno di processi Windows in esecuzione in memoria e senza la necessità di scaricare file in locale, evadendo molti degli antivirus. Inoltre le tecniche di encoding native della PowerShell, come la *base64-encoded*, permettono un migliore offuscamento del malware con minimo sforzo. Non da ultimo, essendo la PowerShell uno strumento di largo e frequente utilizzo in molte attività amministrative Windows, bloccarla porterebbe a conseguenze avverse.
Nel corso dell'anno la PowerShell è stata usata prevalentemente per eseguire VBAScript inseriti all'interno di file Office, allegati a mail di phishing. È stato così nelle campagne di spam [5] [6] che ad Aprile ha veicolato in Italia il malware Zeus Panda, la campagna Danabot di Novembre [12] e ancora in Italia con il malware Ursnif/Gozi [14] [16] a Ottobre e Novembre.

Applicazioni infette negli app store

Usare solo app scaricate da store ufficiali è certamente una pratica virtuosa, ma non risolve del tutto il problema. L'hanno ben imparato le vittime del malware Marcher, veicolato a Gennaio all'interno di app di gaming per Android, alla base di un attacco contro utenti di banche turche. Nel 2017 erano state oltre 400 le app infette con il malware BankBot,

caricate su Play Store [22], e rimosse solo dopo che migliaia di utenti ignari le avevano già installate e usate.
BankBot è un malware Android, inserito all'interno di applicazioni apparentemente legittime, e con capacità di controllare lo schermo attraverso overlay. Il malware rimane silente all'interno dell'applicazione infetta fino a che l'utente non lancia sullo smartphone una delle app per accedere ai servizi di banking. A questo punto BankBot, prende il controllo dello schermo per catturare le credenziali utente. I ricercatori di IBM X-Force hanno individuato sul Play Store, altre 20 app infette da BankBot [23].
Ma come fa il malware a finire su Play Store, raggirando i controlli di sicurezza? L'analisi delle app infette con BankBot ha accertato che tutto comincia con una applicazione benigna, nei casi analizzati un'app contenente video comici o tutorial di cucito, caricata sul Play Store. Dopo che un certo numero di utilizzatori hanno scaricato e installato l'app, si invia un aggiornamento che istruisce l'app a scaricare altro codice, questa volta contenente il malware, attraverso una connessione HTTP diretta, dall'app a un server Internet predisposto.
Sull'onda dei primi risultati allarmanti, l'analisi delle app caricate sugli store ufficiali è continuata, e a Luglio 2018 il team IBM X-Force ha individuato almeno altre 10 app apparentemente legittime [24], ma contenenti downloader per scaricare malware bancario Android da server di Command and Control.
Lo spostamento da app direttamente infette con il malware BankBot, ad applicazioni infette con downloader che poi scaricano aggiornamenti malevoli, può suggerire che i cyber criminali che hanno distribuito malware attraverso Play Store si siano spostati verso un modello di business di *downloader-as-a-service*, presumibilmente offerto anche ad altri gruppi cyber criminali. [24]
Ancora a Luglio, Google rimuove 145 app dal Play Store dopo aver scoperto che erano infette con file Windows malevoli. [25] La ragione di malware Windows all'interno di app Android non è stata mai chiarita, tuttavia queste app hanno raggiunto il risultato nefasto di aver raggirato i controlli automatici dello store. Prima della rimozione, alcune avevano superato le 1000 installazioni, e rating di 4 stelle.
A Novembre 2018 un report di ESET riporta la rimozione di 29 app dal Play Store, installate da circa 30000 utenti, dopo che era stato individuato all'interno del malware bancario. [26]

Furto di credenziali di piattaforme a supporto delle cripto-valute

La deriva di alcuni malware verso il furto di cripto-valuta, ha confermato un andamento iniziato nel 2017, e continuato per tutto il 2018. Oltre a Gootkit [2], anche TrickBot è alla base di campagne per il furto di cripto-valuta [3] nel corso nel 2018.
La vertiginosa crescita del bitcoin che nella fine del 2017 aveva toccato il suo picco massimo in oltre 19000 dollari e una rivalutazione nel corso dell'anno di oltre il 1000%, non era passata inosservata alle bande di cyber criminali che proprio da Settembre 2017 avevano cominciato a prendere di mira anche le piattaforme di scambio di cripto-valute.
Ormai tutti i principali malware, parallelamente agli obiettivi bancari, implementano tattiche per il furto di cripto-valuta.

Cosa aspettarci per il 2019

Da qualche anno il terreno delle frodi finanziare è dominato da gruppi criminali ben organizzati e strutturati, uscendo dal raggio d'azione dell'hacker solitario.
Affinché una frode produca un ritorno economico servono una concomitanza di elementi. Anzitutto la capacità tecnologica di costruire e mantenere un malware di alto livello, assieme alle competenze tecniche per aggiornarlo ogni qualvolta il malware viene identificato dalle soluzioni di advanced fraud protection già esistenti. Anche l'infrastruttura di Command-and-Control richiede mantenimento, congiuntamente alle componenti di anonimizzazione ed encryption del traffico di rete. Gli attacchi richiedono poi una conoscenza accurata dell'interfaccia o della applicazione di eBanking, con la localizzazione nella lingua del soggetto attaccato. Infine, per ogni attacco che ha successo, occorre una rete di spalloni digitali o *money mule* che facciano fluire la somma frodata di conto in conto, fino a renderne difficoltoso un eventuale recupero.

Nel corso del 2018 le reti cyber criminali hanno operato su tutti questi fattori, assieme a nuove scelte, apparentemente finalizzate a rendere l'attacco meno complesso e di conseguenza più profittevole.
Sono promettenti le soluzioni per la *fraud protection* che combinano numerosi indicatori di rischio per identificare la sessione sospetta prima che venga finalizzata la transazione. Fattori di autenticazione, apparentemente non visibili, come il device fingerprinting, la geolocalizzazione, l'IP reputation, la device reputation, i dati degli operatori di telefonia mobile (MNOs), possono contribuire in maniera sostanziale a verificare l'identità dell'utente. Alcune piattaforme di *threat intelligence* sono in grado di fornire già oggi molte di queste informazioni ad applicazioni di terze parti, attraverso API.
La password, come le abbiamo conosciute finora, sono destinate a un inesorabile declino a causa dei molteplici data breach. Il *Future of Identity Study 2018* [29] mostra che l'impronta digitale viene percepita come il metodo di autenticazione più sicuro. Tuttavia, anche nel caso della biometria, troviamo già documentate effrazioni o data breach, possibili schemi di attacco, e limitazioni.
La strada più promettente al momento è quella della *Multi-Factor Authentication* (MFA), o autenticazione a più fattori, nella quale si combinano più elementi di autenticazione per rendere più complessa la compromissione del sistema. I malware che nel corso del 2018 hanno implementato la cattura del secondo fattore di autenticazione (2FA) basato sull'SMS, assieme ai nuovi tool e librerie sviluppate appositamente per questa attività [28], ci invitano ad abbandonate anche dagli SMS quando prima.
Fortunatamente la MFA apre a scenari di autenticazione decisamente più robusti [29] e difficili da raggirare. Tra questi il password-less login basato sulla scansione di un QR Code appositamente creato di volta in volta. Oppure l'uso delle numerose app *authenticator*, con PIN di autenticazione che cambia continuamente nel tempo, associato al dispositivo biometrico del nostro smartphone, sia esso il lettore di impronte digitali, il riconoscimento facciale, o una semplice occhiata davanti al computer. Tale modalità porta con se l'ulteriore

vantaggio di mantenere le credenziali biometriche confinate all'interno del nostro dispositivo. Tra i meccanismi di autenticazione avanzata emerge il FIDO2, che standardizza l'uso dei dispositivi di autenticazione per l'accesso ai servizi online, sia in ambiente mobile che desktop.
La *User Behavior Analytics (UBA)* [30] o analisi comportamentale dell'utente, aggiunge un ulteriore elemento per il calcolo del valore di rischio della singola transazione, e mira ad individuare prontamente le azioni dei cyber criminali che cercano di impersonificare la vittima, autenticandosi con le sue credenziali. Lo fa analizzando una grande quantità di dati e informazioni sul comportamento online dell'utente, generati dai sistemi e dalla rete, e finora ignorati.
Questi elementi, disponibili già oggi, consentono di aggiungere contesto all'utente e al dispositivo usato nella transazione, e contribuire a misurare in maniera accurata il livello di rischio di ciascuna operazione.
Combinando tutti questi nuovi elementi che la tecnologia ci mette già a disposizione, la strada verso cui indirizzarsi è sicuramente quella del *context-based access,* o accesso basato sul contesto, che condiziona l'accesso alla valutazione dinamica del rischio della singola transazione, modulando eventuali azioni aggiuntive di verifica. [31] Le soluzioni di autenticazione e autorizzazione, sia nel caso di login che di disposizione di operazioni, non si limitano più ad autorizzare o bloccare un'operazione, ma offrono una gamma intermedia di possibilità, come ad esempio autorizzare un'operazione ma con dei limiti, oppure richiedere verifiche aggiuntive.
È indubbio che qualsiasi siano le soluzioni messe in campo dai fornitori di servizi finanziari, queste devono essere supportate da continua osservazione e ricerca dell'evoluzione delle tattiche di attacco. In un contesto mutevole come quello descritto, una soluzione non supportata da team di ricerca specializzati nell'analisi del malware, rischia di divenire presto obsoleta e inefficacie. Le soluzioni adottate devono altresì essere in grado di continue riconfigurazioni sulla base delle mutate forme di attacco. Ad esempio un SIEM deve adesso poter individuare utilizzi malevoli della PowerShell.

Indubbiamente, anche l'intelligenza artificiale e le capacità cognitive inserite all'interno delle singole soluzioni, saranno leve importanti nel campo della lotta al cybercrime nel settore finanziario.
L'uso dell'intelligenza artificiale nelle soluzioni di sicurezza offerte sul mercato si sta orientando su tre macro aree. Anzitutto nell'analisi predittiva con sistemi in grado di identificare autonomamente nuove frodi. C'à poi l'area della *intelligence consolidation*, che sfrutta le capacità di interpretazione del linguaggio naturale, analizzando e apprendendo dall'enorme quantità di informazioni, per lo più in forma non strutturata e prodotte continuamente nel campo della sicurezza. Security bulletins, report, grafici, conferenze, notizie di agenzia, tweet, advisories e altre fonti, che altrimenti rischierebbero di finire ignorate in quanto non fruibili dalle soluzioni di sicurezza finora usate. Infine, l'intelligenza artificiale si pone come trusted advisor a supporto del lavoro degli analisti umani, per una più veloce risposta alle

minacce e agli attacchi. Non quindi una tecnologia che sostituisce il security analyst, ma piuttosto una tecnologia a supporto del security analyst, di cui incrementa sensibilmente la produttività.
Fondamentale il ruolo dei Security Operation Center (SOC) e di tutte le figure che in essi operano, come i Security Analyst, i Security Manager e i Network Specialist. A queste figure, con ruoli diversi, sono demandati i compiti controllo e investigazione sulle minacce, attacchi e vulnerabilità che colpiscono l'organizzazione, la sua infrastruttura, le applicazioni e i dati. Il Security Analyst parte dagli allarmi generati a fronte di attività anomale e dalle osservazioni sui log file, ne verifica le potenziali minacce e in pochi minuti deve decidere se procedere con l'investigazione e la difesa, oppure archiviare il caso e passare ad analizzare la successiva minaccia.
La velocità con cui gli attacchi prendono di mira le organizzazioni, la crescente complessità, le tecniche di offuscamento e la moltitudine di sistemi e applicazione, l'automazione, lasciano pochissimo tempo per analizzare il singolo evento, valutarlo e prendere una decisione ponderata.

In questo contesto una *piattaforma di Threat Intelligence* è lo strumento fondamentale per l'investigazione degli eventi di sicurezza, consentendo di verificare e confrontare allarmi, log, file binari, con una fonte autorevole e aggiornata, con lo scopo di confermare o escludere una potenziale minaccia. Inoltre la piattaforma di Threat Intelligence permette la condivisione di informazioni tra membri dello stesso team, oppure all'interno di team estesi accomunati dalla stessa necessità investigativa. La piattaforma di intelligence deve poter essere facilmente interfacciabile alle soluzioni cliente, ad esempio attraverso API, per portare le capacità di detection all'interno della singola soluzione. E la base di conoscenza della threat intelligence deve essere costantemente aggiornata e seguire le nuove minacce, attraverso un aggiornamento continuo degli indicatori di compromissione (IOC) estratti dalle minacce.
La ricerca futura sui pattern di adozione e di abuso dei meccanismi di autenticazione rappresenta un punto sostanziale per la costruzione di tecnologia pragmatica e costruita attorno all'utente.

Bibliografia

[1] AA. VV. *Rapporto CLUSIT 2018 sulla sicurezza ICT in Italia* CLUSIT, Marzo 2018
[2] Limor Kessem *GootKit Malvertising Brings Redirection Attacks to Italian Banks* SecurityIntelligence.com, Maggio 2017 https://securityintelligence.com/gootkit-malvertising-brings-redirection-attacks-to-italian-banks/
[3] O. Harpaz *TrickBot's Cryptocurrency Hunger: Tricking the Bitcoin Out of* Wallets SecurityIntelligence.com, Febbraio 2018 https://securityintelligence.com/trickbots-cryptocurrency-hunger-tricking-the-bitcoin-out-of-wallets
[4] H. Barc *Backswap malware analysis* CERT.PL, Giugno 2018 https://www.cert.pl/en/news/single/backswap-malware-analysis/
[5] *Campagna di diffusione del malware Zeus Panda tramite allegati Excel* CERT-PA, Aprile 2018
[6] *Nuova ondata di malspam su territorio* Italiano CERT-PA, Aprile 2018
[7] *Continua la campagna Ursnif veicolata in Italia* CERT-PA, Giugno 2018 https://www.cert-pa.it/notizie/continua-la-campagna-ursnif-veicolata-in-italia/
[8] *Campagna Ursnif italiana* CERT-PA, Luglio 2018
[9] *Kronos Reborn* Proofpoint, Luglio 2018
[10] Limor Kessem *BackSwap Malware Now Targets Six Banks in Spain* SecurityIntelligence.com, Agosto 2018 https://securityintelligence.com/backswap-malware-now-targets-six-banks-in-spain/
[11] AA. VV. *Rapporto CLUSIT 2017 sulla sicurezza ICT in Italia* CLUSIT, Marzo 2017
[12] *Campagna di Malspam diffonde il Trojan Danabot anche in Italia* CERT-PA, Novembre 2018
[13] *Falsa Mail diffonde Trojan DanaBot* TG Soft, Novembre 2018 https://www.tgsoft.it/italy/news_archivio.asp?id=966
[14] *Nuova campagna di Malspam Italiana volta a distribuire il malware Ursnif* CERT-PA, Novembre 2018
[15] *Public collection*: *Phishing campaigns affecting Italian* organisations XForce Exchange, Agosto 2018
[16] *Public collection: Phishing Campaign uses Hijacked Emails to Deliver URSNIF by Replying to Ongoing Threads* XForce Exchange, Ottobre 2018
[17] *Malspam Gootkit con dropper da 450+ MB* d3lab, Dicembre 2018
[18] Pier Luigi Rotondo *IBM X-Force: un passo avanti nella difesa dagli attacchi finanziari più evoluti* IBM thinkMagazine, Febbraio 2018 https://ibm.biz/pierluigirotondo
[19] Andrea Frollà *Cybercrime, Ibm lancia l'allarme contro le frodi B2B via e-mail* Repubblica, Marzo 2018
[20] Limor Kessem *GootKit Malvertising Brings Redirection Attacks to Italian Banks* SecurityIntelligence.com, Maggio 2017 https://securityintelligence.com/gootkit-malvertising-brings-redirection-attacks-to-italian-banks/

[21] Camille Singleton *An Increase in PowerShell Attacks: Observations From IBM X-Force IRIS* SecurityIntelligence.com, Ottobre 2018 https://securityintelligence.com/an-increase-in-powershell-attacks-observations-from-ibm-x-force-iris/
[22] T. Seals Hundreds of Google Play Apps Infected with the BankBot Trojan infosecurity magazine, Aprile 2017 https://www.infosecurity-magazine.com/news/hundreds-of-google-play-apps/
[23] Limor Kessem After Big Takedown Efforts, 20 More BankBot Mobile Malware Apps Make It Into Google Play SecurityIntelligence.com, Luglio 2017 https://securityintelligence.com/after-big-takedown-efforts-20-more-bankbot-mobile-malware-apps-make-it-into-google-play/
[24] S. Gritzman *Anubis Strikes Again: Mobile Malware Continues to Plague Users in Official App Stores* SecurityIntelligence.com, Agosto 2018 https://securityintelligence.com/anubis-strikes-again-mobile-malware-continues-to-plague-users-in-official-app-stores/
[25] *Mobile App Security Threat Forces Google Play Store to Remove 145 Android Apps* SecurityIntelligence.com, Agosto 2018 https://securityintelligence.com/news/mobile-app-security-threat-forces-google-play-store-to-remove-145-android-apps/
[26] *30000 Android Users Infected With Banking Malware From 29 Bogus Apps* SecurityIntelligence.com, Novembre 2018 https://securityintelligence.com/news/30000-android-users-infected-with-banking-malware-from-29-bogus-apps/
[27] *IBM Future of Identity Study* IBM Security, January 2018 https://ibm.biz/FutureOfIdentity
[28] *New Reverse Proxy Tool Can Bypass Two-Factor Authentication and Automate Phishing Attacks* SecurityIntelligence.com, Gennaio 2019
[29] Pier Luigi Rotondo *Multifactor Authentication Delivers the Convenience and Security Online Shoppers Demand* SecurityIntelligence.com, Gennaio 2019 https://securityintelligence.com/multifactor-authentication-delivers-the-convenience-and-security-online-shoppers-demand/
[30] T. Obremski *Take a Dive: Deep Network Insights for Deeper Analytics* SecurityIntelligence.com, Dicembre 2017 https://securityintelligence.com/take-a-dive-deep-network-insights-for-deeper-analytics/
[31] Pier Luigi Rotondo *Acquisti online? Ecco come farli in modo sempre più sicuro* IBM thinkMagazine, Dicembre 2018 https://ibm.biz/ibmblackfriday

Analisi del cybercrime finanziario in Italia nel 2018

[A cura di Luigi Rocco, Communication Valley Reply]

Nell'anno 2018, analizzando caratteristiche ed evoluzione degli attacchi di maggiore rilievo, abbiamo avuto conferma del trend in forte espansione delle attività legate al cybercrime in ambito finanziario già registrato nel precedente anno. I dati che seguono sono il frutto del monitoraggio, da parte del Cyber Security Operation Center (CSOC) di Communication Valley Reply, dei fenomeni fraudolenti che abbiamo dovuto gestire per conto di alcune delle principali realtà bancarie italiane. Gli attacchi osservati possono essere suddivisi in attacchi di ingegneria sociale (phishing) e attacchi tramite malware, così come verranno approfonditi nel corso del capitolo.

Attacchi di ingegneria sociale (Phishing)

Analisi e diffusione del fenomeno

Il phishing [1] è un fenomeno che attraverso tecniche di ingegneria sociale, cioè imitando per aspetto e contenuti i messaggi legittimi di fornitori di servizi, richiede di fornire informazioni riservate come il numero della carta di credito o le credenziali d'accesso. Il livello di verosimiglianza dei messaggi che vengono inviati è così elevato che sta diventando sempre più difficile per l'utente medio notare la differenza tra le mail mandate in una campagna di phishing e le email inviate legittimamente dai comuni servizi on-line.

In **Figura 1** viene mostrata la percentuale di traffico di phishing identificata durante tutto l'anno 2018 [2].

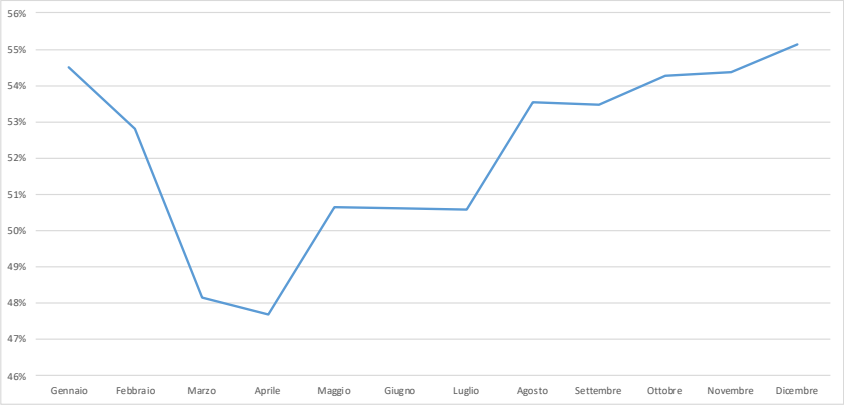


Figura 1 - *Distribuzione traffico di phishing rispetto al traffico mail globale*

Rispetto al 2017 la situazione non è variata più di tanto infatti è possibile notare che i picchi si evidenziano all'inizio e sul finire dell'anno.
L'andamento dei casi di phishing rilevati e gestiti nell'ambito bancario durante il 2018 risulta coerente con l'andamento appena evidenziato, con il 40% circa dei casi totali gestiti a inizio e metà anno, rispettivamente a gennaio ed agosto (**Figura 2**).

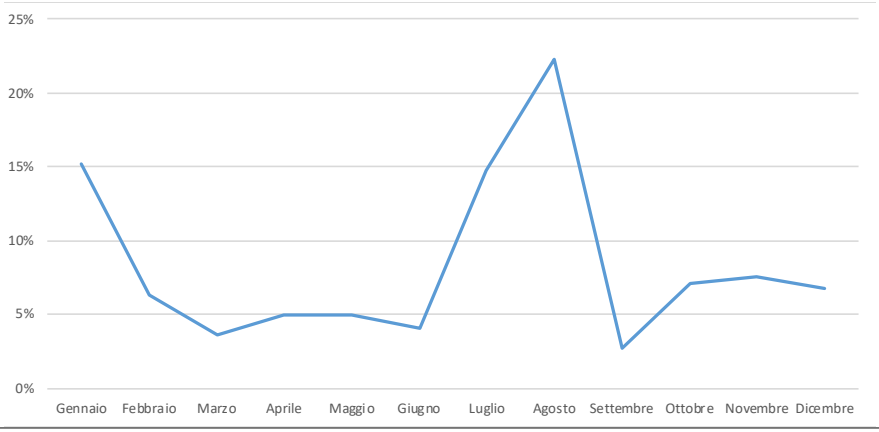


Figura 2 - *Distribuzione percentuale mensile dei casi di phishing rispetto al totale annuale*

Interessante notare come la metà dei siti di phishing relativi all'ambito bancario italiano fosse ospitato su server localizzati negli Stati Uniti (50,2%), mentre i rimanenti siti di phishing sono stati localizzati principalmente in paesi europei, in particolare in Germania il 17,4% dei casi e in Italia il 7,7% dei casi (**Figura 3**).

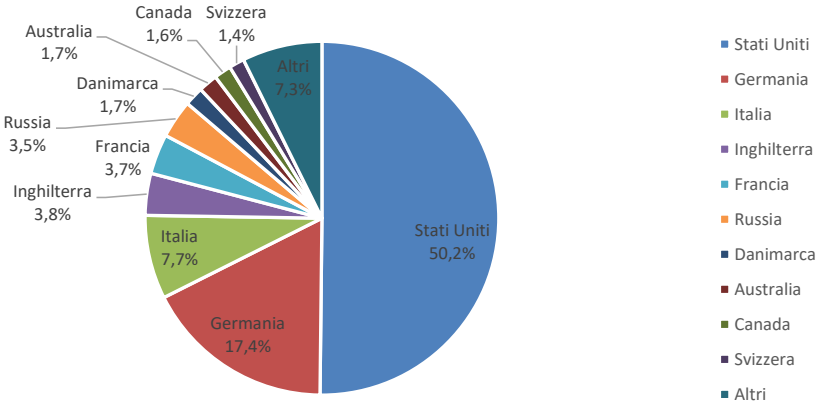


Figura 3 - *Localizzazione siti di phishing per paese*

I contesti aziendali principalmente colpiti dalle email di phishing sono ancora una volta quelli relativi al settore dei pagamenti, in netta crescita rispetto all'anno precedente con il 36,7% delle email di phishing individuate (+20% circa), seguito da quello bancario con il 25,6% al pari dei livelli dell'anno precedente. Il movente per le violazioni di questi tipi di account rimane sicuramente il ritorno finanziario immediato. Seguono i servizi online, in particolare quelli di webmail, con l'11,3% e in leggera diminuzione rispetto all'anno precedente (-7% circa), e poi i servizi di storage su cloud, al 9,9% di email di phishing, e social network, allo stesso livello dell'anno sorso con il 5,3%. Il totale degli altri contesti colpiti dal phishing ammonta all'11,31% e include un incremento rilevante di attacchi contro aziende in settori critici a livello nazionale, in particolare quello energetico [3].

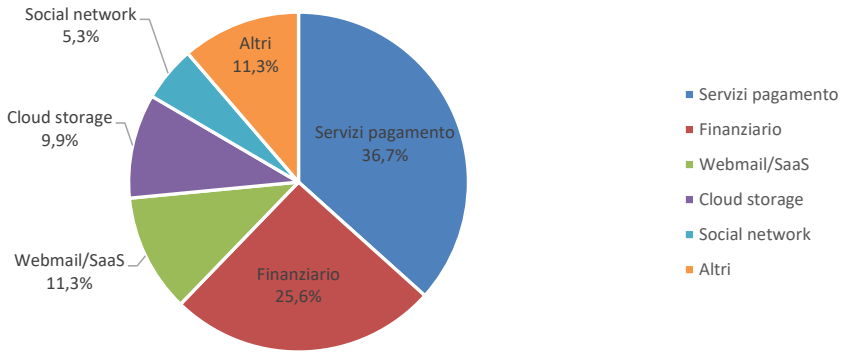


Figura 4 - *Distribuzione delle mail di phishing, suddivise per tematica trattata.*

Le principali campagne di Phishing rilevate

Gli esempi pratici di analisi di campagne di phishing che sono presentati in questa sezione illustrano le due strategie maggiormente utilizzate nel corso del 2018 e riguardano campagne ancora in corso al momento della stesura del presente documento.

Lo scopo finale delle campagne di phishing presentate di seguito può essere duplice. In un primo caso lo scopo del *phisher* è quello di prendere il controllo del computer dell'utente vittima attraverso l'uso di un *malware*, un programma informatico usato dai cyber-criminali solitamente per entrare in possesso di informazioni sensibili, accedere a sistemi informatici privati. Le email costituiscono il mezzo di diffusione principale dei malware, motivata dal fatto che è necessario fornire un contesto credibile che riesca a convincere l'utente ad eseguire software malevolo sul proprio host. Quando la campagna di phishing viene utilizzata come vettore per la diffusione di malware, si parla di campagna di *malspam*, che consiste proprio in una campagna di email di spam per infettare le postazioni degli utenti ignari.

Durante l'intero anno sono state osservate alcune varianti di una campagna di malspam particolarmente insistente e finalizzata alla diffusione di diverse tipologie di malware – da GootKit a Ursnif – che per attirare l'attenzione dei destinatari utilizza contenuti giuridici con riferimento a finte relazioni di sentenze inviate da falsi avvocati. L'oggetto delle email di questa campagna, abbastanza caratteristico e riconoscibile, è simile ai seguenti esempi:

- Relazione di notifica decreto N.718171323228 Del 14/03/18
- Relazione di notifica decreto #73708789094 Del 15/03/18
- Relata di notifica atto N°7164194125 Del 13/04/2018
- Relazione di notifica sentenza No.03499363993 Del 23/03/2018

Un esempio di mail riconducibile a questo caso è quello rappresentato, opportunamente anonimizzato, in **Figura** 5. Si può notare che la mail prende di mira utenti italiani e, come numerosi casi simili riscontrati durante l'anno in diverse campagne, simula proprio l'invio di notifiche di atti giudiziari.

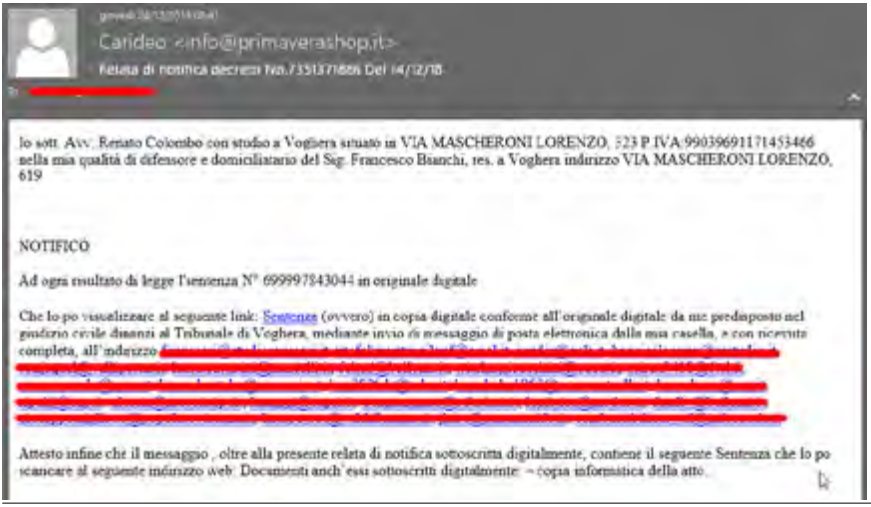


Figura 5
Esempio di email relativa ad una campagna di phishing condotta attraverso link malevoli.

Differentemente dalle campagne osservate a inizio anno, nei casi più recenti della campagna appena descritta il link presente nell'email punta ad un file PDF disponibile su Google Drive. L'alta efficacia di questo tipo di attacco è dovuta alla facilità di predisposizione di questa modalità di condivisione di contenuti malevoli e all'alta probabilità che la mail superi i controlli dei filtri di posta, destando pochi sospetti negli utenti più incauti.
Nel file PDF su Google Drive è presente un ulteriore link che avvia il download di un archivio per l'installazione del malware.

Nella prima metà dell'anno sono state registrate ripetute campagne di diffusione del malware bancario Zeus/Panda, con le seguenti caratteristiche:

- finta notifica DHL con un link a fattura [4]
- conferma di un ordine generico con allegato un file Excel (in formato ".xls") [5]

Nella seconda metà dell'anno si sono invece registrate numerose campagne per la diffusione del malware bancario Ursnif. Una prima variante della campagna includeva generici riferimenti a fatture e in questi casi la mail di phishing non conteneva link ma rimandava a un file allegato, come mostrato in **Figura 6**. Si tratta di un documento Word (in altri sample vengono utilizzati anche file Excel) che, se aperto, presenta un messaggio di errore e invita l'utente ad attivare l'esecuzione delle macro per poter procedere alla lettura del documento (**Figura 7**).

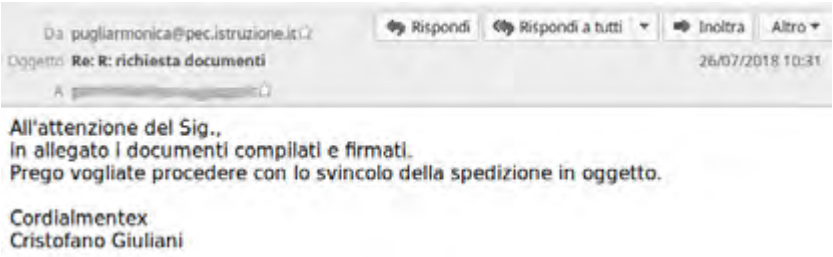


Figura 6
Esempio di mail relativa ad una campagna di phishing condotta attraverso file allegato.

Figura 7
File Word allegato alla mail di phishing con invito all'utente per l'abilitazione dei contenuti

L'abilitazione dei contenuti da parte dell'utente comporta l'esecuzione delle macro configurate nel foglio Excel, che subdolamente avvia una connessione a un server remoto compromesso per effettuare il download di un eseguibile. Il file scaricato è il malware vero e proprio che viene eseguito, sempre dalla macro e attraverso l'uso di PowerShell, sull'host ormai infetto. Dalle analisi condotte il malware utilizzato risulta un esemplare della famiglia Ursnif. Gli utenti che vengono infettati da questa tipologia di malware solitamente non si accorgono di esserlo in quanto non riscontrano alcuna anomalia nel normale funzionamento del proprio PC. In realtà, il malware resta in attesa che l'utente visiti il sito web dell'home banking e si attiva solo in questo caso, raccogliendo informazioni sensibili come le credenziali d'accesso per poi inviarle in remoto ai cyber-criminali.

Numerosi casi relativi alle campagne osservate durante l'anno appena trascorso e aventi come obiettivo solo l'Italia, erano veicolati via PEC e cioè un canale normalmente considerato affidabile (come si può osservare sempre nell'email in

Negli ultimissimi mesi dell'anno sono state rilevate anche campagne di phishing mirate alla diffusione dei malware bancari GootKit e Danabot, con riferimento a ipotetici "Processi di Fatturazione". In base ad una ricerca condotta su campo internazionale [6], le strade delle due famiglie di malware, e ovviamente delle organizzazioni criminali alle loro spalle, si sono incrociate facendo in modo che Danabot, oltre che come trojan bancario, venga utilizzato nella catena di infezione sfruttando gli account webmail compromessi per la distribuzione di malware, puntando proprio a un modulo di download di *GootKit*.

Oltre che per la diffusione di malware, le campagne di phishing vengono messe in atto anche per il furto di dati sensibili dei malcapitati utenti, ad esempio informazioni personali e credenziali di acceso ai portali di home banking.
In tal senso una campagna di phishing particolarmente strutturata si è sviluppata nella prima metà dell'anno, provando a ingannare l'utente con un riferimento ad un finto rimborso INPS. La campagna era organizzata in modo da raccogliere prima i dati personali dell'utente vittima – codice fiscale e numero di telefono, mediante la pagina mostrata in **Figura 8** – e successivamente invitando l'utente a selezionare la propria banca – tramite cui ottenere il rimborso, come mostrato in **Figura 9** – prima di reindirizzarlo al finto sito web dei numerosi istituti bancari coinvolti per il furto vero e proprio delle credenziali di login.

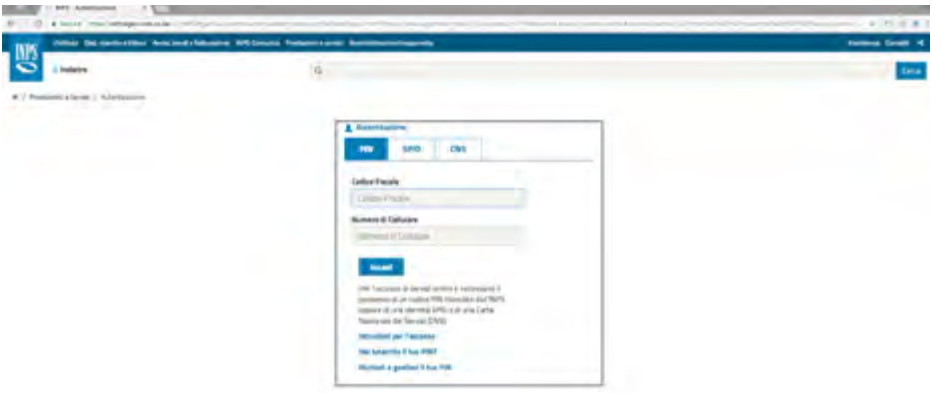


Figura 8 - *Campagna phishing finto rimborso INPS – Fase 1*

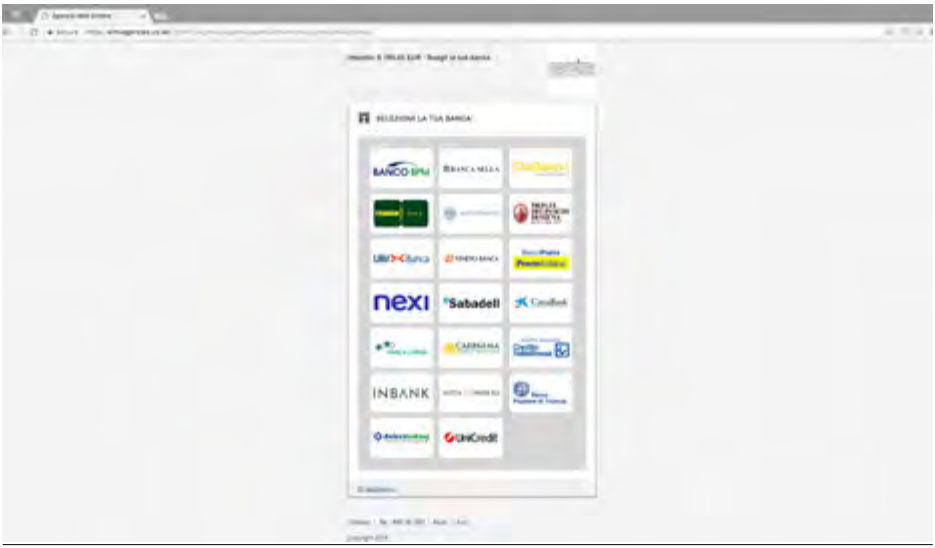


Figura 9 - *Campagna phishing finto rimborso INPS – Fase 2*

Attacchi tramite malware

Le modalità di attacco da parte dei malware bancari rimane quella di tipo Man-in-the-browser, mediante injection di codice malevolo all'interno delle pagine web dei portali di home banking. La web injection può essere effettuata sulla pagina di login, allo scopo di rubare le credenziali di accesso al portale, oppure nelle sezioni interne del portale di home banking per commettere la frode vera e propria. In quest'ultimo caso il malware si interpone nel processo di richiesta di disposizioni bancarie da parte dell'utente in modo da reindirizzarle ingannevolmente verso conti bancari legati alle organizzazioni cyber-criminali.
Basandosi sui comportamenti manifestati dai malware identificati sul campo, il malware si interpone come un proxy nelle comunicazioni tra l'host infettato e il server della banca.

Quando l'utente visita l'home banking della propria banca il malware si attiva e resta in attesa che l'utente si posizioni nella pagina di login o di esecuzione dei bonifici. Appena il malware riesce ad entrare in possesso di una sessione valida tra il cliente e il portale della banca allora inizia la procedura per eseguire una frode mediante due possibili tecniche. In un primo caso il bonifico viene fatto partire in maniera automatizzata e in modo trasparente all'utente non appena quest'ultimo esegue il login sul portale della banca; di solito il bonifico necessita di un codice OTP per poter essere inviato quindi il malware richiede, mediante una tecnica di *socia engineering*, un secondo codice OTP durante la procedura di autenticazione.
Nel secondo caso l'operazione di bonifico iniziata da un cliente della banca viene intercettata dal malware e il destinatario viene modificato prima di inviare la richiesta al server della banca senza che l'utente se ne renda conto. Il cliente rimane ignaro di quanto accaduto poiché il malware altera la struttura grafica delle sezioni interne del portale della banca per nascondere il bonifico fraudolento, ad esempio nelle pagine di conferma e successivo resoconto delle disposizioni effettuate. In alcuni casi il malware blocca le connessioni al provider di posta elettronica sul computer della vittima e rimuove ogni riferimento a numeri o chat di assistenza sul sito web della banca; in questo modo il malware ha più tempo a disposizione prima che la vittima riesca a contattare la banca per segnalare anomalie e bloccare la transazione fraudolenta.
Durante l'analisi dei casi riscontrati nell'anno appena passato, è stato possibile osservare anche nuoci comportamenti che forzavano l'utente a eseguire alcune operazioni manualmente, ad esempio per la compilazione dei dati del destinatario del bonifico, o a impedire ulteriori bonifici in seguito a frodi già messe a segno per lo stesso utente, probabilmente al fine di non destare particolare attenzione eseguendo ulteriori operazioni fraudolente e riconducendo il tutto a un malfunzionamento del portale.

Dalle attività fraudolente rilevate durante il 2018 [7] in ambito bancario italiano, emergono le seguenti considerazioni:

- La grande famiglia dei malware derivati da Zeus continua ad essere fortemente rappresentata nel panorama dei malware bancari, anche per quanto riguarda lo scenario italiano.

- Panda Banker, appartenente alla famiglia Zeus, conferma la predizione fatte durante l'anno passato infatti si sta confermando particolarmente presente in Italia. L'andamento è previsto in crescita per il 2019, soprattutto considerando gli istituti finanziari di numerosi paesi bersagliati dal malware e le modalità di diffusione (i) via campagne di malspam e (ii) per la recente evoluzione di altri malware bancari modulari utilizzati proprio per la diffusione di questa famiglia di malware [8].
- Durante il corso dell'anno 2018 vi è stato un ritorno della minaccia Emotet. Come predetto durante il 2017, il malware è arrivato a bersagliare anche gli istituti bancari italiani e, considerate anche la sua evoluzione a malware per la distribuzione di altri malware bancari [8], è previsto in crescita per l'anno 2019 [9].
- Ursnif, una variante di Gozi, si è aggiunta alle varianti già note e il suo andamento ha avuto un picco nei primi mesi del 2018 e nel mese di settembre. Non si evidenziano particolari tendenze di incremento del fenomeno.

Sul finire dell'anno si è assistito a numerosi attacchi condotti tramite il trojan bancario Danabot, che ha avuto come obiettivo le banche di alcuni paesi tra cui l'Italia. Il principale vettore di infezione rimane l'email di phishing, con i soliti riferimenti a false fatture e l'invito a cliccare su link che reindirizzano a siti per il download del dropper del malware.
Danabot ha avuto molteplici banche italiane come obiettivo, ma anche numerosi provider di webmail tra i più noti. Infatti il malware è stato progettato con funzionalità avanzate ed estese anche ad altri contesti oltre quello bancario, proprio come quello delle webmail, al fine di raccogliere indirizzi email e incrementare la sua diffusione inviando massivamente messaggi di spam tramite le webmail delle vittime.
La modalità di attacco del malware consiste ancora una volta nella tecnica dell'injection di codice malevolo all'interno di una pagina web, ad esempio quella di login al servizio di posta elettronica della vittima. Questa tecnica permette di raccogliere gli indirizzi e-mail contenuti negli account compromessi delle vittime e inviare i dati raccolti al server C&C dell'attaccante. In alcuni casi è stato possibile osservare come i messaggi di spam venissero inviati come risposta a messaggi già ricevuti dall'utente vittima, in modo da rendere l'email più veritiera e aumentare l'efficacia della campagna di infezione.

Conclusioni

Dai casi descritti è evidente come i trojan bancari siano sempre in cima alla lista delle minacce informatiche, risultando il principale payload nelle campagne di diffusione tramite email e, come spesso annunciato durante il corso dell'anno dai principali provider di soluzioni per la sicurezza degli endpoint, avendo superato anche la categoria dei ransomware.

Il trend particolarmente allarmante a cui si è assistito durante l'intero anno è stato quello dell'ampliamento degli obiettivi dei malware per il furto di credenziali, soprattutto nel caso di malware appartenenti a famiglie già note e storicamente indirizzate solo al contesto dei servizi finanziari. Numerosi casi analizzati hanno infatti dimostrato come diversi campioni

in diverse campagne avessero come obiettivo i principali email provider, i sistemi di pagamento elettronico e diversi altri portali che non rientravano nell'ambito finanziario. In uno scenario europeo e mondiale di costante digitalizzazione dei sistemi e dei servizi, non si esclude che la situazione potrebbe ulteriormente aggravarsi con le organizzazioni cybercriminali che potrebbero prendere di mira le credenziali di numerosi altri sistemi per l'accesso a dati sensibili.
Come anticipato lo scorso anno, le organizzazioni criminali continuano ad alimentare il mercato del malware-as-a-service con configurazioni per il furto di credenziali e attuazioni di frodi altamente personalizzate su specifici istituti bancari. Si è assistito anche a una sempre più complessa strategia organizzativa che spesso confluisce in un sodalizio criminale tra i principali attori alla regia di questi attacchi che sempre più spesso condividono obiettivi, infrastrutture, strumenti e procedure operative di infezione e di attacco.

In definitiva, i malware per il furto di credenziali rimangono e si prospettano come una minaccia che non va assolutamente sottostimata, in ambito finanziario così come in tutti gli altri contesti in cui una le sole credenziali di autenticazione sono sufficienti ad accedere a dati sensibili e sistemi di rilevanza strategica.

Riferimenti

[1] Phishing, https://en.wikipedia.org/wiki/Phishing
[2] Fonte Cyber Security Operation Center (CSOC) di Communication Valley Reply
[3] Fonte CERT Nazionale italiano, *Il malware "AVE_MARIA" diffuso in campagna di phishing ai danni di un'azienda italiana*, https://www.certnazionale.it/news/2019/01/14/il-malware-ave_maria-diffuso-in-campagna-di-phishing-ai-danni-di-unazienda-italiana/
[4] Fonte CERT-PA, *Phishing: Finta notifica da parte di DHL*, https://www.cert-pa.it/notizie/phishing-finta-notifica-da-parte-di-dhl/
[5] Fonte CERT-PA, *Campagna di diffusione del malware Zeus Panda tramite allegati Excel*, https://www.cert-pa.it/notizie/campagna-di-diffusione-del-malware-zeus-panda-tramite-allegati-excel/
[6] https://www.welivesecurity.com/2018/12/06/danabot-evolves-beyond-banking-trojan-new-spam/
[7] Fonte CERTFin, a cura di Communication Valley Reply, *Bollettino Mensile sugli Attacchi Informatici*, Dicembre 2018
[8] Fonte malware-traffic-analysis.net, *Emotet malspam infections from 2018-08-13 and 2018-08-14*, https://www.malware-traffic-analysis.net/2018/08/14/index2.html
[9] Fonte abuse.ch, *How to takedown 100,000 malware sites*, https://abuse.ch/blog/how-to-takedown-100000-malware-sites/

Sviluppo di un sistema di *cyber threat intelligence*

[A cura di Pasquale Digregorio e Boris Giannetto, CERT Banca d'Italia][1]

Introduzione

Negli ultimi anni si è assistito ad un considerevole intensificarsi della minaccia *cyber*. Tale fenomeno è legato al crescente sfruttamento delle opportunità offerte dal cyberspazio (abbattimento dei limiti spazio-temporali; minori costi, rischi ed effetti collaterali) per il raggiungimento di scopi politici, militari ed economici da parte di attori diversificati (dagli Stati al *netizen*, da organismi di *intelligence* a società private, fino alla criminalità organizzata). Si assiste, inoltre, ad una rapida evoluzione del grado di sofisticazione dei vettori d'attacco. A livello globale, i *cyber*-attacchi diretti contro le Istituzioni finanziarie sono in aumento: per averne evidenza, basta consultare rapporti di fonti autorevoli come WEF, EUROPOL e FMI. La strutturazione, la velocità, il meta-polimorfismo di questi attacchi rendono necessario un cambio di paradigma: occorre passare da un approccio classico incentrato sul *risk management* ad una *posture* basata su una gestione preventiva della minaccia.

A tal riguardo, una condizione di rischio zero non è perseguibile: in questo ambito - considerando l'attuale scenario, caratterizzato da un alto grado di interconnessione tra minacce di varia natura - un approccio basato sulla stima della probabilità del rischio può risultare poco accurato e inefficace. Per converso, di certa utilità appare il consolidamento di un apparato di *cyber threat intelligence* (CTI), complementare rispetto ai classici presìdi di sicurezza informatica.

Contesto

La *cyber threat intelligence* è la disciplina che si occupa di raccogliere e analizzare dati eterogenei - provenienti da diverse sorgenti informative interne ed esterne -per estrarre informazioni utili a conoscere le caratteristiche dell'attore della minaccia, in modo da poter attribuire un profilo di rischio specifico per i propri *asset* e sviluppare azioni di contrasto efficaci.

In particolare, le attività di CTI si esplicano attraverso un processo di raccolta, classificazione, integrazione e analisi di dati grezzi relativi a minacce che operano nel cyberspazio. Tale processo è finalizzato alla produzione di informazioni utili per la *constituency*, per mezzo di investigazioni su: attori della minaccia, possibili reali motivazioni, connessioni tra *cluster* di eventi, tecniche, tattiche e procedure (TTP) impiegate dall'attaccante.

Nell'attuale scenario internazionale, gli attacchi più strutturati afferiscono a fenomeni diversificati quali *cybercrime*, *cyberterrorism*, *state-sponsored APT* (*Advanced Persistent Threats*) e *cyberwarfare* interstatuale.

[1] [Le opinioni sono espresse a titolo personale e non impegnano la responsabilità dell'Istituto].

Figura 1 - *Rappresentazione dei principali cluster di APT divisi per paese (attribuzioni ritenute maggiormente plausibili)*

In questo quadro, la sola analisi tecnica di un attacco *cyber* non è efficace, data la limitatezza e la volatilità delle evidenze digitali disponibili *ex post*, le peculiarità del cyberspazio e le tecniche di anonimizzazione, offuscamento ed *antiforensics* sviluppate dai principali attori della minaccia. Inoltre, non sono inusuali in questo contesto *false flags operations*, condotte attraverso l'acquisizione e l'utilizzo di artefatti notoriamente ricondotti a terze parti, sulle quali si vuole artatamente veicolare l'attribuzione di un attacco.

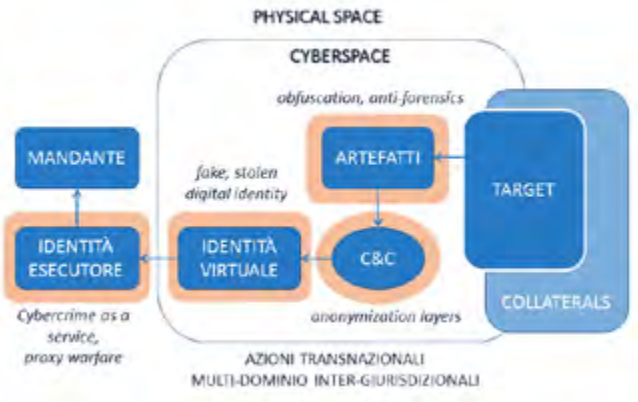


Figura 2 - *Disambiguazione tra prove acquisite nel cyberspazio ed identità del mondo fisico*

Le difficoltà di attribuzione suesposte si traducono sovente in una condizione di *plausible deniability*. Questo rende l'impiego del cyberspazio particolarmente profittevole anche per attività di *warfare*.
Per mitigare l'incertezza relativa all'*attribution*, le principali analisi di CTI svolte su scala globale fanno riferimento in prima istanza a nomi convenzionali, a partire dai quali è talvolta possibile identificare relazioni con gli attori reali, come ad esempio nel caso di: APT1 e APT10, APT28 e APT29, APT33 e APT34, APT37 e APT38.
Gli strumenti più efficaci per addivenire ad evidenze certe (*"smoking guns"*) circa i *threat actors* – che consentono di uscire dal campo del plausibile - sono nella disponibilità di agenzie di *law enforcement* e di *intelligence*: HUMINT, VIRTUAL HUMINT e SIGINT rappresentano attività imprescindibili.
Di qui la necessità, anche per le Istituzioni finanziarie, di una stretta cooperazione con questi organi, attraverso l'approntamento di convenzioni *ad hoc*.

L'indagine sull'attribuzione e sugli attori della minaccia è una prova impegnativa e sfidante, talvolta senza risultati: è tuttavia importante nelle attività di CTI. Non si può sostenere a lungo una difesa contro artefatti provenienti da minacce ignote: tale impostazione equivarrebbe a combattere un antìgene, senza conoscere il ceppo virale da cui ha origine.
In ogni caso, le citate *false flags* e le tecniche di disinformazione spesso trasformano l'arena *cyber* internazionale in un gioco di specchi, alimentato da dinamiche legate a deterrenza, guerra ibrida e attacchi dissimulati.
Tra informazione e controinformazione, *cyber intelligence* e *cyber counterintelligence*, le attività di attori come *Hidden Cobra*, *Grizzly Steppe* e *Stone Panda*, nonché la loro riconducibilità ad entità governative, fanno ormai parte del dominio OSINT.
Lo US CERT – unitamente a NSA, DHS, DoD e FBI – e lo *UK National Cyber Security Centre* (parte del GCHQ) operano spesso in congiunzione con le controparti di Australia

(*Australian Cyber Security Center*), Nuova Zelanda (CERT *New Zealand*) e Canada (*Canadian Cyber Security Centre*). Una posizione peculiare è ricoperta da Israele. Seguono l'Iran ed altri paesi.
L'Unione Europea è impegnata in promettenti iniziative di regolamentazione e ambiziosi piani strategici (ad esempio: *Cybersecurity Act*, Direttiva NIS, Regolamento GDPR, Iniziativa sul *Quantum Computing*), nonostante il rischio del prevalere degli interessi dei singoli Stati. Alcuni sforzi congiunti si concretizzano a livello operativo in seno a CERT-EU, EUROPOL ed ENISA, oltre che tra i CERT di alcune Istituzioni (come ad esempio sull'asse Banche centrali nazionali – BCE).
Sul fronte italiano, l'architettura nazionale *cyber* è stata ridefinita dal Decreto "Gentiloni", in linea con gli obiettivi delineati dal "Piano nazionale per la protezione cibernetica e la sicurezza informatica": un ruolo centrale è svolto dal Dipartimento delle Informazioni per la Sicurezza (DIS) e dal Nucleo per la Sicurezza Cibernetica (NSC); le attività dello CSIRT nazionale sono in fase di avvio. In ambito finanziario, la cooperazione pubblico-privato è promossa attraverso il CERTFin; la Banca d'Italia è attiva col suo CERTBI.
Per quanto riguarda specificatamente il settore finanziario, *cybergang* e *botmaster* sviluppano *financial malwares* evolvendone continuamente i codici, così da rendere sempre più impegnativo il contrasto al *cybercrime*. Tra le principali galassie di questo comparto, si possono annoverare: Ursnif/Gozi/ISFB/Dreambot, Zeus, Carbanak/Cobalt/Anunak/Fin7, Dridex, TrickBot, Emotet, GootKit, Ramnit, Qakbot, Qadars.
Si rileva che le Istituzioni finanziarie – e tra queste le Banche centrali – risultano oggetto di attacchi mirati, volti in particolare al *cyber espionage*, per via delle attività alle quali sono deputate.
L'obiettivo precipuo di *cybergangs* e gruppi APT (in specie quelli *state-backed*) è in effetti l'esfiltrazione di dati strategici di carattere finanziario (secondo l'ENISA *Threat Landscape Report*, rilasciato il 28 gennaio 2019, *"advanced persistent threat (APT) cyberattacks indicate that many financial attacks are motivated by espionage"*), benché i fini siano di solito plurimi ed i vettori d'attacco molteplici.

Sviluppo di un sistema di *cyber threat intelligence*

L'attività di CTI è usualmente espletata da specifiche unità in seno a CERT (*Computer Emergency Response Teams*) o CSIRT (*Computer Security Incident Response Teams*). Uno scenario maturo prevede la gestione, suddivisa e coordinata, di attività tattiche di CTI e attività strategiche di CTI all'interno di un'unica struttura preposta.
I livelli di maturità di un sistema di CTI si dividono di solito in *initial*, *managed*, *repeatable* ed *optimized*. La CTI è generalmente suddivisa in tattica, operativa e strategica. A queste categorie si interpone talvolta la CTI tecnica. Si passa dall'esame degli IOCs allo studio delle TTPs e *del modus operandi* impiegato dagli attori della minaccia, fino ad arrivare all'analisi del contesto geopolitico.
Lo sviluppo di un sistema di CTI non può prescindere dalla definizione di procedure operative e da una ponderata suddivisione dei compiti. Occorre innanzitutto delineare un pro-

cesso interno *ad hoc*, stabilire regole d'ingaggio e definire un *threat model*.
Il processo di CTI può essere innescato da un *trigger* interno o esterno, da una informazione richiesta o ricevuta. In questa fase, l'*infosharing* – con controparti della *community*, in conformità a prestabiliti protocolli TLP e convenzioni *ad hoc* - è fondamentale. Nella fase preliminare di *triage*, occorre attribuire all'evento *cyber* uno *score*, ponderato su grado di capacità offensiva, intento ostile ed opportunità dell'attaccante in relazione al grado di esposizione degli *asset* da proteggere.

L'obiettivo ultimo – che esula dal singolo *case* di analisi - è la produzione di conoscenza sedimentata, una *knowledge base* dalla quale attingere per la trattazione di eventi successivi o per lo sviluppo di analisi di contesto. Anche per questo obiettivo è fondamentale adottare un approccio di tipo multidisciplinare. La conoscenza acquisita non ha la pretesa di azzerare il grado di incertezza relativo alle minacce (non si possono approfondire in questa sede le pur rilevanti connessioni con temi quali l'incertezza sulle condizioni iniziali nei sistemi complessi o l'indeterminazione di tipo quantistico), ma di migliorare il metodo di osservazione e aumentare la conoscenza dei fenomeni, per garantire maggiore prevenzione e gestione sistemica degli stessi.

Figura 3 - *Analisi qualitativa/quantitativa delle minacce*

La complessità dei fenomeni trattati (intesa come quantità e varietà di relazioni non-lineari tra i singoli componenti che costituiscono il dominio *cyber*), richiede l'approntamento di un sistema di CTI adeguato, che interagisca in modo adattativo con l'ambiente esterno, attraverso mutazione ed auto-organizzazione (in linea con i principi della dottrina relativa ai *Complex Adaptive Systems* - CAS).
Il sistema proposto consiste in un insieme di capacità abilitanti, operative nel continuo, a supporto di un ciclo di CTI che viene innescato *case by case*.
Il ciclo, che trae origine dal classico processo di *intelligence*, è implementato in modo iterativo fino al raggiungimento dell'*output* richiesto.
Una fase decisiva è sicuramente quella dell'analisi. In questo stadio, si passa dalla materia grezza (dati) alle informazioni raffinate, sia attraverso la connessione di evidenze tecniche, sia tramite la correlazione di segnali deboli di contesto ("*connecting the dots*").

Per l'analisi tecnica di possibili *intrusions*, è utile l'impiego di *framework* strutturati come la *cyber kill chain* (*Reconnaissance*, *Weaponization*, *Delivery*, *Exploitation*, *Installation*, *Command & Control*, *Actions*) e il *diamond model* (*Adversary*, *Infrastructure*, *Victim*, *Capability*). Per l'identificazione, la prioritizzazione e la rappresentazione sinottica delle azioni da intraprendere è efficace l'utilizzo della *course of action matrix* (composta da due azioni passive - *Discover* e *Detect* – e cinque attive - *Deny*, *Disrupt*, *Degrade*, *Deceive*, *Destroy*).

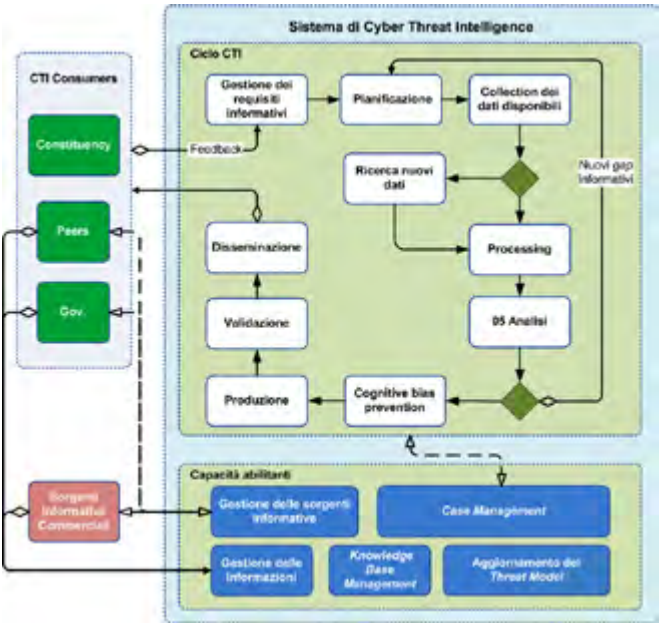


Figura 4 - *Sistema di cyber threat intelligence con dettaglio di fasi e sotto-fasi del ciclo*

Le analisi tecniche afferenti a *DFIR* e *malware analysis*, devono essere accompagnate da analisi di contesto. A tal riguardo, di ausilio per questo tipo di indagini, sono le attività di *cyber intelligence* (CYBINT).
Questa disciplina trae origine dalla declinazione classica delle attività di *intelligence* (INTs), con riferimento alle peculiarità del dominio di ricerca informativa in ambito *cyber*. L'attività CYBINT si evolve includendo attività di analisi strategica e analisi di contesto su *trend* di eventi, scenari geopolitici e previsionali.
In un modello compiuto, la CTI dovrebbe essere integrata da attività di *cyber threat counterintelligence*, per contrastare – e se del caso sfruttare nel continuo – le attività di CTI svolte dagli attaccanti.
Nell'ambito dell'analisi multilivello di CTI, alcuni strumenti evoluti a supporto di un *threat modeling* sono il ricorso ad analisi di *pattern* comportamentali, ad elementi di teoria dei

grafi e scienza delle reti, a modelli statistici Bayesiani, a *clusterizzazione* di APT per galassie.
Le attività di CTI possono essere supportate e potenziate attraverso l'impiego di specifici supporti tecnologici, denominati *threat intelligence platform* (TIP).
Le TIP implementano una piattaforma tecnologica a supporto degli analisti: sono strumento utile per correlare ed esaminare dati relative a minacce, aggregando informazioni grezze da fonti molteplici ed automatizzando alcune parti del ciclo di CTI.
Le TIP attraverso automazione, integrazione, standardizzazione, correlazione e collaborazione permettono di incrementare l'efficienza delle attività di CTI aumentando l'efficacia dell'*intelligence* generata in termini di tempestività, pertinenza e accuratezza.

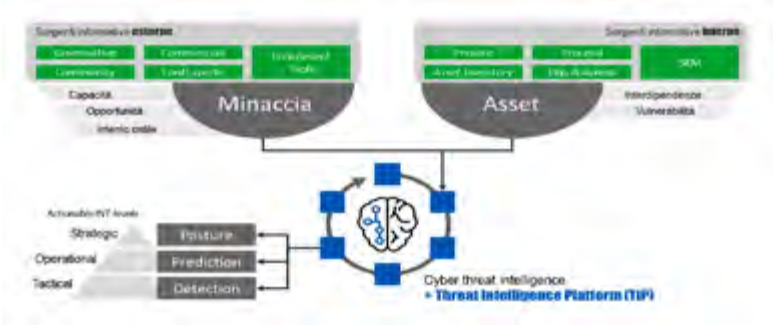


Figura 5 - *Fonti Informative (interne/esterne) e Threat Intelligence Platform (TIP)*

In particolare, le TIP sono utilizzate per la raccolta, l'arricchimento e la fusione di dati interni ed esterni. Tali piattaforme consentono di raggruppare e classificare una grande mole di informazioni grezze provenienti da fonti multiple, anche in presenza di formati eterogenei e dati non strutturati. Esse consentono, quindi, una normalizzazione delle informazioni grezze e la costruzione di modelli e tassonomie comuni. Inoltre, le principali TIP possono essere integrate con sistemi di sicurezza già presenti (ad es. i SIEM), attraverso un flusso bidirezionale di informazioni e segnali.
Le TIP forniscono altresì supporto nella fase di analisi, le cui risultanze sono da sottoporre in ogni caso a validazione da parte dell'analista.
A tal proposito, nello sviluppo di un sistema di CTI, occorre dosare l'impiego di strumenti di automazione, ricavandone il massimo vantaggio e trovando il più efficiente equilibrio nel rapporto uomo-macchina, prediligendo l'elemento umano nella fase decisionale e strategica.

Implicazioni derivanti dall'introduzione di un sistema di CTI in una Banca centrale

I *cyber* attacchi diretti contro una Banca centrale mirano principalmente all'esfiltrazione di dati strategici e in genere al *cyber-espionage*. Tuttavia, in un'ottica di *worst case scenario*, i *target* maggiormente sensibili sono costituiti dalle infrastrutture critiche, a supporto delle principali piattaforme finanziarie gestite.
In ambito europeo, tra i compiti istituzionali di una Banca centrale vi è la promozione del regolare funzionamento del sistema dei pagamenti, attraverso la gestione diretta dei principali circuiti. Tale attività, unitamente all'azione di supervisione sui mercati, mira a contribuire alla stabilità del sistema finanziario e a favorire l'efficacia della politica monetaria.
In questo contesto, le funzioni aziendali e istituzionali si saldano e si connettono nelle implicazioni sistemiche derivanti dal corretto funzionamento delle infrastrutture, piattaforme e applicazioni di mercato gestite da una Banca Centrale (nel caso europeo, gestite in cooperazione o in via esclusiva, sotto supervisione BCE).
I sistemi informativi e di pagamento di una Banca centrale sono immersi nel cyberspazio e sono esposti a una vasta gamma di minacce *cyber*. Si intuiscono le possibili ripercussioni per il sistema finanziario di riferimento, con effetti trasmissivi a catena sul tessuto finanziario globale.

Anche in quest'ottica, le attività preventive di CTI appaiono cruciali per anticipare le minacce e comprenderne i *trend*: a queste si deve accompagnare una gestione sistemica e adattativa verso eventi avversi di varia natura, che implichino risvolti di tipo *cyber*, garantendo una risposta resiliente.
A questo scopo, le attività di CTI rimangono centrali: appare efficace la locuzione di derivazione britannica "*intelligence-led cyber resilience*". Le attività di *intelligence* richiedono quindi lo sviluppo di *framework* ed architetture IT volti a garantire un sistema di *cyber resilience*. In questo scenario, da una parte i sistemi e le infrastrutture informatiche, dall'altro il personale (importante per questo l'*awareness*) e i processi aziendali devono essere pronti a garantire stabilità, attraverso una reazione flessibile e adattativa, a fronte di mutevoli condizioni ed eventi avversi di varia natura (in particolare *cyber*). La *cyber resilience* mira a recuperare e mantenere livelli accettabili di erogazione del servizio, migliorando in seguito all'evento, sulla base di *lessons learned*.
Lo sviluppo di un sistema di CTI all'interno di una Banca centrale presenta indubbi vantaggi, ma può comportare anche risvolti sfavorevoli che è opportuno prevedere e mitigare, tenendo presenti le implicazioni di *policy* a livello aziendale, settoriale e sistemico, sia sul piano nazionale che globale.
L'introduzione di regole e tecnologie per l'espletamento di attività di CTI possono avere effetti positivi, diretti e indiretti.
La prima conseguenza concreta derivante dalla loro introduzione può essere un aumento di capacità di prevenzione e gestione coordinata di attacchi *cyber*.

Un indubbio vantaggio è l'ausilio dato dall'automazione all'analista di *intelligence*, nelle fasi di raccolta, catalogazione, correlazione e analisi dei dati. Inoltre, vi può essere un effetto leva per tecnologie collegate alla TIP e con essa interagenti; un aumento di competenze tecniche sia per gli addetti alla piattaforma, sia per il personale IT impiegato in altre attività. Un effetto collaterale virtuoso è rappresentato dal possibile miglioramento di alcuni processi di *business*, derivante da un efficientamento indiretto, a valle della risoluzione preventiva e celere di problematiche *cyber*.
Tra i possibili risvolti negativi, vi può essere un eccessivo peso/costo di gestione delle tecnologie e dello *staff* addetto, possibile *lock-in* per *asset* infungibili, problemi di regolamentazione interna ed esterna all'organizzazione, incertezze nel *trade-off* automazione-elemento umano, sfasamento tra linee IT e *business*, problemi legati alle peculiarità delle attività di *intelligence*.
Riguardo a quest'ultimo punto, le attività di CTI e di INT in genere (ad es. protocolli di sicurezza, gestione di informazioni confidenziali, corretto utilizzo di dispositivi elettronici, aree ad accesso limitato o segregato, documenti riservati, regole di condotta e norme di comunicazione etc.) richiedono qualità comportamentali specifiche, che vanno oltre le pur necessarie competenze tecniche. Questi aspetti possono essere potenziati attraverso specifici percorsi di formazione e addestramento. Oltre a ciò, appare però necessario valutare il talento investigativo, l'intuito, la capacità inventiva e le caratteristiche psicologiche delle persone da impiegare nelle attività di *intelligence*.
Alcuni problemi si possono presentare nella fase di analisi, con insorgenza ad esempio di *bias* cognitivi. Per farvi fronte, oltre all'impiego di tecniche di analisi strutturata (SAT - *structured analytic techniques*), è utile definire un processo e regole *ad hoc*, non tralasciando un approccio il più possibile multidisciplinare e sincretico per le analisi svolte (con l'impiego di professionisti di varia estrazione e formazione).

Conclusioni

Per far fronte al crescente numero di attacchi cibernetici diretti contro Istituzioni finanziarie, in particolare Banche centrali, occorre un cambio di paradigma, che sposti il baricentro dal *risk management* alla prevenzione della minaccia.
Gli strumenti classici di *cybersecurity* non garantiscono un'adeguata efficacia nell'identificazione e prevenzione di operazioni *cyber* di tipo strutturato. Attacchi come *APT e DDoS* massivi possono mettere a dura prova gli ordinari presìdi di sicurezza. Le classiche contromisure difensive possono perfino essere vanificate, se gli attacchi afferiscono a più ampie operazioni di *cyberwarfare* (es. tramite CNOs – *Computer Network Operations*), strategie di destabilizzazione (es. per mezzo di PSYOPs - *Psychological Operations*) o campagne di interferenza di tipo statuale.
I *cyber-attacks* sferrati contro Istituzioni finanziarie mirano generalmente alla esfiltrazione di dati sensibili e strategici, attraverso operazioni di *cyber-espionage*. Tali attacchi possono però avere come *target* anche la compromissione di infrastrutture critiche, comprese quelle a supporto di piattaforme finanziarie e sistemi di pagamento transnazionali.

La CTI appare uno strumento cruciale per aumentare le capacità di difesa e prevenzione delle Istituzioni finanziarie, in particolare in organizzazioni articolate come le Banche centrali; le attività in questione possono prevenire attacchi strutturati e aiutare a gestire in modo coordinato ed efficace ogni evento di tipo *cyber*, garantendo una reazione resiliente.
La conseguenza diretta dell'introduzione di un sistema basato su questi strumenti è quindi la crescita della capacità di prevenzione e gestione adattativa delle minacce di tipo *cyber*. Ciò implica non soltanto un aumento della sicurezza delle infrastrutture e delle piattaforme gestite dall'Istituzione finanziaria, ma anche un effetto trasmissivo su gangli vitali del settore finanziario, con incremento della resilienza sistemica.
Alcune piattaforme finanziarie sono peraltro gestite in modo congiunto da diverse Istituzioni a livello europeo: l'introduzione di un sistema di CTI all'interno di una di queste (al netto di processi di *threat intelligence* condivisi), può avere effetti benefici indiretti anche per altre.

Al di là delle implicazioni sistemiche, l'approntamento di un programma di CTI può comportare internamente vantaggi, che spaziano dall'avanzamento tecnologico al miglioramento dei processi di *business*. Tuttavia, tra i possibili risvolti negativi da mitigare vi sono l'aumento dei costi di gestione, possibili *bias* cognitivi nella fase di analisi, incertezze nella gestione del rapporto uomo-macchina, possibili interferenze geopolitiche sui servizi commerciali di *threat intelligence* utilizzati.
Con riguardo al contesto globale, l'introduzione di un sistema di CTI, appare necessario per far fronte alle crescenti attività di *hacktivism*, *cybercrime*, *cyber espionage*, *cyberterrorism*, *nation-state* e *state-sponsored campaigns*.
La natura e l'interconnessione di questi fenomeni, nonché le peculiarità del dominio *cyber*, richiedono che la CTI faccia ricorso ad analisi di contesto, con impiego di competenze multidisciplinari, ad integrazione della DFIR e della *malware analysis*. Tali analisi di contesto si rendono vieppiù necessarie in presenza di *cyberwarfare* e operazioni di tipo statuale.
In concreto, è opportuno servirsi di strumenti quali analisi geopolitica, *cyber intelligence* e *cyber counterintelligence* e istituire cooperazioni con agenzie di *intelligence* e di *law enforcement*.
Le attività di CTI – così come le attività di INT in genere – richiedono qualità personali specifiche, oltre a determinate competenze tecniche; agli *skills* professionali, si affiancano caratteristiche comportamentali e psicologiche idonee.
La CTI mira ad analizzare ed elaborare dati grezzi per fornire *actionable intelligence*: informazioni impiegabili concretamente dagli organismi di *governance*. Da questi ultimi e dalla trasmissione efficace della conoscenza sviluppata dipende il risultato delle azioni preventive.

In conclusione, pare opportuno indugiare ancora sulle implicazioni di carattere sistemico. L'introduzione di un sistema di CTI all'interno di una Banca centrale, può aumentare il grado di resilienza delle infrastrutture e delle piattaforme finanziarie gestite, proteggendo nel contempo dati sensibili e strategici contro tentativi di *cyber espionage*.

Considerato l'alto grado di interconnessione e gli effetti trasmissivi che caratterizzano il sistema finanziario, un tale apparato di CTI - garantendo una reazione adattativa agli eventi avversi e potenziando la prevenzione di minacce di tipo *cyber* - è in grado di aumentare la stabilità e la resilienza del comparto nel suo complesso.

Bibliografia essenziale

- *Bank of England - CBEST Intelligence-Led Testing Understanding Cyber Threat Intelligence Operations Version 2.0.*
- *Central Intelligence Agency (US) - "A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis" Prepared by the US Government (2009), available at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Tradecraft%20Primer-apr09.pdf.*
- *Central Intelligence Agency (US) - The World Factbook 2019. Washington, DC: Central Intelligence Agency, 2019 - https://www.cia.gov/library/publications/the-world-factbook/index.html.*
- *Christine Lagarde – "Estimating Cyber Risk for the Financial Sector" (Giugno 2018).*
- *Christopher Wray – Director of the Federal Bureau of Investigation (FBI) - "Keeping Our Financial Systems Secure: A Whole-of-Society Response" available at https://www.fbi.gov/news/speeches/keeping-our-financial-systems-secure-a-whole-of-society-response - 01 Novembre 2018.*
- *Decreto Presidenza del Consiglio dei Ministri - 17 Febbraio 2017.*
- *ENISA Threat Landscape Report 2018 - 15 Top Cyberthreats and Trends- 28 Gennaio 2019.*
- *Eric M. Hutchins and others - Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains - available at https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf.*
- *Direttiva UE 2016/1148 (NIS Directive).*
- *EU Quantum Computing - europa.eu/rapid/press-release_IP-18-6205_en.htm, 29 Ottobre 2018.*
- *EU Regulation 2016/679 (GDPR Regulation).*
- *FBI - Foreign Influence Task Force (FITF): https://www.fbi.gov/investigate/counterintelligence/foreign-influence.*
- *Federal Reserve System – Information Technology Guidance - https://www.federalreserve.gov/supervisionreg/topics/information-technology-guidance.htm.*
- *Framework for Improving Critical Infrastructure Cybersecurity (last version 1.1 - Aprile 2018) of the National Institute of Standards and Technology (NIST).*
- *G7 fundamental elements for effective assessment of cybersecurity in the financial sector (Giugno 2018).*
- *Governatore della Banca d'Italia - 1st Bank of Italy World Bank International Research Workshop - Building Human Capital for 21st Century Jobs – 15 Novembre 2018.*

- *Guidance on cyber resilience for financial market infrastructures of CPMI-IOSCO (Giugno 2016).*
- *https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed.*
- *https://www.dhs.gov/news/2018/10/06/statement-dhs-press-secretary-recent-media-reports-potential-supply-chain-compromise, 6 Ottobre 2018.*
- *https://www.fbi.gov/news/stories/chinese-hackers-indicted-122018*
- *https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf.*
- *https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed.*
- *https://www.ecb.europa.eu/paym/initiatives/cyber-resilience/fmi/html/index.en.html.*
- *https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections.*
- *https://securityintelligence.com/how-to-defend-with-the-courses-of-action-matrix-and-indicator-lifecycle-management/.*
- *https://www.santafe.edu/.*
- *https://www.us-cert.gov.*
- *https://www.ncsc.gov.uk.*
- *https://www.fireeye.com/current-threats/apt-groups.html.*
- *https://www.group-ib.com/media/cbrf-double-attack/.*
- *https://nchoucri.mit.edu/cyberspace-cyberpolitics.*
- *IBM X Force - https://securityintelligence.com/q1-2018-results-gozi-ursnif-takes-larger-piece-of-the-pie-and-distributes-icedid/.*
- *IMF Regional Economic Outlook "Managing the Upswing in Uncertain Times" on Europe (Maggio 2018).*
- *Institute of International Finance (IIF) - Addressing regulatory fragmentation to support a cyber-resilient global financial services industry– Aprile 2018.*
- *Internet organized crime threat assessment (IOCTA – 18 Settembre 2018) by EUROPOL.*
- *Decreto Legislativo 65/2018.*
- *James Andrew Lewis senior vice president at the Center for Strategic and International Studies in Washington, D.C. – Evaluating a "Cybersecurity Moonshot" - 26 Giugno 2018.*
- *Kalyan Veeramachaneni and others - AI2: Training a big data machine to defend – available at https://people.csail.mit.edu/kalyan/AI2_Paper.pdf.*
- *MI6 Chief Alex Younger - Secret Intelligence Service, SIS - https://www.gov.uk/government/speeches/mi6-c-speech-on-fourth-generation-espionage - 3 Dicembre 2018.*
- *Matteo E. Bonfanti - "Cyber Intelligence: In Pursuit of a Better Understanding for an Emerging Practice"– Maggio 2018.*
- *NATO Wales Summit Declaration - 2014.*
- *NATO Warsaw Summit Communiqué – 2016.*
- *OECD Interim Economic Outlook, 20 Settembre 2018.*
- *OECD http://www.oecd.org/eco/outlook/economic-outlook/, November 2018.*

- *Office of the Director of National Intelligence - National Counterintelligence and Security Center - Foreign Economic Espionage in Cyberspace – 2018 - https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf.*
- *Prof. Alan Turing, quotation, from "Intelligent Machinery: A Report by A. M. Turing," (Summer 1948), submitted to the National Physical Laboratory (1948) and published in Key Papers: Cybernetics, ed. C. R. Evans and A. D. J. Robertson (1968) and, in variant form, in Machine Intelligence 5, ed. B. Meltzer and D. Michie (1969).*
- *Prof. Gerardo Beni "From Swarm Intelligence to Swarm Robotics" – in Lecture Notes in Computer Science - 2004.*
- *Prof. Ettore Majorana "Il valore delle Leggi Statistiche nella Fisica e nelle Scienze Sociali" – Anni 1930 – pubblicato postumo.*
- *Prof. Marco Dorigo and Christian Blum "Ant colony optimization theory: A survey" – in Theoretical Computer Science – 2005.*
- *Prof. Richard Feynman - "Six Easy Pieces" and "Six Not-So-Easy Pieces".*
- *Prof. Roland Kupers - Resilience in complex organizations - Oxford University – in The Global Risks Report del WEF.*
- *Tallinn Manual 2.0.*
- *TIBER-EU (Threat Intelligence-based Ethical Red Teaming) initiative.*
- *William Dixon and Amy Jordan - https://www.weforum.org/agenda/2018/12/why-the-fourth-industrial-revolution-needs-more-arts-graduates/ - World Economic Forum - 11 Dicembre 2018.*
- *World Bank Financial Sector's Cybersecurity: A Regulatory Digest (aggiornamento continuo).*
- *World Economic Forum - The Global Risks Report 2019 – 16 Gennaio 2019.*
- *World Economic Outlook 2018 – Less Even Expansion, Rising Trade Tensions - Update – Luglio 2018.*

Carding – Scenario ed evoluzione dei canali di vendita nel 2018

[A cura di Luca Sangalli e Luca Dinardo, Lutech]

Introduzione

Il presente report redatto dal Team di **Cyber Threat Intelligence di Lutech**, ha lo scopo di presentare lo scenario attuale relativo alla compravendita illegale di carte di credito su internet, fenomeno noto come *Carding*.

Attraverso i nostri sistemi proprietari di ricerca, attivi su fonti pubbliche e private, presenti nel deepweb e nel darkweb, comprensivo anche del recente sistema di DNS basato su Blockchain, sono stati raccolti e analizzati dati riconducibili al tema del carding, sui diversi canali sul quale viene trattato.

Nelle successive sezioni viene descritto il fenomeno del carding in generale ("***Il fenomeno del Carding***"), viene presentato lo scenario attuale e le principali differenze con gli anni passati ("Blackmarket – Scenario attuale"), un aggiornamento sulle principali caratteristiche dei market e dei dati delle carte di pagamento che vengono vendute ("***Caratteristiche dei Blackmarket***" e "***Aggiornamento sui dati delle carte di pagamento – 2018***") e viene riportato un caso di un'operazione condotta dalla Guardia di Finanza che ha messo fine ad un'attività illecita che operava attraverso blackmarket presenti nel darkweb ("***Operazione Darknet.Money***").

Il fenomeno del Carding

Con il termine *Carding* si identifica principalmente lo scambio e compravendita di informazioni riguardanti carte di credito, debito o account bancari, che vengono poi utilizzate per eseguire truffe di carattere finanziario acquistando beni o trasferendo fondi ai danni dei legittimi proprietari. Il carding è una delle attività più diffusa e popolare nell'underground;

è possibile trovare numerosi market specializzati nella sola vendita di dati di carte di credito così come interi forum e thread dedicati all'argomento, con annunci di compravendita, guide e metodi sempre più aggiornati per riuscire a portare a termine questo tipo di truffe.

La maggior parte della compravendita di carte di credito avviene tramite i blackmarket, questo perché come per il normale e-commerce legale, è il canale più comodo sia per i compratori alla ricerca di questo prodotto che per i venditori che lo offrono. In questo modo i contatti fra le due parti vengono ridotte al minimo e la gestione della trattativa è affidata al market.
Questo sistema si è evoluto negli anni da semplici siti web a veri e propri marketplace di informazioni illegali, completi di filtri di ricerca, news sui prodotti aggiunti, servizi di feedback e customer care, rimborsi e altro ancora.

Blackmarket – Scenario attuale

Rispetto alla situazione analizzata nell'anno passato, il numero complessivo dei market è leggermente diminuito, ad ulteriore conferma della tendenza sulla minore durata della vita presentata nel rapporto Clusit 2017 ("*Analisi blackmarket – Scenario e focus sul carding in Italia*"); tuttavia in compenso è aumentato il numero di mirror dei market attivi e la loro presenza su canali alternativi, in particolare è stata rilevata una sempre maggiore presenza di tali market all'interno del sistema di DNS basato su blockchain, confermando quanto presentato nel rapporto Clusit 2018 ("*Carding – Tecniche di vendita: evoluzioni recenti e future*").

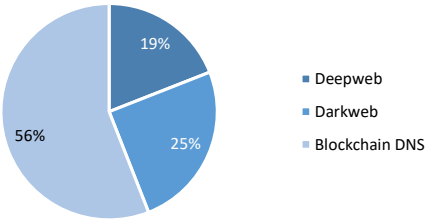
Nelle immagini si possono vedere due annunci di market che pubblicizzano i loro sistemi; si può notare che entrambi hanno mirror presenti su blockchain DNS e utilizzano altri canali alternativi come Telegram

Caratteristiche dei Blackmarket

Dal punto di vista delle funzionalità dei market specializzati in carding, non sono stati introdotti elementi significativi rispetto agli anni passati, pertanto le loro caratteristiche sono rimaste coerenti con quanto mostrato nel rapporto Clusit 2017 ("*Analisi blackmarket – Scenario e focus sul carding in Italia*").

La principale differenza riguarda la loro presenza in rete: i blackmarket tuttora attivi hanno aumentato il numero di mirror in modo da essere più resistenti a tentativi di takedown, in particolare è stato rilevato un **sempre maggior utilizzo della tecnologia di DNS basata su blockchain**.

Distribuzione presenza dei market



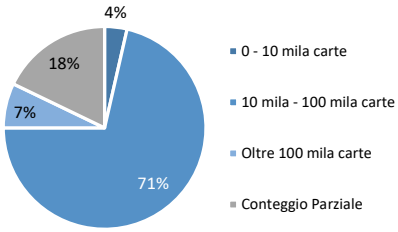
Il numero di market presenti sul sistema di DNS basato su blockchain è elevato perché vengono registrati molti mirror dei market stessi utilizzando diversi domini, messi a disposizione da questa tecnologia quali .bazar, .lib, .emc, .bit, .coin, …

Aggiornamento sui dati delle carte di pagamento – 2018

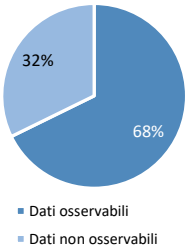
In questa sezione viene riportato un aggiornamento sulle statistiche relative ai dati delle carte di pagamento estratti dai market di carding, su cui è stato possibile verificarne l'effettiva presenza. Vengono riportati diversi indicatori sulla distribuzione di vendita di tali informazioni.

I dati numerici relativi ad ogni blackmarket sono stati estratti durante la fase di raccolta delle informazioni.

Distribuzione quantità di carte per market

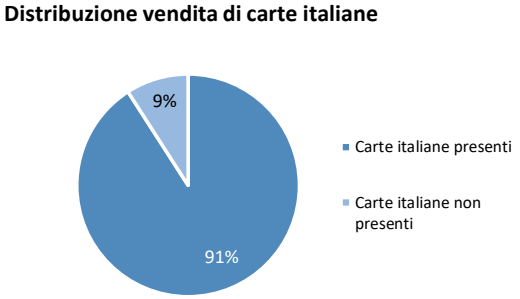


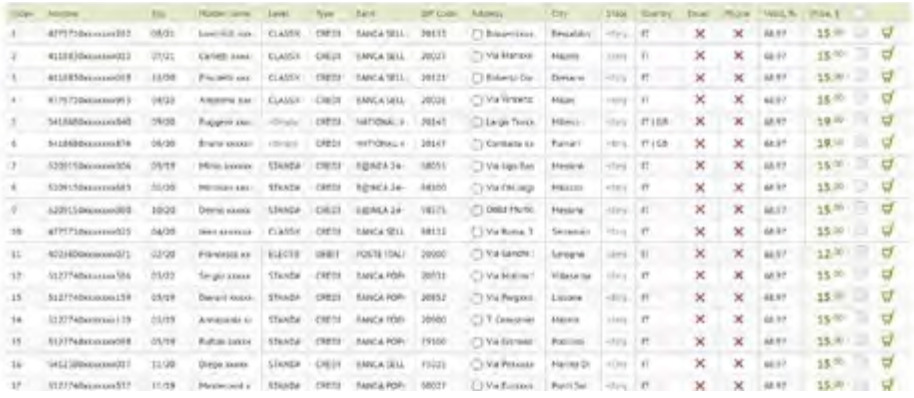
Visibilità dati venduti sui market



Diversi market di carding necessitano di un deposito iniziale per poter visualizzare i dati messi in vendita. Generalmente viene richiesta una cifra che varia dai 30 ai 50 dollari.

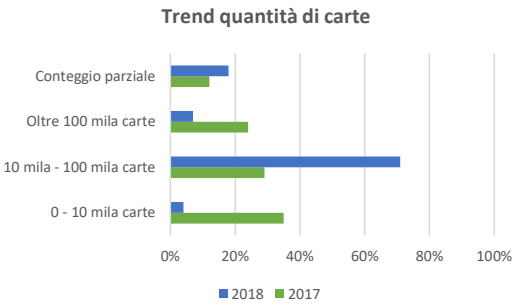
La maggior parte dei dati messi in vendita sui blackmarket è relativa a carte di pagamento statunitensi, poiché l'utilizzo del chip elettronico integrato non è frequente e la banda magnetica non è una protezione adeguata; tuttavia, anche se in numero minore, ormai quasi tutti i market elencano dati di carte emesse da istituti di altri paesi, fra cui l'Italia.

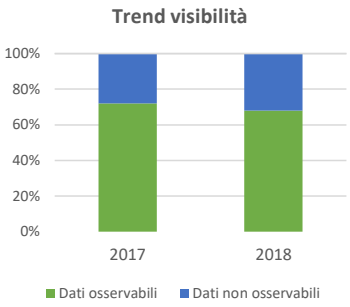


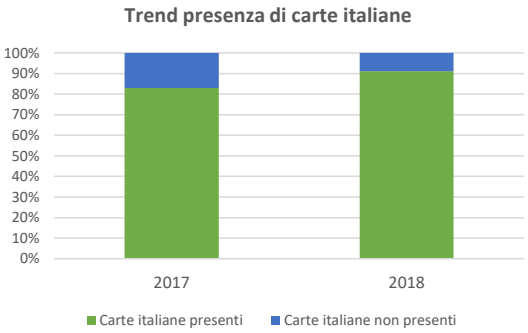


Esempio dei risultati di una ricerca di carte emesse da istituti italiani

Mediamente, il numero complessivo di dati di carte di pagamento presenti sui market è aumentato rispetto all'anno passato in cui sulla prevalenza di essi era messo in vendita un numero inferiore alle 10 mila unità. Ad oggi i market elencano un numero compreso fra le 10 mila e le 100 mila unità di dati di carte di pagamento.
Il conteggio di tali quantità è stato estratto dai market tuttavia è necessario precisare che **non è indicativo dell'effettivo volume di vendita dei market** in quanto può riferirsi al numero di carte di credito in vendita in quel momento, a quelle non scadute oppure all'intero storico di informazioni che sono state presenti sui market stessi.







Confermando la situazione degli anni precedenti, il prezzo delle carte di pagamento messe in vendita sui market si attesta intorno ai 20 dollari, dipendentemente dalla quantità di informazioni disponibili, quali:

- Solo dati della carta (Numero, scadenza e CVV)
- Nome intestatario
- Indirizzo
- Numero di telefono
- PIN

Operazione Darknet.Money

Il sempre maggior utilizzo di tecnologie che rendono più facile l'anonimato degli utenti e conseguentemente più difficile il tracciamento degli stessi, rendono indubbiamente più complicato il lavoro e atto a contrastare questi fenomeni di compravendita illegale.

Nonostante questa difficoltà crescente, sono state condotte con successo operazioni da parte delle forze dell'ordine come quella denominata "Darknet.Money" da parte del Nucleo Speciali Frodi Tecnologiche della Guardia di Finanza di Roma, coordinato dalla Procura della Repubblica di Brescia che ha messo fine ad una fiorente attività illecita dedita alla falsificazione di banconote e di metalli preziosi, all'utilizzo di carte di credito e SIM telefoniche clonate, alla vendita di documenti falsi, all'accesso abusivo a sistema informatico e riciclaggio.

L'indagine di questo nucleo speciale della GdF ha avuto inizio dall'analisi degli annunci di vendita presenti sui vari market, che ha permesso di ricavare informazioni che sono state successivamente elaborate arrivando ad accertare come il soggetto principale svolgesse la propria attività illegale insieme ad altri due soggetti, nella città di Napoli. Ulteriori riscontri svolti sul campo hanno consentito di appurare che i tre erano dediti alla compravendita di banconote false e oro contraffatto, oltre ad utilizzare i proventi dell'utilizzo di carte di credito e SIM telefoniche clonate per acquistare beni di consumo da rivendere sul mercato locale. In particolare, le carte di credito clonate appartenevano per lo più ad ignari cittadini spagnoli e tedeschi i cui codici di accesso erano oggetto di compravendita sui blackmarket. Gli investigatori del Nucleo Speciale Frodi Tecnologiche della Guardia di Finanza di Roma hanno quindi ricostruito l'intero sodalizio criminale attraverso le fonti di prova attribuibili ai tre soggetti e su disposizione dell'Autorità Giudiziaria di Brescia, hanno eseguito tre misure cautelari consistenti rispettivamente in una ordinanza di custodia in carcere, una ordinanza di custodia agli arresti domiciliari e un obbligo di firma presso l'Autorità di Polizia.

Conclusioni

Il mercato di compravendita illegale di carte di credito è tuttora florido e conta un numero considerevole di marketplace dedicati che sempre più spesso creano dei mirror presenti nel clearweb, darknet e nel più recente sistema di DNS basato su Blockchain; al fine di rendere più difficile il controllo ed evitare la chiusura e il tracciamento dei market stessi, potendo registrare e gestire tali domini in maniera anonima.

Ciononostante queste pratiche illegali vengono contrastate con successo attraverso sofisticate indagini tecniche come quella condotta dal Nucleo Speciale Frodi Tecnologiche della Guardia di Finanza di Roma qui presentata, in cui gli investigatori sono riusciti a mettere fine ad un'attività illecita che operava attraverso blackmarket presenti nel darkweb.

Lo stato di adeguamento al GDPR

Survey a cura dell'Osservatorio Information Security & Privacy del Politecnico di Milano

Il 25 maggio 2018 il Regolamento europeo sulla Protezione dei Dati Personali (GDPR) è diventato pienamente applicabile. Si è assistito a un innalzamento dell'attenzione verso la tutela dei dati personali, con l'obiettivo dichiarato di favorire la crescita della fiducia dei cittadini europei nell'economia e nella società digitale. Per contro, gli attacchi informatici non danno tregua alle organizzazioni, costringendole a correre ai ripari. Per contrastare questo fenomeno, in crescita incessante, le aziende italiane hanno incrementato la spesa in soluzioni tecnologiche legate alla protezione dei dati e stanno investendo nella sensibilizzazione dei propri dipendenti, ma è necessario internalizzare meccanismi di adattamento per evitare di venire travolti dai cambiamenti in atto e dalle sfide future.
In questo scenario si è mosso l'Osservatorio Information Security & Privacy – promosso dalla School of Management del Politecnico di Milano – in collaborazione con CEFRIEL e DEIB e con il patrocinio di ANRA (Associazione Nazionale dei Risk Manager) e CLUSIT (Associazione Italiana per la Sicurezza Informatica).

L'Osservatorio, al suo quarto anno di Ricerca, si è posto l'obiettivo di rispondere al bisogno di conoscere, comprendere e affrontare le principali problematiche dell'information security & privacy e monitorare l'utilizzo di nuove tecniche e tecnologie a supporto di tale area da parte delle aziende end user, creando una community permanente di confronto.
La Ricerca 2018 dell'Osservatorio ha proposto una Survey di rilevazione che ha coinvolto 667 CISO, CSO, CIO, Compliance Manager, Risk Manager, Chief Risk Officer e DPO di imprese italiane. In particolare sono state coinvolte 166 organizzazioni grandi (>249 addetti) e 501 PMI (tra 10 e 249 addetti).
L'indagine sulle grandi imprese, oltre a monitorare il mercato dell'information security e le scelte delle diverse realtà rispetto agli aspetti organizzativi, si è soffermata ad analizzare il percorso di adeguamento delle aziende ai requisiti imposti dal GDPR. La rilevazione ha esplorato cinque aspetti in particolare: lo stato dei progetti di adeguamento, il budget dedicato, le azioni implementate, le principali criticità riscontrate e la figura del DPO.[1]
In questo contesto, per il rapporto CLUSIT è stata inoltre svolta un'indagine in esclusiva finalizzata a indagare gli elementi sopra citati all'interno di differenti settori merceologici (GDO, Finance, Manufacturing e Utility).

[1] La rilevazione è stata condotta tra settembre e dicembre 2018.

Dalla rilevazione emergono alcune peculiarità tipiche dei diversi settori di business analizzati. Giova anticipare il dato secondo cui, rispetto alla rilevazione condotta l'anno precedente, il tema dell'adeguamento al GDPR non sembra più fortunatamente interessare solamente le imprese appartenenti ai settori del Finance e della Grande Distribuzione Organizzata (GDO), ossia contesti in cui il trattamento del dato personale appare essere core-business: anche le aziende appartenenti a settori diversi, quale quello manifatturiero, hanno infatti avviato e portato a termine importanti e complessi progetti di adeguamento al GDPR.

Non essendoci stato alcun rinvio relativamente alla data di effettiva applicazione, il 2018 ha visto la quasi totalità delle aziende adoperarsi per mettere in campo adeguati progetti di adeguamento alla normativa o per ottimizzare i processi e le soluzioni già in essere. L'indagine ha rilevato che nel 59% delle organizzazioni è tuttora in corso un progetto strutturato di adeguamento al GDPR, mentre nel 23% dei casi tali progetti sono stati completati: quasi un quarto delle aziende si è pertanto dichiarata conforme ai requisiti imposti dalla normativa europea in materia di protezione dei dati. Coerentemente sono diminuite le imprese che dichiarano una scarsa conoscenza delle implicazioni del GDPR, passando dal 15% del campione dell'anno scorso al 10% di quest'anno: occorre però precisare che quest'ultima percentuale si riferisce ad aziende in cui il tema non è ancora posto all'attenzione del vertice ma è comunque noto alle funzioni specialistiche quali IT Security, Legal e Compliance.[2]

Infine, un altro sintomo del raggiungimento di un maggiore grado di maturità e consapevolezza sul tema è dato dalla limitata percentuale di aziende (8%) che si trova ancora nella fase di analisi dei requisiti richiesti e dei piani di attuazione possibili, laddove nel 2017 tale quota si attestava sul 34% (**Figura 1**).

[2] Dai dati della Ricerca 2017 dell'Osservatorio, il 7% delle organizzazioni dichiarava che le implicazioni del GDPR erano note nelle funzioni specialistiche ma non era ancora un tema posto all'attenzione del vertice, mentre l'8% affermava che le implicazioni del GDPR non erano note in dettaglio. Quest'ultima percentuale si attesta sullo 0% nella rilevazione 2018.

Figura 1 - *Il percorso di adeguamento al GDPR – Fonte: Osservatorio Information Security & Privacy, School of Management Politecnico di Milano*

Per quanto riguarda il settore bancario, il percorso di adeguamento al GDPR risulta essere ben tracciato: il 90% delle aziende ha infatti dichiarato che è in corso un progetto strutturato in materia o addirittura di averlo già completato. Il settore manifatturiero è quello che registra una percentuale di crescita maggiore rispetto alla rilevazione condotta l'anno precedente, passando dal 42% delle aziende all'87% nel 2018. Anche le utility e le aziende operanti nella Grande Distribuzione Organizzata (GDO) registrano percentuali elevate (rispettivamente l'85% e l'84% delle organizzazioni), mentre si riscontra un ritardo relativamente alle aziende operanti nel mercato assicurativo, con solo il 57% di esse che dichiara essere in corso un progetto strutturato di adeguamento alla normativa (**Figura 2**).

Figura 2 - *Il percorso di adeguamento al GDPR per settore di mercato – Fonte: Osservatorio Information Security & Privacy, School of Management Politecnico di Milano*

Parallelamente allo stato di avanzamento dei progetti di adeguamento si registra un notevole incremento del budget dedicato a misure di adeguamento al GDPR. Mentre nel 2017 solamente nel 58% dei casi esisteva un budget dedicato, nell'ultimo anno la percentuale ha raggiunto l'88%. È evidente tuttavia come il focus debba ora spostarsi principalmente verso tutte quelle misure volte ad assicurare il mantenimento della compliance normativa, quali a titolo esemplificativo le attività periodiche di audit, la revisione del registro dei trattamenti e l'aggiornamento delle procedure e delle tecnologie di sicurezza e protezione dei dati. Per tutte queste attività, il 67% delle organizzazioni ha stanziato un budget, mentre nel restante 33% non è presente (nel 25% dei casi tuttavia verrà stanziato nei prossimi 12 mesi). È invece inferiore la percentuale di aziende che dichiara l'esistenza di un budget dedicato a misure di risposta agli eventi di sicurezza che potrebbero verificarsi (es. data breach), voce che include i costi di notifica e le implicazioni economiche che possono derivare da un eventuale contenzioso: poco più di metà delle aziende (51%) ha stanziato un budget, il 21% provvederà entro il prossimo anno, mentre il 28% non lo prevede nemmeno per il futuro (**Figura 3**).

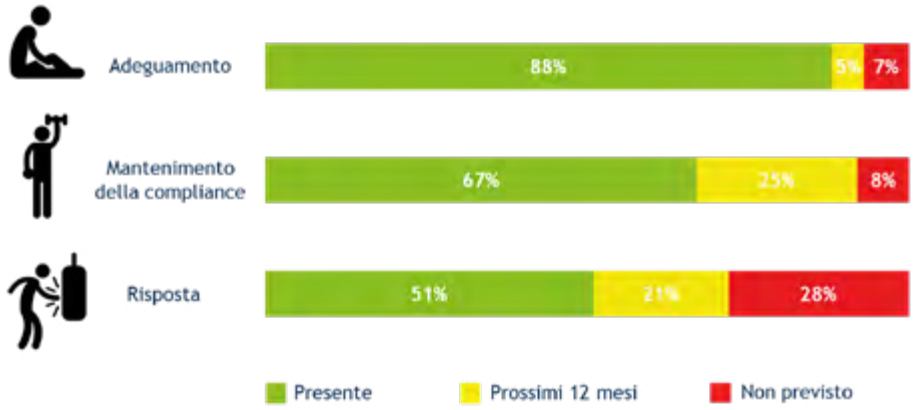


Figura 3 - *Il budget dedicato al GDPR – Fonte: Osservatorio Information Security & Privacy, School of Management Politecnico di Milano*

Focalizzandosi sul budget dedicato a misure di adeguamento al GDPR, la percentuale di organizzazioni operanti nel mondo della GDO che ha già provveduto a stanziarlo si attesta sull'82%, ma il dato che più sorprende in negativo è quello per cui ben il 12% ha dichiarato non solo l'assenza di un budget ma anche l'intenzione di non prevederlo in futuro. In campo assicurativo, nonostante il ritardo riscontrato nei progetti di adeguamento alla normativa messi in campo dalle organizzazioni, un budget dedicato è stanziato nella totalità dei casi, mentre nel settore bancario la percentuale scende leggermente al 94%. Tra le aziende manifatturiere, l'86% ha stanziato un budget dedicato a misure di adeguamento al GDPR,

mentre tra le utility la percentuale scende al 77%, anche se il restante 23% dichiara che verrà stanziato entro i prossimi 12 mesi. Nessuna azienda del settore ha infatti dichiarato di non prevedere investimenti (**Figura 4**). Per quanto riguarda invece i budget dedicati a misure di mantenimento della compliance e a misure di risposta agli incidenti di sicurezza, il settore assicurativo si conferma il più maturo (con rispettivamente il 67% e l'83% delle organizzazioni che ha stanziato un budget), mentre con riferimento agli altri settori di business analizzati non emergono sostanziali differenze.

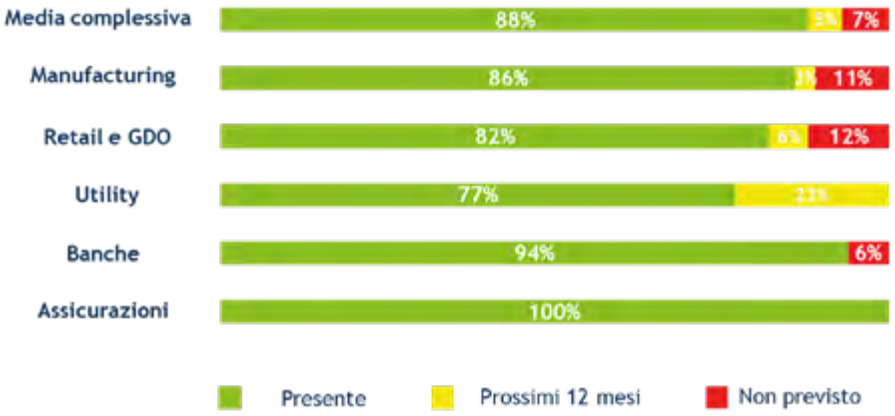


Figura 4 - *Il budget dedicato a misure di adeguamento al GDPR per settore di mercato – Fonte: Osservatorio Information Security & Privacy, School of Management Politecnico di Milano*

Entrando nello specifico nelle fasi che compongono il processo di adeguamento al GDPR, le principali azioni che sono già state implementate dalle organizzazioni riguardano la creazione del registro dei trattamenti (85%), l'individuazione dei ruoli e delle responsabilità (81%), la raccolta e la mappatura dei dati (78%), la modifica della modulistica (76%), la procedura di data breach notification (68%), la definizione delle politiche di sicurezza e di valutazione dei rischi (66%), la valutazione d'impatto sulla protezione dei dati personali (56%), l'implementazione dei processi per l'esercizio dei diritti dell'interessato (54%) e la revisione della contrattualistica con le terze parti/fornitori di servizi tecnologici (48%).

Come nel 2017, tra i processi in fase più avanzata di attuazione rientrano la creazione del registro dei trattamenti e l'individuazione dei ruoli e delle responsabilità all'interno dell'organizzazione. A tale proposito è opportuno sottolineare la crescita della percentuale dei rispondenti che ha dichiarato di aver implementato tali attività che, nell'anno precedente alla piena applicabilità della normativa, si attestava rispettivamente al 13% e al 19%. Ana-

logamente all'anno scorso una delle maggiori difficoltà riscontrate è invece relativa all'implementazione dei processi per l'esercizio dei diritti dell'interessato. Inoltre, problematico risulta essere il tema della contrattualistica con i fornitori di servizi tecnologici e, quindi, dell'esternalizzazione dei trattamenti di dati personali a terze parti.
Dalla rilevazione emerge infine che per tutte le fasi che compongono il processo di adeguamento al GDPR, le organizzazioni si sono avvalse o intendono avvalersi anche delle prestazioni di consulenti esterni. In media un'azienda su cinque si è rivolta a specialisti del settore, e le attività per cui è richiesto maggiormente un supporto riguardano le fasi di raccolta e mappatura dei dati (25%), modifica della modulistica (23%) e creazione del registro dei trattamenti (22%).

Che la fase di raccolta e mappatura dei dati personali risulti essere particolarmente complicata per le aziende è testimoniato dal fatto che circa un'impresa su due (52%) l'abbia indicata come fattore che ha reso difficile l'adeguamento ai requisiti imposti dal GDPR. Le altre principali criticità riscontrate riguardano la mancanza di sensibilizzazione sul tema da parte dei dipendenti aziendali (38%), la scarsa sponsorizzazione da parte del Top Management (37%), le difficoltà di comprensione della normativa (27%), la mancanza di figure professionali competenti sul tema (23%), la mancanza o l'inadeguatezza del budget stanziato (20%) e l'inefficacia delle soluzioni tecnologiche di protezione e delle iniziative organizzative (20%) (**Figura 5**).

Figura 5 - *Le principali criticità riscontrate – Fonte: Osservatorio Information Security & Privacy, School of Management Politecnico di Milano*

A livello di singoli settori, la fase di raccolta e mappatura dei dati personali ha rappresentato la principale criticità per quattro delle cinque categorie di mercato analizzate: Banche (61%), Manufacturing (55%), Utility (55%) e Retail e GDO (53%). Dall'analisi sul settore assicurativo emerge invece come la principale problematica sia la mancanza di sensibilizza-

zione sul tema da parte dei dipendenti aziendali (57%), fattore che comunque si conferma particolarmente critico anche per le organizzazioni rientranti negli altri settori di mercato considerati. Un dato interessante che emerge dalla rilevazione è quello per cui il 44% delle aziende del settore bancario lamenta soluzioni tecnologiche di protezione e iniziative organizzative inadeguate, mentre negli altri settori di business analizzati tale fattore rappresenta la criticità minore riscontrata dalle imprese in fase di adeguamento ai requisiti imposti dal GDPR.

La Ricerca ha indagato anche la presenza del Data Protection Officer (DPO) all'interno delle aziende. La figura del DPO è presente formalmente nel 65% delle organizzazioni, mentre nel 6% dei casi si tratta di una presenza di tipo informale. Rispetto alla rilevazione condotta l'anno precedente si è registrato un incremento del 46% di aziende che hanno introdotto la figura in esame nel proprio organico: nel 2017 infatti le percentuali si attestavano rispettivamente al 15% e al 10%. Coerentemente, è diminuita la quota di rispondenti che ha dichiarato di voler introdurre la figura del DPO nel prossimo futuro (5% contro il 57% del 2017) e la percentuale di imprese che afferma di non prevederne l'introduzione (6% contro il 15% del 2017). Infine, il restante 18% del campione ha dichiarato che la responsabilità è delegata a una figura esterna all'azienda (**Figura 6**).

Figura 6 - *La presenza del DPO – Fonte: Osservatorio Information Security & Privacy, School of Management Politecnico di Milano*

La figura del DPO è presente formalmente nel 95% delle banche e nell'86% delle aziende operanti nel mercato assicurativo. Una percentuale più bassa ma comunque interessante si registra nelle utility, dove il 69% ha dichiarato di avere formalizzato la figura in esame all'interno dell'azienda. Percentuali inferiori si registrano invece tra le aziende del settore manifatturiero (45%) e nelle organizzazioni operanti nel settore Retail (39%); con riferimento a quest'ultima categoria, tuttavia, un ulteriore 39% del campione ha dichiarato che la responsabilità è delegata a una figura esterna all'azienda (**Figura 7**).

Figura 7 - *La presenza del DPO per settore di mercato – Fonte: Osservatorio Information Security & Privacy, School of Management Politecnico di Milano*

In conclusione, il quadro che emerge dall'indagine sullo stato di adeguamento delle imprese al GDPR è sostanzialmente positivo. Il 63% delle organizzazioni ha rilevato un aumento rispetto al passato della sensibilità del Top Management sul tema della protezione dei dati. Più della metà delle aziende del campione ha inoltre posto in essere almeno una DPIA (Data Protection Impact Assessment), ha introdotto corsi di formazione indirizzati ai dipendenti sulla tematica in oggetto e afferma di tener conto degli aspetti relativi alla sicurezza nella fase che precede ogni nuovo trattamento (privacy by design). Il 47% delle imprese ha infine effettuato investimenti in tecnologie, mentre il 34% ha inserito in organico nuove figure professionali dedicate al tema della protezione dei dati.
Guardando il rovescio della medaglia, il 26% delle organizzazioni ha registrato criticità da un punto di vista organizzativo, ad esempio per quanto riguarda l'individuazione dei ruoli e delle relative responsabilità all'interno dell'azienda, mentre l'8% ha addirittura rilevato un generale rallentamento dei processi e delle attività quotidiane. Ma si tratta di "incidenti di percorso" rispetto alla percezione di uno scenario maturo in cui le aziende che lo compongono stanno dimostrando di essere ormai proiettate verso il futuro e verso le sfide che le nuove tecnologie pongono in materia di data protection e, in definitiva, di aver preso piena coscienza dell'intera tematica.

2019: data protection 4.0

[A cura di Sergio Fumagalli]

Il 2018 è stato un anno cruciale per la Data Protection e non solo perché il 25 maggio il GDPR è entrato pienamente in vigore: per la prima volta è emersa con chiarezza, nella consapevolezza della pubblica opinione, la relazione fra la protezione dei dati personali e quelle libertà e quei diritti degli interessati, cioè di tutti noi, così spesso richiamati dagli articoli del GDPR.
Il caso Cambridge Analytica, con le sue connessioni con le elezioni presidenziali americane, da un lato, e, dall'altro, con il calo del valore borsistico di Facebook, è stato il primo caso di incidente relativo alla protezione dei Data Protection in cui il nodo centrale non fosse legato alla sicurezza dei dati personali.
Il significato dirompente di quell'evento è duplice: un trattamento illecito di dati personali non è tollerato dall'opinione pubblica e può essere credibilmente sospettato di avere conseguenze rilevanti per la democrazia del Paese più potente del mondo. Sono notizie die questo inizio 2019 le preoccupazioni concrete dell'UE sulle possibili interferenze esterne con le prossime elezioni europee.
L'UE, che su questo fronte ha consolidato, con il GDPR, una leadership mondiale incontestabile, non è per questo isolata: anche la California, nel 2018, ha adottato una legge statale sulla protezione dei dati personali molto simile al GDPR.

Le imprese, anche in Italia, hanno reagito al GDPR investendo, naturalmente chi più e chi meno (un altro articolo del Rapporto Clusit 2019 cercherà di illustrare, con basi più oggettive, quanto e come).
Si può dire che una prima fase di adeguamento sia oggi conclusa o si avvii ad esserlo: le informative, quasi tutte, fanno riferimento al GDPR, i registri dei trattamenti sono stati redatti, i DPO sono stati nominati, i Data protection agreement sono in corso di progressivo adeguamento all'art. 28, i primi data breach sono stati notificati.
In questo senso, siamo, sembra, in un momento simile al 2006, dopo l'approvazione del d.lgs. 196/03. Allora, al picco di interesse seguì subito il periodo del disimpegno, culminato con la cancellazione, nel 2011, dell'obbligo di redigere il DPS, ad opera del Governo Monti con finalità di semplificazione. Succederà lo stesso?
Il quadro al contorno è molto cambiato, dal 2006 ma anche dal 2011. La trasformazione digitale delle relazioni sociali, economiche, politiche e della stessa nozione di conflitto fra Stati sovrani è talmente profonda che solo amministratori ciechi possono oggi guardare ai prossimi anni con la stessa leggerezza di allora: "qualcosa abbiamo fatto, adesso torniamo a pensare al business".
I dati personali, oggi, sono il business o, forse più precisamente, sono la materia prima del business: sono le persone fisiche che votano, lavorano, comprano prodotti e servizi e ne fruiscono, direttamente o indirettamente. Le preferenze, le aspettative, le abitudini, i com-

portamenti, le propensioni delle persone guidano le scelte collettive e le scelte di mercato: conoscerle e saperle interpretare in anticipo fa la differenza.
Il GDPR contrasta il far west nell'uso dei dati personali, che ha caratterizzato la fase nascente della digital economy e contribuisce a disegnare il contesto, più maturo e sostenibile, in cui dovrà essere ricollocato il bisogno delle imprese e delle organizzazioni pubbliche e sociali, di comunicare e di realizzare prodotti e servizi in modo sempre più mirato e individualizzato.
Finito il periodo dell'adeguamento, si apre quello del vantaggio competitivo costruito sulle nuove regole, la Data Protection 4.0: sviluppare, in modo conforme al GDPR e alla sensibilità del pubblico, tutto il potenziale dell'innovazione digitale.
Non una singola tecnologia ma l'intero potenziale delle tecnologie disponibili e dalla loro intersezione e integrazione: applicare, ad esempio, in modo conforme al GDPR, l'intelligenza artificiale ai big data prodotti dall'esplosione dell'Internet delle cose, perché questo contribuisce a rendere l'innovazione sostenibile sia in relazione al rischio compliance, cioè a quelle sanzioni che hanno impressionato molti, sia nel rapporto con i consumatori e la pubblica opinione in genere.
Mentre i progetti di adeguamento si sono concentrati, inevitabilmente, su Registro dei trattamenti, informative e consensi, per la nuova fase, la data protection 4.0, diventano cruciali altri articoli del GDPR:

- Gli articoli 25 (Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita), 35 (Valutazione d'impatto sulla protezione dei dati) e 36 (Consultazione preventiva) che governano complessivamente il processo di innovazione;
- Gli articoli 32 (Sicurezza del trattamento), 33 (Notifica di una violazione dei dati personali all'autorità di controllo) e 34 (Comunicazione di una violazione dei dati personali all'interessato) che disegnano il presidio e la gestione della sicurezza dei dati personali;
- L'articolo 28 (Responsabile del trattamento) che ridisegna il rapporto fra il Titolare e la sua catena di fornitura, l'ecosistema produttivo e di servizi che gli consente di svolgere il suo ruolo.

Sono questi alcuni dei temi su cui le aziende dovranno concentrarsi prioritariamente dopo aver raggiunto un ragionevole livello di conformità.
La complessità della nuova fase risiede in due fattori:

- l'imprevedibilità dell'innovazione e
- l'assenza di modelli di riferimento a cui ispirarsi nel porla in essere.

Proviamo a guardare la nuova fase, la data protection 4.0, da queste due angolature.

Imprevedibilità dell'innovazione

L'investimento necessario per avere accesso a tecnologie innovative si abbassa di continuo e i prodotti tendono ad incorporare nativamente funzionalità evolute ad alto impatto per il trattamento di dati personali: le telecamere per la video sorveglianza, ad esempio, tendono progressivamente ad incorporare capacità sempre più evolute di riconoscimento e analisi delle immagini, senza che il compratore ne sia consapevole o le richieda.

Dotarsi di videosorveglianza, o rinnovare gli impianti esistenti, è una decisione in sé abbastanza ordinaria, certamente molto frequente e non percepita come strategica. L'uso di quelle capacità può, però, trasformare uno strumento installato per aumentare la sicurezza in qualcosa che può fornire indicazioni sui visitatori di un negozio e sul loro comportamento, o sull'attività che si svolge all'interno di un impianto produttivo e cambiandone la valenza, anche sotto il profilo della conformità e della responsabilità.
Governare l'innovazione richiede, dunque, una focalizzazione specifica, per evitare che decisioni assunte con leggerezza e, magari, investimenti marginali, possano comportare un'esposizione e un rischio non desiderati e non valutati dal titolare. L'innovazione, infatti, può avvenire, auspicabilmente per altro verso, in qualsiasi punto dell'organizzazione e in qualsiasi momento.
Dotarsi di una procedura aziendale che realizzi il dettato dell'art. 25 è il primo passo ma non sarà una procedura a risolvere il problema: è necessario assicurare che sia effettivamente conosciuta e applicata. Dunque, formazione e controllo.
L'art. 25, da qualunque prospettiva si guardi, è, dunque, assai più complesso da soddisfare del temutissimo DPIA che invece sembra riempire di preoccupazioni i Titolari. Non solo: una corretta gestione della Data protection by Design è la premessa essenziale per un altrettanto corretto approccio agli articoli 35 e 36 che governano il DPIA.

Assenza di modelli di riferimento

L'innovazione ci pone di fronte a situazioni che non hanno precedenti: come si riconosce l'errore software da un errore di modellizzazione e da un risultato inatteso ma corretto, nell'applicazione dell'IA? Eppure, sulla base di quel risultato, il mio CV potrebbe essere scartato e la mia carriera pregiudicata, o una diagnosi puntare in una direzione piuttosto che in un'altra.
Relazioni sempre più complesse rendono difficile individuare chi abbia la responsabilità di cosa, perché i ruoli si mischiano e si confondono e solo un'analisi attenta e una contrattualistica conseguente stringente possono evitare abusi e confusione, oltre a rischi non secondari per il Titolare coinvolto. In altri ambiti questi aspetti si sono già presentati in tutta la loro complessità (es. regolamentazione delle responsabilità condivise nel caso di servizi cloud).
L'articolo 28 che governa i rapporti tra il Titolare e la catena di fornitura a cui si approvvigiona, diventa qui centrale insieme a tutti i diversi temi coinvolti nella stesura di un contratto, afferenti anche a discipline diverse (diritto di immagine, proprietà intellettuale, diritto del lavoro, pubblica sicurezza).
L'innovazione consente di disegnare per i fornitori ruoli sempre più complessi e "interni" ai processi di business, abbinando attività delegate da Titolare a funzioni e dati raccolti dal fornitore sulla base del proprio modello di business. Questa complessità può coinvolgere a sua volta i sub fornitori.
L'assenza di modelli di riferimento riguarda anche un altro insieme di obblighi introdotti dal GDPR, quello riferito alla gestione del tempo di conservazione e, quindi, della cancellazione o anonimizzazione dei dati stessi. L'intera architettura applicativa IT è interessata

da questi nuovi requisiti funzionali che richiedono, per essere soddisfatti, una capacità di governo del dato ad oggi normalmente non disponibile.
Esistono certamente modelli ormai riconosciuti per regolare le tipologie di fornitura e di partnership più frequenti ma la capacità di intercettare e di gestire correttamente i casi anomali, cioè quelli più innovativi e infrequenti è spesso priva di modelli di riferimento e richiede un'attenzione particolare, anche sotto il profilo della sicurezza.

Conclusioni

Certamente vi sono settori più sensibili di altri alla protezione dei dati personali e all'innovazione nel rapporto con gli interessati introdotta dal GDPR: le aziende che si rivolgono al consumatore (B2C), ad esempio, sono più esposte di quelle che operano in un mercato B2B; quelle che operano in settori innovativi più di quelle che operano in mercati tradizionali.
Non vi sono, però, settori totalmente estranei al tema e questo sarà sempre più vero per la propensione a trasformare in senso digitale anche attività che, a tutt'oggi, sembrano interessate solo marginalmente ai dati personali: ormai, tutto è smart o lo sta diventando. I fornitori di penumatici, ed esempio, sembrerebbero operatori molto lontani dalle tematiche regolate dal GDPR. Invece, stanno dotando i loro prodotti di chip in grado di farli dialogare con gli altri sistemi di bordo e, in prospettiva, con le altre auto. Si tratta di dati personali? Chi deve essere informato del trattamento e da chi? Cosa devono fare i produttori di pneumatici per assicurare o, almeno, consentire un utilizzo conforme dei dati che raccolgono al resto del mondo automotive?

Infine, questa distinzione non è riconducibile alla dimensione dell'impresa: il GDPR rischia di scaricare sulle PMI oneri e responsabilità difficili da assumere. La sottovalutazione dell'importanza degli artt. 40 e 41 che prospettano e regolano la redazione di Codici di Condotta è, sotto, questo profilo, difficilmente comprensibile, in particolare nel contesto economico italiano.

Riassumendo, le priorità della nuova fase che si apre dopo che una ragionevole conformità al GDPR sia stata raggiunta, cioè, le priorità della Data Protection 4.0 sono le seguenti:

- La gestione dell'innovazione. L'innovazione è qualsiasi cambiamento: quelli rilevanti che richiedono ingenti investimenti e quelli minori che possono svilupparsi in qualsiasi punto dell'organizzazione in modo anche incontrollato. Sviluppare una App che utilizza in modo innovativo informazioni contenute nel Data warehouse aziendale, infatti, può costare poche migliaia di Euro ed essere compatibile con il budget e l'autonomia decisionale di molti manager. Pensare il processo di gestione dell'innovazione in modo che questa nasca sicura e conforme è un modo per ridurre i rischi ad essa connessi, non solo relativamente alla Protezione dei Dati personali ma all'operatività in generale.
- La sicurezza delle informazioni. Questo è il tema più tradizionalmente associato alla Protezione dei dati personali. Anzi, si può dire che la Privacy è stato il cavallo di Troia che ha introdotto il tema della sicurezza dei dati nel lessico aziendale. È dunque l'ambito più

frequentato ma non per questo da trascurare, considerato che le sfide sono in continua evoluzione.

- Il trasferimento degli obblighi di compliance, inclusa la sicurezza, all'intero ecosistema di partner e fornitori che concorre alla realizzazione dei prodotti e dei servizi del titolare impone una revisione della contrattualistica e del processo stesso di selezione dei fornitori
- Il governo dei dati. La gestione della base giuridica che sorregge la legittimità del trattamento dei dati, in relazione alle finalità di questo e ai tempi di conservazione e, dunque, ai processi di cancellazione dei dati è un tema assai complesso che coinvolge la progettazione stessa dell'architettura delle applicazioni e delle basi di dati.
  È un tema rilevantissimo che qui ci si limita a menzionare per completezza, lasciandone l'approfondimento ad altri interventi.

Al centro del successo di una azienda rimane sempre l'eccellenza dei prodotti, dei servizi e dei processi aziendali non la conformità al GDPR.
È il concetto di eccellenza che non può più essere disgiunto dalla capacità di gestire e sfruttare i dati personali in modo rispettoso dei diritti e delle libertà degli interessati. Questo riguarda le aziende ma anche coloro che in esse operano.
A un progettista di auto degli anni 50 del secolo scorso, verosimilmente, il marketing aziendale, per un nuovo modello da sviluppare, chiedeva prestazioni e affidabilità. Lo shock petrolifero degli anni 70 introdusse il tema dei consumi. Poi venne la sicurezza. Oggi la motorizzazione diesel, dopo 20 anni di successo e indubbie qualità prestazionali e di consumi e di investimenti enormi, rischia di essere archiviata, almeno per le auto, per la difficoltà di raggiungere gli standard ambientali richiesti.

La professionalità di un progettista ma anche del marketing aziendale non può, oggi, prescindere da questi aspetti. Una nuova auto non concepita "by design" per rispondere a questi requisiti non è neppure pensabile.
È qualcosa di più di una analogia.

La terza fase del GDPR

[A cura di Alessandro Vallega]

La prima fase è stata quella legale, la seconda fase quella della sicurezza. Quale sarà la terza? È evidente che il GDPR ha avuto un forte impatto sulle aziende e pubbliche amministrazioni e sulle organizzazioni che operano con l'Europa. Dopo le prime due fasi probabilmente partirà una terza fase che descriviamo in questo focus.

1. La fase "legale" è quella delle informative, dei registri del trattamento e dei data protection officer. Molte aziende l'hanno percorsa o lo stanno facendo. Le aziende che sperano di potersi fermare sbagliano.
2. La fase "sicurezza" è quella delle misure di sicurezza, gestione organizzativa dei data breach, del by design e by default, della DPIA[1], e della consultazione preventiva[2]. Come spiegava Fumagalli nell'articolo precedente, questa fase ha il problema di gestire l'imprevedibilità dell'innovazione e dell'assenza di modelli di riferimento. Ma è una fase fondamentale per non esporre l'azienda al rischio di compliance e a danni di reputazione.
3. È quella della "modifica delle applicazioni per i diritti degli interessati", ovvero dei progetti atti a garantire:
    a. l'uso adeguato delle informazioni rese disponibili dal consenso prestato o in conseguenza dell'applicazione di altre basi giuridiche;
    b. la minimizzazione dei dati e la limitazione della conservazione;
    c. il diritto all'oblio;
    d. l'obbligo di notifica ai destinatari.

Nella nostra esperienza le aziende si sono solamente affacciate alle attività di quest'ultima fase e spesso hanno adottato delle soluzioni tampone. Ignorarla può causare danni molto seri alla reputazione aziendale e ovviamente si può incorrere in sanzioni. Anche se è possibile che l'Autorità per la protezione dei dati personali non si accorga velocemente delle violazioni di questi principi, è sicuro che lo faranno gli interessati, quindi il danno reputazionale è molto importante soprattutto nel settore B2C.

La necessità di una terza fase formalizzata come "progetto" dipende molto dal tipo di azienda e dei sistemi informativi che gestisce (tipo, qualità e vastità).

---

[1] È più usato l'acronimo inglese che il nome esteso in italiano "Valutazione d'impatto sulla protezione dei dati"

[2] Il tema della gestione delle catene fornitura con i relativi articolo 28 e i cosiddetti DPA (data protection agreement) è un po' a cavallo delle due fasi.

In cosa consiste la terza fase

Pensando agli obiettivi di questa fase, si comprende facilmente il ruolo centrale di un sistema informatico ben fatto. Per esempio le applicazioni dovrebbero aiutare l'utente utilizzatore a tenere conto del consenso prestato, negato o ritirato e ad evitare di trattare il dato quando non sia permesso; i sistemi dovrebbero cancellare automaticamente i dati quando si verificano le condizioni necessarie e, nel contempo, dovrebbero continuare ad operare senza malfunzionamenti[3]; infine, dovrebbero tenere traccia dei destinatari dei dati per poter propagare le richieste di cancellazione o rettifica da parte degli interessati.
Visto che tutto questo non è stato progettato inizialmente, si tratta di aggiustare manualmente i programmi (o sostituirli con del software più moderno). In una nostra precedente ricerca[4], l'area dei requisiti sugli applicativi era la più arretrata del processo di adeguamento al GDPR.

Si sa che il software è complesso: è molto probabile che questa terza fase sia la più onerosa e quindi varrebbe la pena cercare di ottenere il massimo beneficio dall'uso delle risorse impegnate. In pratica si tratta di approfittare di questa massiva revisione dei sistemi informativi per migliorarli e cogliere tutte le opportunità. Potrebbe essere il caso di rinnovare il CRM? È il momento di centralizzare in un solo punto le anagrafiche dei clienti? Si può incidere sulla qualità dei dati? È il momento di implementare un data warehouse?

Operativamente nella terza fase ci sono attività volte:

1. a comprendere nel dettaglio i requisiti legali; questo richiede una specifica competenza legale spesso non disponibile agli esperti di software;
2. ad aumentare la conoscenza degli oggetti software (programmi, applicazioni, data store, interfacce, web services, servizi esterni...) sui quali intervenire;
3. ad adeguare o sostituire parte del software; attività che richiedono specifiche competenze di system integration ed eventualmente l'utilizzo di nuovi pacchetti applicativi on-premises o servizi nel cloud.

Qualsiasi intervento sul software richiede una conoscenza precisa degli oggetti sui quali intervenire. Di solito, nelle medio-grandi aziende italiane tale conoscenza è insufficiente. Le aziende non sanno dove sono i loro dati e come fluiscono da un sistema all'altro. Non conoscono le interfacce e le logiche con i quali sono trattati. Questo vale sia per quelli personali soggetti al GDPR sia per gli altri di business. Le aziende ne producono sempre di più, lo fanno anche in maniera destrutturata senza il controllo dell'IT e spesso vengono resi accessibili in modalità self-service a molte aree e utenti aziendali. Come verranno usati?

[3] Questo è un problema sentito: molti esperti, visto che nei sistemi tale funzionalità non è stata progettata inizialmente, temono che si possano riscontrare degli errori nei calcoli o dei bug a fronte delle cancellazioni.

[4] Giugno 2018, Oracle Community for Security, Europrivacy, Aused e Clusit "GDPR: Maturità delle Imprese italiane rispetto agli adempimenti richiesti". https://privacyeu.clusit.it/#/

A chi verranno mandati? Purtroppo se ne perde il controllo proprio quando aumenta sensibilmente l'importanza e il valore di conoscerli!

In questo contesto va enfatizzato il ruolo positivo di metodologie e strumenti di data governance.

Non si devono giustificare questi investimenti con il solo obbligo di compliance al GDPR; bisogna assolutamente rivalutare i vantaggi di tipo business. Le aziende e la pubblica amministrazione italiane sono di nuovo di fronte all'opportunità di approfittare degli obblighi normativi per innovare e migliorare: ne vale la pena perché non c'è ormai alcun settore merceologico in cui l'IT non sia una leva strategica.

Figura 1 - *Cosa serve per specificare gli interventi software relativi al GDPR*[5]

È semplice la terza fase?

Purtroppo non è semplice per niente.
La conoscenza del sistema informativo è difficile da mantenere e ri-acquisire. Normalmente sta nelle persone interne o esterne all'azienda e si perde con il turn-over. La documentazione è assente o obsoleta e comunque non è in grado di rispondere alle domande che le vengono poste. Manca di struttura e di standardizzazione. Una domanda che sentiamo continuamente ripetere è "ma dove sono i dati personali che trattiamo?".

Alla mancanza di informazioni, inoltre, si aggiunge la complessa relazione tra la parte legale e quella tecnica. Non basta sapere dove sia il dato personale: bisogna metterlo in relazione con le applicazioni e i trattamenti svolti.

[5] Per ulteriori informazioni si veda anche "Il GDPR nei sistemi informativi complessi: best practice per la compliance normativa" dove ho trattato questo stesso tema da un altro punto di vista https://www.cybersecurity360.it/legal/privacy-dati-personali/il-gdpr-nei-sistemi-informativi-complessi-best-practice-per-la-compliance-normativa/.

Come affrontare la terza fase

Il GDPR e il sistema informativo condividono i dati personali, ma sono fondalmente estranei. Parlano delle lingue differenti che bisogna continuamente tradurre.

Non esiste una ricetta unica per ogni azienda; bisogna andare nel merito di come l'azienda è fatta, come sono fatti i suoi sistemi informativi e come l'azienda e l'IT dovranno trasformarsi secondo un piano strategico.
Però è possibile dare alcuni suggerimenti:

- È importante fare l'analisi del rischio partendo da dei registri dei trattamenti di buona qualità. Affinché siano efficaci essi devono contenere l'informazione degli asset IT tramite i quali si effettua il trattamento.
- Nel definire gli investimenti non bisogna accontentarsi dell'obiettivo di compliance. Un investimento IT può dare al business benefici sostanziali in termini di efficacia, efficienza, qualità, flessibilità e reputazione…
- Vale la pena valutare la sostituzione delle applicazioni più vecchie con altre che abbiano "by design" e "by default" considerato il tema della protezione dei dati. Può convenire rispetto a soluzioni tampone soprattutto per le aree vicino al core business aziendale dove il ritorno può essere maggiore.
- Si deve instaurare una relazione positiva con i fornitori affinché diano del software migliore e che si prendano più facilmente in carico la loro parte di responsabilità. Un buon fornitore può portare in campo esperienze multiple e sapere come si fanno le cose.
- Conviene valutare strumenti e metodologie di data governance - metadata management affinché sia più facile riacquisire le conoscenze perse e si creino i presupposti per non riperderle in futuro;
- Negli interventi di adeguamento del software bisogna investire su soluzioni ingegnerizzate per riusare il software e l'esperienza ottenendo una maggior qualità a parità di costo.

Buon viaggio!

Cifratura dei dati personali e adeguamento al nuovo Regolamento Europeo per la Protezione dei Dati Personali (GDPR)

[A cura di Paola Meroni]

Come le moderne tecniche di cifratura possono contribuire ad una efficace protezione dei dati personali e in che misura sono in grado di incrementare il livello di compliance ai più elevati standard di sicurezza e al GDPR.

Attacchi informatici, violazione dei sistemi e delle reti, furto di dati personali, "data breach": ogni giorno, sotto i nostri occhi, il Cybercrime sta assumendo proporzioni tali da richiedere alle aziende e alle organizzazioni pubbliche l'adozione di strategie di difesa adeguate. La protezione dei dati personali assume quindi un ruolo centrale nel momento in cui si tratta di decidere come proteggere i propri asset con modalità adeguate rispetto a quanto richiesto dalle normative e in particolare con quanto prescritto dal recente Regolamento Europeo per la Protezione dei Dati Personali o GDPR. La comprensione e conseguentemente l'adozione delle tecnologie più appropriate a questo scopo costituisce un passaggio fondamentale nella definizione dei piani di sviluppo aziendali (e quindi anche nella quantificazione del budget necessario): la cifratura dei dati è senz'altro tra le misure di sicurezza e di compliance da tenere in considerazione, sulla base delle caratteristiche dei dati trattati e della conseguente valutazione di rischio. Ma cifrare i dati è sempre sufficiente per garantirne una adeguata protezione?

Proviamo quindi a passare in rassegna gli aspetti di compliance agli standard di sicurezza e alle normative vigenti che fanno riferimento alle tecniche di cifratura, le varie opzioni che il mercato mette a disposizione, gli aspetti organizzativi che rendono realmente efficace questa misura di sicurezza.

Cifratura dei dati e standard di sicurezza

La cifratura dei dati è finalizzata alla protezione della confidenzialità, dell'autenticità e dell'integrità delle informazioni; per questo motivo si tratta di una misura tecnica riportata dagli standard di sicurezza più rilevanti, iniziando dallo ISO 27001 per proseguire con lo standard NIST o con il PCI-DSS, solo per citarne alcuni.

La cifratura end-to-end consente, ad esempio, di prevenire attacchi del tipo "man-in-the middle", di proteggere le credenziali evitando quindi i furti di identità, di tutelare la confidenzialità delle informazioni trasmesse, di garantire il non-ripudio di un messaggio, di offrire garanzie sull'autenticità dell'identità di due soggetti che partecipano ad uno scambio di dati.

Le tecnologie che abilitano la cifratura sono quindi, in una parola, le fondamentali alleate della sicurezza delle informazioni, da indispensabile forma di difesa dal cybercrime per arrivare a necessaria garanzia della compliance normativa.

Articolo 32 del GDPR: il principio di responsabilità, la valutazione del rischio e la garanzia di un "livello di sicurezza adeguato"

Nell'articolo 32 il Regolamento Europeo per la protezione dei Dati Personali si sofferma sul principio cardine di "responsabilità", da parte del titolare o del responsabile, nel mettere in atto "misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio". Tra queste misure vengono menzionate la psudonimizzazione e la cifratura dei dati personali. Nel "considerando 83" si sottolinea, in particolare, quanto la valutazione delle più appropriate misure di sicurezza sia la diretta conseguenza di una accurata valutazione del rischio associato al trattamento del dato anche in base alla natura del dato stesso. Tale valutazione di rischio si basa, in fase iniziale, sull'individuazione delle tipologie di dati e della quantità degli stessi nei diversi trattamenti e sul relativo danno in cui potrebbero incorrere gli interessati in assenza di idonee misure di sicurezza. Il rischio effettivo netto è invece il rischio residuo che permane dopo aver applicato le misure di sicurezza adeguate. La riduzione del rischio diviene quindi indice della bontà e dell'efficacia degli interventi/investimenti effettuati per incrementare la sicurezza.

Articolo 33 e 34 del GDPR: la notifica di una violazione dei dati personali all'autorità di controllo

Anche negli articoli del GDPR relativi alla notifica di una violazione dei dati personali, quando questa presenti un rischio elevato per i diritti e le libertà delle persone fisiche, ricorre il fondamentale tema della sicurezza tecnica applicata al dato, e, ancora una volta, la cifratura viene menzionata esplicitamente.
Se, nell'articolo 33, infatti, si stabilisce l'obbligo, per il titolare, di notificare all'Autorità di Controllo l'evento di violazione dei dati personali ove possibile entro 72 ore dal momento in cui il titolare ne è venuto a conoscenza, l'articolo 34 è invece focalizzato sulla comunicazione ai soggetti interessati, che deve avvenire "senza ingiustificato ritardo" da parte del titolare. Tuttavia tale comunicazione non è richiesta se "il titolare del trattamento ha messo in atto le misure tecniche ed organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura".

La normativa, dunque, menziona in più occasioni la cifratura del dato come una misura di sicurezza a disposizione del titolare o del responsabile per tutelare la confidenzialità, ma anche l'integrità, del dato. Ovviamente la normativa non fornisce generalmente mai indicazioni di carattere tecnico e operativo per l'implementazione delle varie soluzioni di sicurezza, e ciò vale anche, naturalmente, per i sistemi di cifratura dei dati.
Proviamo quindi a dare qualche indicazione aggiuntiva di carattere tecnico che sarà da intendersi applicata sia ai dati a riposo, cioè nello storage, sia ai dati in transito, cioè durante il trasporto in rete.

Cifratura per i dati in transito

Il protocollo di riferimento è il TLS (Transport Layer Security) nelle sue ultime versioni, che consente l'utilizzo di protocolli sicuri ad esempio per le comunicazioni su web (HTTPS), o su email. Raccomandato anche l'utilizzo di tunnel VPN, soprattutto per comunicazioni tra reti che debba avvenire su Internet.
Inoltre, l'utilizzo degli algoritmi di cifratura nei certificati non solo garantisce confidenzialità e integrità dei dati scambiati tra le parti ma abilita la mutua autenticazione end-to-end tra le parti stesse aumentando significativamente il livello di sicurezza durante la trasmissione.

Cifratura per i dati "at rest"

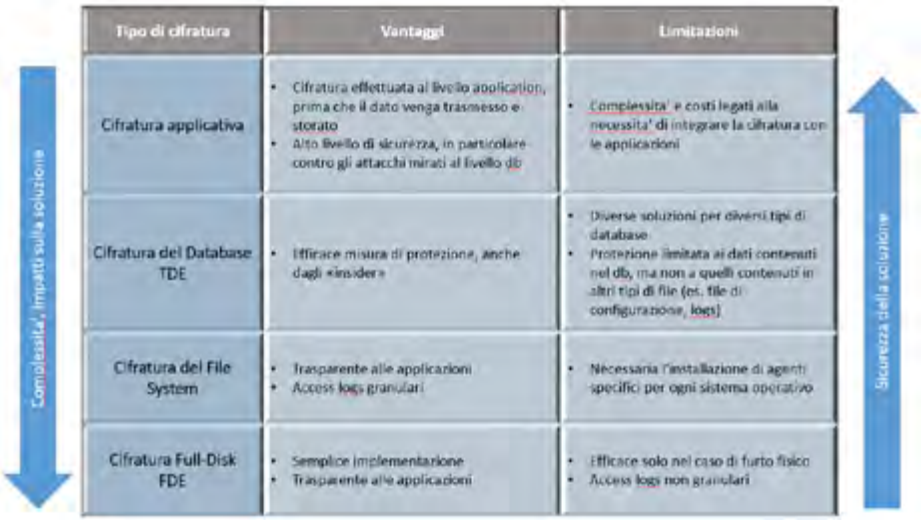
Diverse sono le soluzioni di cifratura "at rest" o "a riposo" disponibili sul mercato. In generale possiamo individuare quattro tipologie di cifratura, effettuate a diversi "livelli":

1. Cifratura a livello del disco (full-disk), o genericamente del media
2. Cifratura a livello del file system
3. Cifratura a livello del database
4. Cifratura a livello applicativo

In generale:

- Più basso è il livello in cui andiamo ad applicare la soluzione di encryption, minori saranno gli impatti sui livelli superiori dello stack applicativo
- Più elevato è il livello in cui andiamo ad applicare la soluzione di encryption, maggiore sarà il livello di sicurezza garantito e la possibilità di mitigare le minacce più diffuse.

Riportiamo uno schema sintetico dei diversi livelli di cifratura rapportati al livello di sicurezza che sono in grado di garantire



Tipo di cifratura	Vantaggi	Limitazioni
Cifratura applicativa	• Cifratura effettuata al livello application, prima che il dato venga trasmesso e storato • Alto livello di sicurezza, in particolare contro gli attacchi mirati al livello db	• Complessita' e costi legati alla necessita' di integrare la cifratura con le applicazioni
Cifratura del Database TDE	• Efficace misura di protezione, anche dagli «insider»	• Diverse soluzioni per diversi tipi di database • Protezione limitata ai dati contenuti nel db, ma non a quelli contenuti in altri tipi di file (es. file di configurazione, logs)
Cifratura del File System	• Trasparente alle applicazioni • Access logs granulari	• Necessaria l'installazione di agenti specifici per ogni sistema operativo
Cifratura Full-Disk FDE	• Semplice implementazione • Trasparente alle applicazioni	• Efficace solo nel caso di furto fisico • Access logs non granulari

Ciò che osserviamo, quindi, è che la tecnologia adottata per la cifratura è fortemente dipendente da molti fattori propri dell'ambiente in cui questa andrà applicata, tra cui:
- una valutazione dell'attuale livello di protezione dei dati e del livello di rischio associato alla loro gestione
- la complessità tecnologica di servizi e applicazioni aziendali
- la presenza di sistemi e applicazioni legacy
- la misura in cui sono già state implementate adeguate misure di protezione fisica e logica.

Scegliere, quindi, la più opportuna strategia di cifratura significa avere una visione chiara dell'attuale "fisionomia" tecnologica della propria azienda, con l'obiettivo di mitigare i rischi del presente ma sempre con uno sguardo attento ai futuri piani di sviluppo e di investimento tecnologico.

Le tecnologie di cifratura a supporto di una corretta Governance della Sicurezza
Lo abbiamo detto: cifrare i dati significa introdurre un importante livello di sicurezza ma richiede di sapere esattamente cosa, dove e come cifrare. Le tecnologie di cifratura sono molteplici ma hanno un costo in quanto l'introduzione di un layer di cifratura:
- può comportare un aumento della potenza di calcolo richiesta e quindi vanno condotte attente valutazioni relative al dimensionamento delle risorse.
- rende certamente necessario un assessment di dettaglio del tipo di dato interessato (personale, ma non solo) e delle applicazioni e infrastrutture che lo trattano e lo rendono disponibile

- richiede una verifica preliminare sulla reale applicabilità di una efficace modalità di cifratura sui sistemi più datati, cosa che di per sé deve anche spingere ad una riflessione sulla necessità di uno svecchiamento delle tecnologie in uso
- introduce significativi impatti anche a livello organizzativo, in particolare per quanto riguarda attività come la corretta gestione (generazione, rinnovo, revoca, backup, ripristino) delle chiavi di cifratura: l'assegnazione di ruoli e responsabilità in questo senso diventa cruciale in quanto questo aspetto, se non governato in maniera rigorosa, rischia di minare o vanificare completamente la reale efficacia della soluzione tecnica.

L'azienda o organizzazione che mette in campo una misura di sicurezza come la cifratura impegna quindi risorse economiche che si traducono in tecnologie e persone con skill adeguati, allo scopo di garantire non solo la compliance normativa ma anche una concreta protezione del più importante degli asset aziendali, l'insieme dei dati che ogni giorno vengono trattati per supportare il Business.
L'impianto di Policy e Procedure, che costituiscono l'ossatura della Governance aziendale, rivestono un ruolo fondamentale nell'indirizzare concretamente l'utilizzo delle tecnologie di encryption prescrivendone l'obbligatorietà quando il dato trattato possieda caratteristiche tali da renderlo particolarmente critico, ad esempio:
- per la protezione dei dati classificati come Confidential o Secret (in una policy sulla Data Classification)
- per la protezione dei dati personali, dal dato anagrafico al dato "particolare", sia at rest sia in transito over Internet (in una policy sulla gestione della Privacy)
- per i dati di pagamento
- in ambito Big Data
- quando il dato è ospitato in Data Center esterni o presso Cloud Provider.

In particolar modo nei grandi Data Center, dove il livello di rischio associato alla gestione di dati personali risulta elevato a causa del trattamento massivo di dati personali di un numero ingente di soggetti interessati, la cifratura del dato farà certamente parte delle misure di sicurezza ritenute adeguate per la gestione dello stesso.

Il richiamo al tema delle Policy ci porta però rapidamente ad ampliare il nostro sguardo sull'insieme delle misure di sicurezza di cui certamente la cifratura del dato fa parte: è necessario un approccio olistico in cui la sicurezza tecnologica applicata a sistemi, applicazioni e infrastrutture, la sicurezza fisica, i processi di account management, i processi di sicurezza operativa, un impianto di policy e procedure aggiornato, la formazione costante del personale, la costituzione di una cultura aziendale della sicurezza e un profondo commitment trasversale alle varie funzioni aziendali, concorrano in maniera sinergica alla creazione di un "sistema" di protezione dei dati realmente efficace.

Per concludere

La cifratura è quindi un alleato potente al fianco delle organizzazioni nella difesa dei dati personali dalle minacce informatiche e a garanzia della necessaria compliance a livello normativo, ma non solo: superando una logica implementativa legata al rispetto del puro obbligo normativo, l'attivazione di robuste metodologie di cifratura, affiancata ad una Governance della sicurezza ad ampio spettro, può costituire un importante fattore differenziante nell'offerta di prodotti e servizi destinati a clienti business o consumer sempre più esigenti e consapevoli.

Intelligenza Artificiale: il Buono, il Brutto, il Cattivo

[a cura di Fabio Roli, Università di Cagliari]

Uno dei padri dell'intelligenza artificiale, Marvin Minsky, definì l'intelligenza una "suitcase word", una parola che contiene in sé stessa molti significati e che pertanto si presta a generare ambiguità e confusione se non chiariamo bene in che senso parliamo di "intelligenza". Èanche per questo che scrivere un articolo non strettamente tecnico sull'intelligenza artificiale è sempre un rischio, specialmente per un addetto ai lavori e specialmente oggi che il il termine intelligenza artificiale è più che mai una "valigia" in cui tutti mettono un po' di tutto. In questo articolo ho cercato di disfare almeno un po' questa valigia e di mettere ordine. L'ho fatto seguendo il mio personale gusto. Come il lettore noterà subito il titolo è un piccolo tributo al celebre film di Sergio Leone. Non sono il primo a usare questo leitmotiv per parlare di intelligenza artificiale. L'intelligenza artificiale ha sicuramente degli aspetti che possono essere definiti "buoni", "brutti" e "cattivi", metterli in evidenza aiuta a comprendere che cosa sia l'intelligenza artificiale oggi. Sempre tenendo a mente che, come nel caso dei tre personaggi del film, il buono, il brutto e il cattivo non possono essere separati nettamente.

Breve storia dell'Intelligenza Artificiale

Sebbene la riflessione sulla possibilità di costruire macchine intelligenti preceda di molto l'invenzione dei moderni calcolatori elettronici[1] gli addetti ai lavori concordano nel dire che il termine "Intelligenza Artificiale" (IA o AI all'inglese nel seguito) sia stato coniato nel leggendario "workshop" di Dartmouth dell'Agosto 1955, dove un piccolo gruppo di scienziati, oggi ritenuti i padri dell'IA, si era dato come obiettivo quello di simulare alcuni aspetti dell'intelligenza umana con un calcolatore[2]. Nei primi vent'anni dell'IA (1950-1970) prevalse fra i ricercatori una visione dell'intelligenza come prodotto del ragionamento "logico" e "simbolico" e tale ragionamento veniva "implementato" su calcolatore con algoritmi di "ricerca" (**Figura 1**). L'obiettivo era simulare l'intelligenza umana nella soluzione di semplici giochi e nella dimostrazione di teoremi. Ben presto divenne chiaro che questi algoritmi di ricerca non potevano essere usati per risolvere problemi reali come il movimento di un robot in una stanza sconosciuta: sarebbe servita un'enorme "conoscenza" del mondo reale per evitare un'esplosione "combinatoriale" del problema di ricerca.

[1] Si pensi alla riflessione sul dualismo mente/corpo di Renato Cartesio

[2] Dartmouth Research Project: https://www.aaai.org/ojs/index.php/aimagazine/article/view/1904

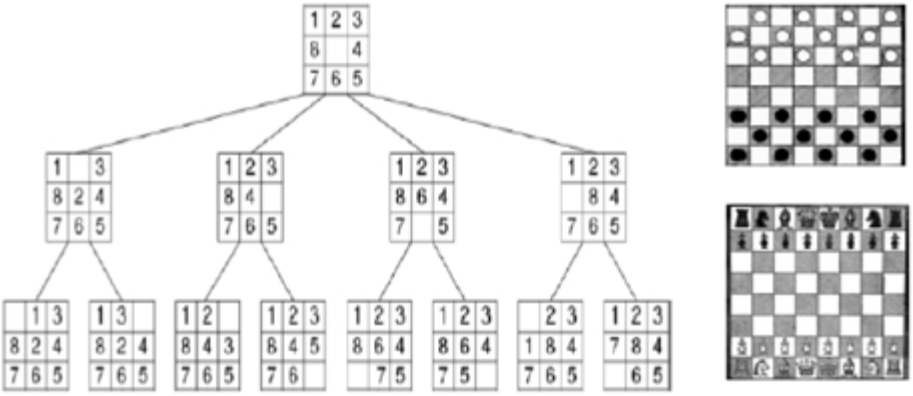


Figura 1 - *Intelligenza come "ricerca" di soluzioni*

Negli anni '80 si decise pragmaticamente di limitarsi alla simulazione di comportamenti intelligenti per la soluzione di problemi molto specifici quali la diagnosi medica di una particolare patologia. Fu questa l'epoca dei così detti "sistemi esperti" in grado di simulare con successo l'intelligenza di un esperto umano in ambiti ristretti e ben definiti[3]. Parallelamente crebbe la consapevolezza che alcuni comportamenti intelligenti come il riconoscimento della parola scritta non potevano essere realizzati con un algoritmo fatto di una sequenza di istruzioni definite a priori. Era invece possibile collezionare molteplici esempi degli oggetti da riconoscere e usare algoritmi che ne imparavano le caratteristiche essenziali (**Figura 2**).

Fu la nascita di quello che oggi chiamiamo "machine learning": il processo di apprendimento dei calcolatori poteva essere formulato come un problema di ottimizzazione matematica e spiegato con modelli probabilistici e statistici [1]. Alcuni degli algoritmi di apprendimento che si ispiravano al cervello umano vennero chiamati "reti neurali artificiali" (**Figura 3**).

[3] https://www.britannica.com/technology/expert-system

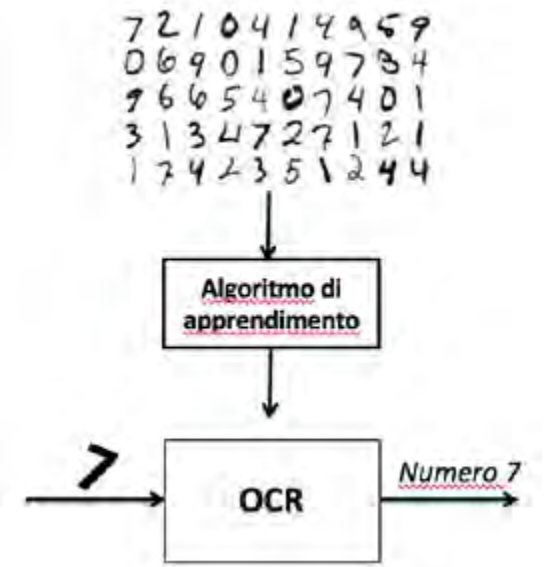


Figura 2 - *Apprendimento automatico da esempi ("machine learning")*

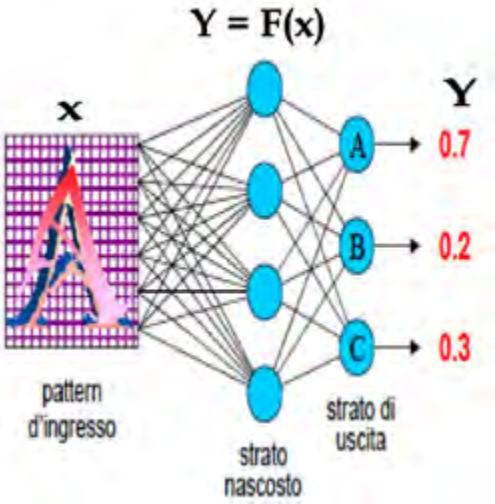


Figura 3 - *Reti neurali artificiali*

Nei suoi primi quattro decenni l'IA è passata attraverso periodi di euforia seguiti da fasi di ristagno causate dalle aspettative disattese ("AI winter"). All'inizio degli anni 2000 la progressiva verticalizzazione su problemi specifici e gli investimenti crescenti hanno portato ai primi traguardi storici: sistemi di IA con prestazioni superiori a quelle degli esseri umani in compiti molto specifici[4]. Fino all'attuale fase nella quale l'enorme disponibilità di dati ("big data") unita alla crescente potenza dei calcolatori ha consentito di mettere a frutto la ricerca dei decenni precedenti all'interno dei modelli di IA ad apprendimento profondo ("deep learning"), dando il via a quello che alcuni ritengono l'inizio della quarta rivoluzione industriale (**Figura 4**).

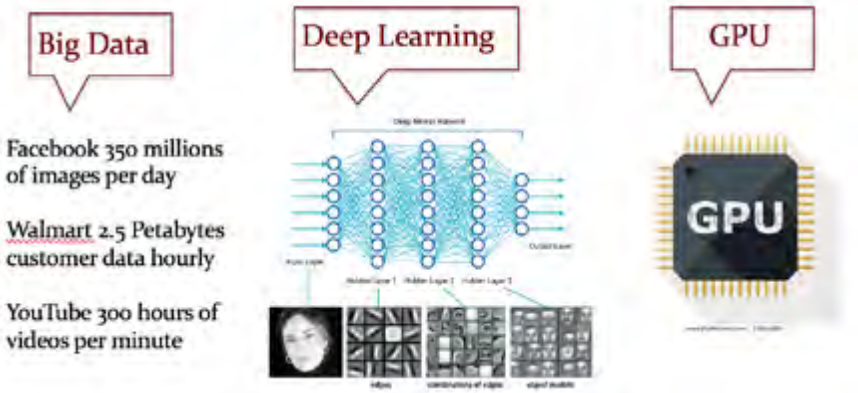


Figura 4 - *Il paradigma del "deep learning"*

Cosa vuol dire che una macchina è "intelligente"?

Con l'invenzione dei calcolatori la discussione sulla natura dell'intelligenza che aveva impegnato i filosofi per migliaia di anni si è concretizzata nella domanda del titolo. Già qualche anno prima del convegno di Dartmouth un altro dei padri storici dell'IA, Alan Turing, si era posto questa domanda e nel cercare una risposta aveva proposto un "test", oggi noto come "test di Turing", per valutare l'intelligenza di una macchina [2]. Supponiamo di mettere in una stanza un essere umano e un calcolatore che sostiene di essere intelligente.

Un altro essere umano, il "giudice", può comunicare con loro in forma scritta e parlata, ma senza vederli. Il giudice pone una serie di domande ai due interlocutori e poi decide chi è l'essere umano (**Figura 5**). L'errore del giudice è la prova dell'intelligenza della macchina, è la prova che la macchina è indistinguibile da un essere umano intelligente.

Questa definizione d'intelligenza risolve molte delle ambiguità che si incontrano nel definire cosa sia l'intelligenza. Non pretendiamo che il calcolatore pensi come noi o ragioni come noi, così come non abbiamo preteso che gli aerei volino come uccelli.

[4] https://www.scientificast.it/uomo-vs-macchina-watson-gioca-jeopardy/

Ci accontentiamo che il calcolatore non sia distinguibile da un essere umano per una serie di compiti che richiedono quella che chiamiamo intelligenza. La complessità e la vastità dei compiti richiesti distingue quella che è stata definita "Narrow AI" (intelligenza artificiale limitata, quella degli attuali calcolatori che giocano a scacchi) dalla "General AI" dei futuri sistemi che dovrebbero essere in grado di mostrare un'intelligenza di livello umano, o superiore, per una vasta gamma di compiti.

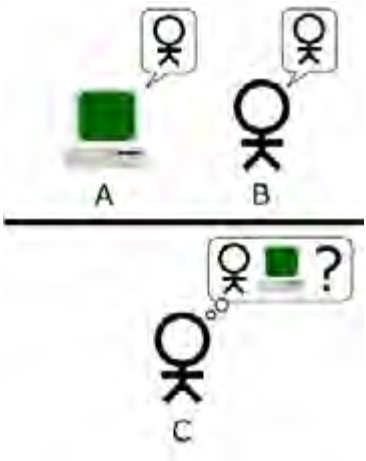


Figura 5 - *Il test di Turing ("the imitation game")*

Il buono

Nel seguito illustro tre aspetti dell'IA che, a mio personale giudizio, la rendono una tecnologia benefica per lo sviluppo economico e sociale.

IA è buona perché funziona (se usata per quello che oggi può fare…)

Come ha ben descritto Rodney Brooks, professore del MIT e fondatore delle aziende Rethink Robotics and iRobot, nel suo articolo sui "sette peccati capitali" dell'IA, c'è in giro molta confusione su cosa oggi l'IA può fare e non fare [3]. Molte delle persone chiamate a prendere delle decisioni sull'IA oscillano fra aspettative irrealistiche e sfiducia immotivata. La confusione è spesso aumentata da messaggi pubblicitari che definiscono "intelligenti" dei prodotti che usano delle tecnologie tradizionali in modo leggermente diverso. Il problema di fondo è una mancata comprensione di come funziona e cosa può fare l'IA.

L'IA oggi è sostanzialmente "machine learning" unito a grandi capacità di memorizzazione ed elaborazione dati e come tale è in grado di "generalizzare" dai casi visti durante la fase di apprendimento a nuovi casi su cui si troverà ad operare. Addestro gli algoritmi di IA con milioni di immagini di oggetti e questo li rende capaci di riconoscere le stesse tipologie di

oggetti in nuove immagini che l'algoritmo non aveva ancora visto, con una precisione che di recente ha superato quella dell'essere umano[5]. Ma il buon funzionamento, o come dicono gli addetti ai lavori la capacità di "generalizzazione" dell'attuale IA, dipende fortemente dall'assunto che il "futuro", i nuovi casi da riconoscere, non sia troppo diverso dal "passato", i casi già imparati. Fra i futuri casi mai visti e quelli passati deve esistere una relazione probabilistica che garantisce la così detta "stazionarietà" dei dati; questione tecnica difficile, ma ben nota dal punto di vista pratico nel settore della sicurezza informatica: gli attacchi "mai visti prima", senza nessuna relazione con quelli passati (gli "unknown unknowns" di Donald Rumsfeld[6]), non si possono prevedere, almeno non con l'IA attuale. L'altro elemento rilevante per il buon funzionamento dell'odierna IA è la "qualità" dei dati forniti in fase di addestramento, quando l'algoritmo impara.

La questione è tecnicamente complessa ma semplice da intuire: gli errori, di varia natura, presenti nei dati di addestramento possono causare errori più o meno gravi nel funzionamento della nostra IA. Se addestro un algoritmo a discriminare fra applicazioni legittime e maligne ("malware") ma gli mostro soprattutto esempi dove il malware è un file compresso (uno zip), l'algoritmo imparerà erroneamente che tutti i file compressi sono maligni.

Se addestro un algoritmo a predire la probabilità che una persona commetta un crimine ma gli mostro solo esempi dove i criminali sono persone di colore l'algoritmo imparerà che tutte le persone di colore hanno un'alta probabilità di commettere un crimine. Sembrerebbe banale evitare questi errori, ma così non è quando i dati di addestramento sono milioni e provengono da sorgenti disparate dalla rete Internet. In conclusione l'IA odierna è buona perché funziona, in alcuni casi anche meglio degli esseri umani, ma per farla funzionare occorre comprenderne bene le ipotesi di buon funzionamento.

IA è buona perché è utile

Assunto che l'IA funziona se la si usa per quello che può fare, la domanda successiva è ovviamente: quello che oggi può fare è utile? La risposta è positiva, esistono molte applicazioni a grande valore aggiunto che soddisfano le ipotesi di buon funzionamento dell'IA o dove l'uomo può sopperire facilmente alle attuali limitazioni dell'IA. Per comprendere a fondo la concreta utilità dell'IA è importante capire che l'IA non deve necessariamente funzionare senza l'uomo per essere utile, non servono futuristici sistemi intelligenti completamente "autonomi", è più che sufficiente che l'IA possa sostituire l'uomo in alcune parti di un compito ("automazione") o che possa collaborare con l'uomo per svolgere meglio o con meno sforzo un certo compito ("human-machine teaming")[7]. L'IA non ha avuto bisogno di diventare completamente "autonoma" per essere utilissima nel settore automobilistico.

I sistemi ADAS (Advanced Driver Assistance Systems) sono ormai a bordo di molti autovei-

[5] http://www.cinaforum.net/riconoscimento-immagini-baidu-batte-google/

[6] http://archive.defense.gov/Transcripts/Transcript.aspx?TranscriptID=2636

[7] https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf

coli e utilizzano tecnologie di IA sviluppate nei decenni scorsi per coadiuvare il guidatore in alcuni compiti come la frenata per evitare la collisione con un pedone. In alcune applicazioni l'IA può essere utilissima perché è complementare all'uomo. In un recente studio medico per la diagnosi del cancro si è mostrato che un sistema progettato per far collaborare l'IA e un radiologo aveva prestazioni nettamente migliori della sola IA o del solo radiologo. Ciascuno era complementare all'altro[8].

IA è buona per un "moon shot approach"

A uno sguardo retrospettivo il progetto dell'Agosto 1955 dei padri dell'IA potrebbe sembrare un esempio di quello che oggi chiamiamo "moon shot approach"[9]. Un progetto super ambizioso con un obiettivo "incredibile", ma che può produrre risultati e vantaggi anche se non lo raggiungi. Il progetto che diede il nome all'approccio "moon shot" fu coronato dal successo, il 21 Luglio 1969 un uomo mise piede sulla luna.

L'originale progetto dell'IA non ha portato dove pensavano i padri fondatori, non abbiamo robot con un'intelligenza umana, ma abbiamo Alexa, l'autore di questo articolo prende finalmente il taxi in Cina senza foglietti con la traduzione in cinese del nome dell'albergo[10], e molti altri risultati concreti e utili. La storia può ripetersi anche oggi. L'IA può davvero innescare dei progetti "moon shot" a livello di singoli paesi e a livello sovranazionale. Alcuni paesi hanno già lanciato i loro progetti "moon shot" sull'IA. La Cina ha annunciato nel 2017 il suo piano strategico per la supremazia mondiale nell'IA, con più di 10 trilioni di RMB di investimento. Gli Stati Uniti pur non avendo un piano strategico simile a quello cinese mantengono a livelli altissimi le attività e gli investimenti sull'IA, alcuni rapporti non classificati dicono che il solo Pentagono voglia investire qualcosa come 7,4 bilioni di dollari sull'IA.

La Commissione Europea sta portando avanti un programma coordinato sull'IA[11]. Molti altri paesi hanno annunciato le loro strategie nazionali sull'IA (**Figura 6**) [4]. Non ultima l'Italia che ha recentemente creato un laboratorio nazionale sull'IA[12].

8 https://arxiv.org/pdf/1606.05718v1.pdf

9 https://whatis.techtarget.com/definition/moonshot

10 https://www.travelchinacheaper.com/best-voice-translation-apps-for-china

11 https://ec.europa.eu/digital-single-market/en/artificial-intelligence

12 https://www.consorzio-cini.it/index.php/it/laboratori-nazionali/artificial-intelligence-and-intelligent-systems

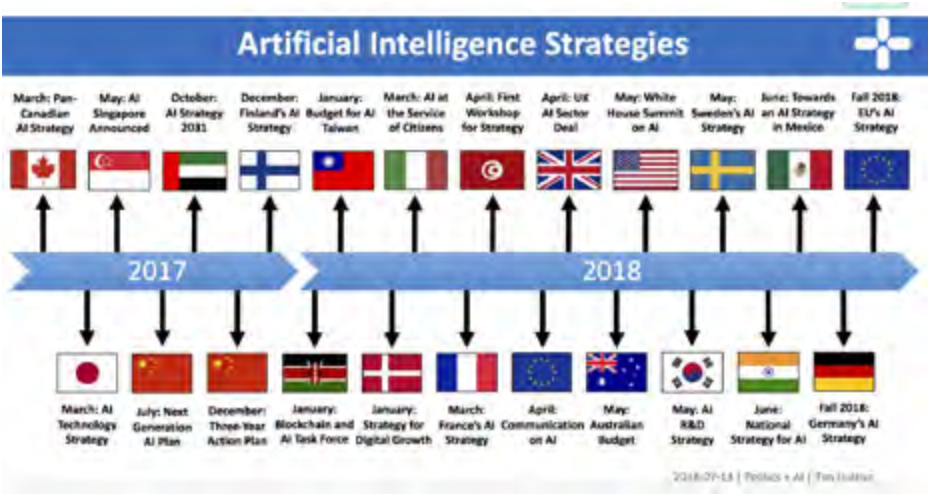


Figura 6 - *Strategie sull'intelligenza artificiale nel mondo*

Il brutto

Nel seguito illustro due aspetti che considero "brutti" nel senso di estremamente critici per il futuro dell'IA. Vanno a mio avviso considerati con estrema attenzione, pena un altro "inverno" dell'IA con ridotto interesse e finanziamenti tagliati.

Ci possiamo fidare dell'IA?

La storia insegna che creare "fiducia" in una tecnologia è fondamentale per farla diventare di largo uso e massimizzarne i benefici. L'IA non fa eccezione. Un esempio paradigmatico è quello di "Watson for Oncology" di IBM, tecnologia basata sull'IA sviluppata per coadiuvare i medici nel trattamento di dodici tipi di cancro[13]. I risultati della sperimentazione hanno mostrato che i medici non si fidavano del sistema Watson e usavano i suoi consigli solo quando coincidevano con le loro opinioni, altrimenti tendevano a pensare che Watson stesse sbagliando. D'altronde la fiducia umana è spesso basata sulla nostra comprensione di come pensano gli altri e sull'esperienza fatta della loro affidabilità; dell'IA abbiamo ancora poca esperienza e il suo funzionamento è spesso poco comprensibile alla maggioranza.
Per questi motivi la Commissione Europea ha messo al centro della sua strategia sull'IA lo sviluppo di una "Trustworthy AI made in Europe"[14]. L'obiettivo è promuovere lo sviluppo di una tecnologia che rispetti i diritti fondamentali dei cittadini europei e sia tecnicamente affidabile.

[13] http://theconversation.com/people-dont-trust-ai-heres-how-we-can-change-that-87129

[14] https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_draft_ethics_guidelines_18_december.pdf

Explainable AI

Una delle chiavi per una "Trustworthy AI" sarà rendere la tecnologia "trasparente". I nuovi algoritmi di "deep learning" stanno rendendo i sistemi di IA sempre più delle "black box", degli oracoli imperscrutabili. Ma l'avvento del GDPR, con l'Art. 22 e altri articoli, sembra imporre un "diritto alla trasparenza" dei cittadini europei. La trasparenza sarà quindi la chiave per costruire e mantenere la fiducia dei cittadini. Sul tema della trasparenza la ricerca sta ponendo grande enfasi sotto il cappello di quella che viene detta "Explainable AI"[15] [6]. L'obiettivo è quello di creare una IA le cui decisioni e azioni siano comprensibili e di cui ci si possa pertanto fidare.

Adversarial Machine Learning

Non ci può essere fiducia senza sicurezza. Il "machine learning" negli anni '80 fu salutato come il "silver bullet" della sicurezza, in particolare della cybersecurity. L'anello forte della catena in grado di rilevare minacce "mai viste prima" che non potevano essere rilevate dai tradizionali sistemi basati su firme[16]. Fu pertanto un piccolo shock quando i ricercatori mostrarono che gli algoritmi di machine learning potevano essere facilmente ingannati, fino al punto da fargli riconoscere un autobus per uno struzzo (**Figura 7**).
Oggi la ricerca dedica grande attenzione alla sicurezza e l'adversarial machine learning (apprendimento automatico in ambiente ostile) è uno dei temi di maggior interesse [7].

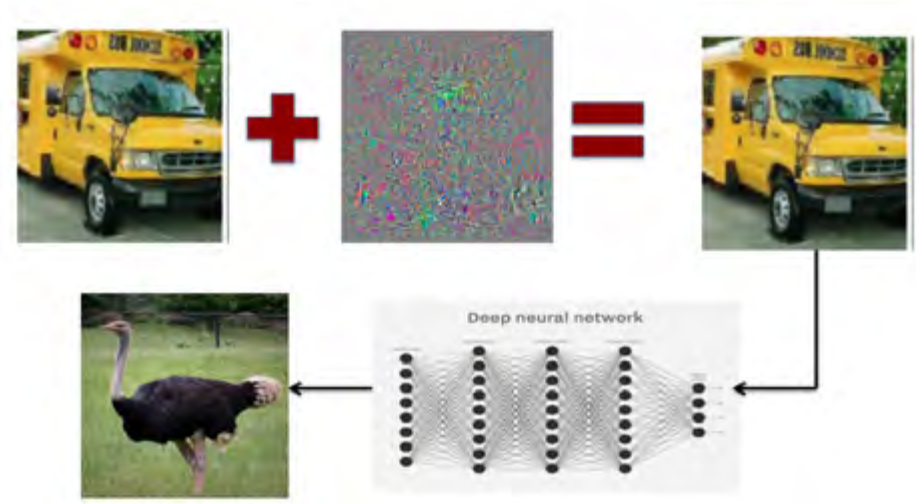


Figura 7 - *Adversarial Machine Learning [7] - https://sec-ml.pluribus-one.it*

[15] https://www.darpa.mil/program/explainable-artificial-intelligence

[16] https://it.wikipedia.org/wiki/Signature_based_intrusion_detection_system

Non vi è dubbio che dal risultato della sfida sulla "fiducia" intesa come sicurezza e trasprenza dipenderà il futuro dell'IA.

Ignoranza e false aspettative

Lo abbiamo già visto negli anni '70 e poi di nuovo negli anni '80, la mancata comprensione su cosa l'IA possa davvero fare può creare false aspettative a cui seguono periodi di disillusione con ridotto interesse e tagli drastici dei finanziamenti. Rodney Brooks ha ben descritto quali sono i principali errori di comprensione e prospettiva [3].
Uno dei pericoli maggiori per il futuro dell'IA è che molti tendono a sovrastimare quello che l'IA può fare oggi e a sottostimare quello che potrà fare in futuro. Vediamo algoritmi in grado di "taggare" una foto con la frase "persona che gioca a frisbee" e automaticamente sovrastiamo quello che l'algoritmo può fare: pensiamo che possa riconoscere il nostro volto in una foto anche a distanza di anni. Crediamo a chi scrive che i robot sostituiranno tutti i muratori in 10 anni quando invece le abilità manuali degli attuali robot sono ancora limitatissime se l'ambiente di lavoro non è ben noto.

Il cattivo

Sugli aspetti "cattivi", nel senso di pericolosi, dell'IA si è scritto molto. Il Future of Life Institute ritiene che l'IA comporti un "rischio esistenziale", sia cioè una delle tecnologie, insieme al nucleare e alle biotecnologie, che, se mal governata, potrebbe portare all'estinzione della razza umana[17]. Altre autorevoli voci sono meno pessimiste. Rodney Brooks ritiene un errore preoccuparsi della possibilità di una intelligenza artificiale "maligna" nei prossimi cento anni[18].
Pur ritenendo importante la discussione sul rischio esistenziale dell'IA nel seguito mi concentrerò su due pericoli a più breve termine.

"Dual use" dell'IA

L'IA è chiaramente una tecnologia con un "dual use", non v'è dubbio che può essere usata sia per scopi civili che militari e, più in generale, per fini benefici e dannosi [5]. Molti dei compiti che l'IA può automatizzare già da ora hanno un intrinseco "duplice uso".
I sistemi intelligenti in grado di trovare delle vulnerabilità nel software possono essere usati sia per scopi difensivi che offensivi, un drone semi autonomo può essere utilizzato per consegnare i pacchi o per trasportare esplosivi. Più in generale la ricerca che mira ad aumentare la nostra comprensione dell'IA, delle sue potenzialità e del nostro controllo su di essa è intrinsecamente di duplice uso. Èquindi di estrema importanza che i ricercatori e più in generale gli addetti ai lavori si assumano la responsabilità di promuovere gli usi vantaggiosi dell'IA e cerchino di prevenire gli usi nocivi.

[17] https://futureoflife.org/background/existential-risk/

[18] https://www.edge.org/response-detail/26057

IA e manipolazione dell'informazione

In un recente articolo Giorgio Giacinto discute il ruolo fondamentale dell'"ingegneria sociale" nella manipolazione dell'informazione e di come essa poggi sull'asimmetria di conoscenze e sul dominio tecnocratico: le maggiori conoscenze e competenze tecniche consentono una facile manipolazione e il controllo dell'informazione[19]. Se questo è vero allora diventa facile capire il ruolo attuale e quello futuro dell'IA nella manipolazione dell'informazione. L'IA può ampliare il divario di conoscenze e competenze tecniche, ma soprattutto l'IA può automatizzare la creazione di disinformazione, disinformazione di cui le "fake news" sono un particolare veicolo. L'esempio più semplice viene dal così detto "spear phishing" dove gli algoritmi di machine learning possono automatizzare la raccolta di informazioni sulle potenziali vittime [5]. Gli algoritmi consentono di sfruttare l'asimmetria di conoscenze di cui sopra. Sulla base dei dati disponibili in rete possono identificare gli utenti meno esperti distinguendoli da quelli che sicuramente sanno cos'è lo spear phishing. I primi sono sicuramente dei buoni obiettivi e delle potenziali vittime di una campagna di spear phishing.
La brevità e la semplicità del linguaggio di alcuni social media hanno già reso possibile l'uso di algoritmi detti "bot" per la manipolazione dell'informazione: la guerra in Siria e le elezioni statunitensi del 2016 sembrano avere dato evidenza di ciò.
Oggi i bot sono ancora guidati da persone ma recenti studi hanno mostrato che un bot ha buona possibilità di sembrare "umano" su Twitter[20]. L'ultima frontiera sembra oggi quella del "deep fake", algoritmi di deep learning in grado di creare foto o video falsi che sono sempre più realistici (**Figura 8**).
Le Cassandre già parlano di "realtà sotto attacco" e invocano futuri Voight-Kampff test[21], ma anche qui ritengo che stiamo sovrastimando il presente e sottostimando il futuro dell'IA. Non sarebbe la prima volta.

[19] http://www.difesaonline.it/evidenza/approfondimenti/campagne-di-manipolazione-dellinformazione-quando-la-difesa-fa-il-gioco

[20] https://www.blackhat.com/docs/us-16/materials/us-16-Seymour-Tully-Weaponizing-Data-Science-For-Social-Engineering-Automated-E2E-Spear-Phishing-On-Twitter-wp.pdf

[21] https://www.youtube.com/watch?v=Umc9ezAyJv0

Figura 8 - *Deep fakes*

Bibliografia

[1] M. Gori, Machine Learning: a constraint-based approach, Morgan Kaufmann, 2017.
[2] A. Turing, Computing Machinery & Intelligence, Mind, Vol. 59(236), 1950.
[3] R. Brooks, The Seven Deadly Sins of AI Predictions, MIT Technology Review, Nov./Dec. 2017.
[4] T. Dutton, An Overview of National AI Strategies, June 2018, https://medium.com
[5] The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. Feb. 2018. https://arxiv.org/pdf/1802.07228.pdf.
[6] M. Melis, Maiorca, D., Biggio, B., Giacinto, G., e Roli, F., Explaining Black-box Android Malware Detection, 26th European Signal Processing Conference (EUSIPCO '18) 2018.
[7] B. Biggio e Roli, F., Wild Patterns: Ten Years After the Rise of Adversarial Machine Learning, Pattern Recognition, vol 2018.

L'Intelligenza Artificiale è Sicura?

[A cura di Battista Biggio, Università di Cagliari]

Lo so, la domanda è mal posta. Non si può dimostrare che un sistema è sicuro, se non in relazione a un definito modello di attacco e sotto assunzioni ben precise.
È invece possibile dimostrare, in modo molto più diretto, quando un sistema è vulnerabile, ed è quello che cercheremo di fare in questo articolo, in relazione ai sistemi di Intelligenza Artificiale (IA).
È noto che la *sicurezza di un sistema dipende unicamente dalla robustezza del suo anello più debole*. L'IA è ormai pervasiva e integrata in maniera trasparente all'utente in diversi scenari applicativi. È quindi lecito chiedersi se, dal punto di vista della sicurezza informatica, questi algoritmi non introducano vulnerabilità nei sistemi che li utilizzano, trasformandosi potenzialmente nell'anello debole della catena. In questo articolo, proveremo a fare un po' di chiarezza su questo problema, discutendo, da una parte, i principali vettori di attacco che possono essere utilizzati per *confondere* un sistema di IA, in diversi contesti applicativi e, dall'altra, le contromisure più promettenti volte a mitigare questo rischio.

La rivoluzione dell'IA nelle applicazioni moderne

L'IA è stata definita la nuova *elettricità*. Andrew Ng, professore aggiunto all' Università di Stanford, co-fondatore di Coursera e chief scientist di Baidu, insieme a molti altri addetti ai lavori, sostiene infatti che gli algoritmi di IA stiano aprendo la via per una nuova rivoluzione industriale.

IA e apprendimento profondo. Qui è necessario fare un doveroso distinguo, per disambiguare il significato della parola IA. In questo contesto, quando si parla di IA, si parla prevalentemente di algoritmi di *apprendimento profondo* o *deep learning*, per usare il più diffuso termine anglofono. Questa categoria di algoritmi appartiene al sottoinsieme degli algoritmi di IA noti come algoritmi di *apprendimento automatico* o *machine learning*. In particolare, il termine apprendimento *profondo* deriva dalla particolare struttura di questi algoritmi, basati perlopiù su reti neuronali *profonde*, ovvero caratterizzate da *molti* strati o livelli, connessi in maniera sequenziale.

La fase di riconoscimento. Assimilando ogni livello ad una operazione di filtraggio del dato in ingresso, l'intuizione dietro il funzionamento di questi algoritmi è quella di applicare una determinata sequenza di filtri al dato in ingresso (ad esempio, una immagine rappresentante un determinato oggetto). Ogni livello, o filtro, è caratterizzato da un insieme di neuroni che vengono attivati solo quando percepiscono una determinata struttura ("*pattern*") al loro ingresso. Questo meccanismo, in linea di principio, permette via via di comprimere l'in-

formazione contenuta nell'immagine di partenza e costruire rappresentazioni più astratte dell'oggetto che si vuole riconoscere, fino a poterne determinare la classe di appartenenza. Nella fattispecie, *classificare* correttamente l'oggetto rappresentato nell'immagine.
Questo comportamento è schematizzato in **Fig. 1**.

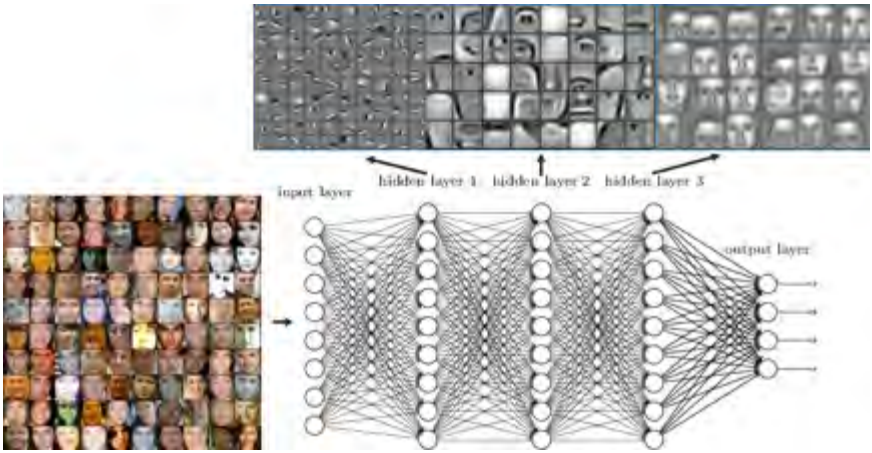


Fig. 1 - *Esempio delle rappresentazioni imparate ai diversi livelli da una rete neurale profonda in un problema di riconoscimento dei volti. Si noti come, attraversando i vari livelli, si passi da rappresentazioni di basso livello (che rilevano bordi, tessiture, ecc.) a rappresentazioni di livello più astratto (dove si riconosce il volto di un determinato soggetto). Fonte: https://www.rsipvision.com/exploring-deep-learning/*

La fase di addestramento. La complessità di questi algoritmi sta chiaramente nel costruire queste rappresentazioni in maniera automatica, ovvero nel comprendere come costruire la sequenza di operazioni di filtraggio da applicare al dato in ingresso. A questo scopo, questi algoritmi necessitano di una fase di *addestramento*, in cui al sistema sono sottoposte diverse immagini di oggetti che il sistema dovrà essere in grado di riconoscere, insieme alla loro etichetta di classe.
Durante la procedura di addestramento, l'algoritmo cerca di predire la classe corretta di questi oggetti e, in caso di errore, corregge i suoi parametri in modo che all'iterazione successiva la predizione risulti diversa, avvicinandosi via via a quella corretta. Questo corrisponde a variare il modo in cui ogni neurone risponde a determinate strutture o *pattern* osservati nei dati.
Alla fine di questo processo, l'algoritmo avrà imparato a distinguere oggetti di classi diverse sulla base di correlazioni statistiche e particolari *pattern* associati alle diverse tipologie di oggetti presenti nei dati.
È facile intuire come questo meccanismo sia profondamente diverso dal complesso proce-

dimento di apprendimento degli umani, non fosse altro per il fatto che noi non abbiamo bisogno di milioni di esempi per riconoscere gli oggetti e il mondo che ci circonda.

Prestazioni super-umane. Tuttavia, stante l'enorme disponibilità di dati che è possibile raccogliere oggi e l'imponente potenza di calcolo dei nuovi calcolatori e delle architetture cloud, in alcuni scenari applicativi specifici, l'apprendimento profondo ha dimostrato di raggiungere perfino prestazioni *migliori* degli esseri umani. Un esempio molto popolare in cui questi algoritmi hanno raggiunto prestazioni cosiddette super-umane è il caso di ImageNet (www.image-net.org). ImageNet è un database contenente più di 14 milioni di immagini e da diversi anni viene usato come base per dar vita alla competizione ImageNet Large Scale Visual Recognition Challenge (ILSVRC). In questa competizione, diversi algoritmi si sfidano per riconoscere correttamente oggetti appartenenti a 1,000 classi differenti.
In **Fig. 2** viene mostrato il progresso della percentuale di errato riconoscimento degli oggetti in questa competizione negli anni. È immediato notare come nel 2015, l'algoritmo migliore della competizione abbia raggiunto un'accuratezza superiore all'accuratezza media riportata dagli esseri umani su questo problema. Per onestà intellettuale, va detto che alcune immagini sono ambigue e noi stessi non saremmo d'accordo su quale oggetto esse rappresentano, ma è comunque sorprendente che un algoritmo automatico registri prestazioni così elevate su una competizione così difficile.

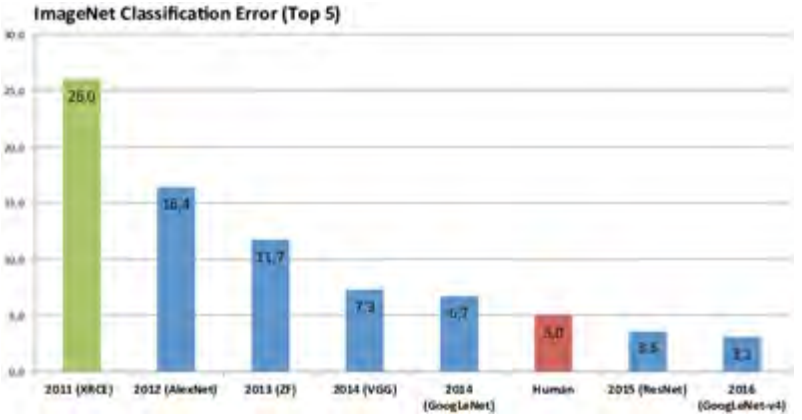


Fig. 2 - *Progresso della percentuale di errato riconoscimento degli oggetti nella competizione ILSVRC negli anni.*
Fonte: https://www.researchgate.net/publication/324476862_Survey_of_neural_networks_in_autonomous_driving/

Il caso di ImageNet, tuttavia, non è il solo a registrare il successo dell'IA. Un altro caso emblematico, e forse anche più conosciuto, è quello dei videogiochi e dei giochi di strategia. Da tempo gli algoritmi di IA si sono dimostrati molto più bravi degli umani nel gioco

degli scacchi, ma ultimamente si stanno dimostrando superiori anche in giochi e videogame molto più complessi, sparatutto inclusi. Di recente, DeepMind ha perfino mostrato che l'IA può imparare autonomamente a sconfiggere giocatori umani molto esperti in un videogame complesso come StarCraft II.[1] Anche qui, la forza del loro algoritmo, chiamato AlphaStar, risiede nella possibilità di poter osservare molti dati. Nello specifico, l'algoritmo può giocare potenzialmente infinite partite e osservarne il risultato. In questo modo, usando *l'apprendimento per rinforzo* è possibile *addestrare* l'algoritmo di IA a migliorarsi partita dopo partita.

Ci sono poi tutta una serie di altre applicazioni dove le reti neuronali profonde hanno stabilito nuovi standard di prestazione, dalla segmentazione e riconoscimento di oggetti nei video,[2] alla diagnosi di particolari malattie fatta a partire da immagini mediche, fino al riconoscimento vocale (si pensi ai numerosi assistenti vocali disponibili oggi sui nostri telefoni cellulari o come assistenti domestici).
Perfino nell'ambito della sicurezza informatica, l'IA viene ormai usata pervasivamente come ausilio nella rilevazione di attacchi informatici, dalla rilevazione di domini e siti web malevoli che perpetrano varie truffe verso gli utenti finali (si pensi alle pagine di phishing o vendita di prodotti farmaceutici illegali), alla rilevazione di intrusione in reti aziendali (tramite profilazione del comportamento dei dipendenti dell'azienda), fino a problemi di video sorveglianza in aree critiche.

Stante quanto detto finora, potrebbe sembrare quindi che l'IA e, in particolare, il deep learning siano il nuovo Eldorado, la panacea di tutti i mali. Ma sappiamo bene che non è tutto oro quel che luccica…

Si può ingannare l'IA?

Gli algoritmi di IA, nonostante il loro nome altisonante, soffrono di allucinazioni piuttosto particolari. Esistono infatti determinate manipolazioni dei dati forniti in ingresso a questi algoritmi che sono capaci di confonderli, in alcuni casi, anche clamorosamente. L'esempio ostile (dall'inglese *adversarial example*) più eclatante e popolare è forse quello riportato in figura 7 dell'articolo di Roli di questo Speciale AI, estrapolato dal famoso articolo scientifico "*Intriguing properties of neural networks*", pubblicato dai ricercatori di Google Brain nel 2013. Questo esempio mostra come una immagine di uno scuolabus, modificata con un rumore *ostile* ma impercettibile all'occhio umano, venga erroneamente riconosciuta come l'immagine di uno struzzo proprio da uno di quegli algoritmi di IA che avevano stabilito un record super-umano su ImageNet.

Dopo questa scoperta, la comunità scientifica si è scatenata, fantasticando di attacchi contro i sistemi di riconoscimento del volto in applicazioni biometriche o forensi (**Fig. 3**), con-

[1] https://deepmind.com/blog/alphastar-mastering-real-time-strategy-game-starcraft-ii/

[2] Un esempio si può trovare nel video a questo link: https://www.youtube.com/watch?v=dYVH3p-RuPQ

tro i sistemi di riconoscimento dei segnali stradali per i veicoli a guida automatica (**Fig. 4**) e perfino contro gli assistenti vocali, mostrando come questi ultimi possano essere confusi da un rumore audio quasi impercettibile all'orecchio umano.[3]

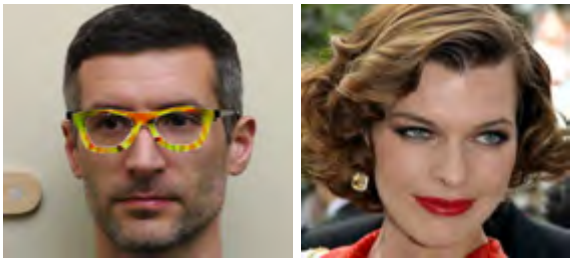


Fig. 3 - *Nell'articolo "Accessorize to a crime: real and stealthy attacks on state-of-the-art face recognition" pubblicato nel 2016, alcuni ricercatori hanno dimostrato che, indossando una bizzarra montatura per occhiali, erano in grado di ingannare un sistema di riconoscimento facciale, inducendolo a credere di essere di fronte alla famosa attrice Milla Jovovich.*

Tuttavia, nonostante l'esuberanza ritrovata dalla comunità scientifica nel 2013, il problema della (in)sicurezza degli algoritmi di IA era già noto da tempo a chi, questi algoritmi, li applicava in problemi di sicurezza informatica. Il motivo è semplicemente che, in queste applicazioni, era chiaro fin dal principio che l'algoritmo di IA avrebbe avuto a che fare con un attaccante intelligente e adattivo, ma soprattutto motivato od incentivato economicamente ad ingannarlo. Già dal 2004, gli algoritmi di IA per il riconoscimento delle email di spam si erano mostrati facilmente vulnerabili ad attacchi mirati, in cui gli spammer potevano alterare il testo delle email senza compromettere la leggibilità del messaggio per gli esseri umani.
E, più recentemente, intorno agli anni 2012-2013, si erano già costruiti algoritmi di attacco in grado di bucare anche le reti neurali.[4]

Fig. 4 - *Nell'articolo "Robust Physical-World Attacks on Deep Learning Models" pubblicato nel 2018, alcuni ricercatori hanno dimostrato come ingannare un sistema di riconoscimento dei segnali stradali a bordo di un veicolo a guida automatica, semplicemente posizionando degli adesivi su un segnale di stop. Davanti a questa manipolazione, l'algoritmo è infatti indotto a riconoscere il cartello come un segnale di limite massimo di velocità.*

[3] Alcuni esempi di attacco audio sono disponibili qui: https://nicholas.carlini.com/code/audio_adversarial_examples/

[4] Per chi volesse approfondire, consiglio la lettura del nostro articolo "Wild Patterns: Ten Years after the Rise of Adversarial Machine Learning", pubblicato nel 2018.

In particolare, lo scenario descritto sopra, identifica solo una particolare vulnerabilità degli algoritmi di IA. Questo scenario, noto anche come *evasion*, consiste nel confondere la classificazione del dato in ingresso manipolandone il contenuto, da parte di un algoritmo precedentemente addestrato.

In uno scenario differente, noto come *poisoning*, l'attaccante può contaminare i dati di addestramento per impedire al sistema di funzionare correttamente, causando un disservizio (*denial of service*) per gli utenti legittimi (ad esempio, impedendo a un dipendente di autenticarsi correttamente sui servizi aziendali), o impiantando delle *backdoor* nel sistema (in modo da potersi garantire accesso ad un sistema protetto, o causare errori di funzionamento del sistema quando il dato in ingresso attiva la *backdoor*).

Esistono anche attacchi che mirano a violare la privacy del sistema di IA o dei suoi utenti. È stato dimostrato infatti che è possibile ricostruire l'immagine del volto di un utente di un sistema di riconoscimento facciale semplicemente osservando ripetutamente l'uscita del sistema su una particolare sequenza di immagini (**Fig. 5**). Questo significa che, quando il sistema viene messo a disposizione come servizio remoto su web, ad esempio, un attaccante che ha facoltà di effettuare richieste ripetute a questo servizio può violarne la privacy.
Usando un meccanismo simile, è perfino possibile "rubare" il modello, costruendone una copia – il che potrebbe essere un problema per un'azienda che offre un servizio di questo tipo a pagamento via web. O ancora, potrebbe essere un problema nel caso in cui l'attaccante riuscisse a replicare il funzionamento di un sistema anti-virus, ad esempio, poiché questo gli faciliterebbe il compito di costruire dei virus informatici in grado di evadere la rilevazione da parte del sistema stesso.

Fig. 5 - *Ricostruzione dell'immagine del volto di un utente, ottenuta mediante una serie di richieste inviate al sistema di riconoscimento facciale. A sinistra si riporta l'immagine originale, a destra quella ricostruita. Fonte: "Model inversion attacks that exploit confidence information and basic countermeasures", 2015.*

Perché l'IA è vulnerabile? E quali sono le possibili contromisure per renderla sicura?

A prima vista, queste vulnerabilità dell'IA possono sembrare piuttosto incredibili, stante le prestazioni super-umane di questi algoritmi in alcuni ambiti applicativi. Tuttavia, la questione risulta molto meno sorprendente se pensiamo a come questi algoritmi "imparano" dai dati. Come detto in precedenza, gli algoritmi di IA imparano da grandi volumi di dati *etichettati* (almeno nel paradigma più diffuso dell'apprendimento supervisionato), secondo un processo di ottimizzazione che via via forza l'algoritmo ad imparare correttamente l'etichetta assegnata ad ogni dato di addestramento, modificandone i parametri interni. Questi algoritmi sono quindi profondamente *influenzati dai dati* utilizzati per il loro addestramento e da come si costruisce il *processo di ottimizzazione* che ne simula l'apprendimento.

È chiaro che, avendo la possibilità di manipolare questi dati e sfruttando le peculiarità del processo di ottimizzazione, questi algoritmi possono essere attaccati, anche in modi diversi e complementari tra loro, come evidenziato in precedenza; ad esempio, introducendo correlazioni spurie nei dati, manipolando l'oggetto che si vuole riconoscere, o ancora alterando i dati di addestramento.
In pratica, la vulnerabilità di questi algoritmi è intrinseca al loro funzionamento e alle assunzioni di fondo sotto cui sono stati progettati; nessuno di essi è stato infatti progettato per riconoscere correttamente alcune particolari trasformazioni *ostili* dei dati in ingresso.

Di recente, la comunità scientifica si è adoperata massicciamente per trovare una soluzione, proponendo una serie di contromisure volte a mitigare il problema. Parecchie di queste contromisure si sono dimostrate inefficaci, ma alcune hanno ottenuto risultati promettenti. In particolare, esistono soluzioni più o meno mature ed efficaci per mitigare il problema della contaminazione dei dati di addestramento e preservare la privacy dei sistemi di IA. Mentre rimane un problema aperto trovare una soluzione realmente efficace per gli attacchi evasivi volti a confondere il sistema di IA in fase di classificazione.

Tra le soluzioni più promettenti alle varie tipologie di attacco, è sempre possibile trovare un denominatore comune, ovvero una modellazione più o meno esplicita delle potenziali manipolazioni dei dati che il sistema può incontrare. In sostanza, quello che si cerca di fare è fornire al sistema di IA una conoscenza aggiuntiva su come può comportarsi un attaccante, conoscenza che tipicamente non è e non può essere disponibile nei dati di addestramento. Questo è abbastanza chiaro nel caso degli attacchi informatici, dove non è possibile aspettarsi di avere una collezione esaustiva e rappresentativa di tutti i potenziali attacchi, che sono anzi molto rari. Non a caso, il problema dei cosiddetti attacchi *zero day,* mai visti prima, rimane un nervo scoperto nelle applicazioni di cybersecurity.

La sfida è dunque aperta. Come modellare gli attacchi per migliorare la sicurezza dei sistemi di IA in maniera proattiva e come integrare questi modelli nel processo di appren-

dimento, per renderlo *secure by design* rimane tutt'oggi un problema complesso. Alcuni immaginano che, in futuro, gli algoritmi di IA si sfideranno uno contro l'altro emulando un gioco tra attaccante e difensore, altri sostengono che questo non sia sufficiente e l'esperienza dell'esperto umano sia imprescindibile per migliorare realmente la sicurezza di questi sistemi. La risposta, come sempre, è: *there's no free lunch* – molto probabilmente, non esiste una soluzione generale al problema, ma andranno studiate soluzioni diverse, specializzate sui diversi contesti applicativi.

L'intelligenza artificiale come strumento "dual use" nella cybersecurity

[A cura di Federico Santi e Danilo Benedetti, DXC Technology]

Tra le innumerevoli applicazioni degli algoritmi di intelligenza artificiale, un campo non secondario è rappresentato dalla cybersecurity, dove già da diversi anni sono presenti strumenti di sicurezza che utilizzano tali algoritmi per potenziare la capacità di individuare le minacce. La flessibilità e le potenzialità di questi algoritmi, unite alla larga disponibilità di kit software per la loro implementazione, offrono però un'opportunità anche ai cyber criminali, che potranno usare tali capacità per accrescere la sofisticazione o l'ampiezza degli attacchi. L'unione di queste due tendenze segnerà molto probabilmente l'avvio di una "corsa agli armamenti", tra attacco e difesa, per cui il ruolo dell'intelligenza artificiale acquisirà un'importanza crescente per i due schieramenti. L'articolo si pone l'obiettivo di descrivere le opportunità, e le minacce, che l'introduzione dell'IA in ambito cyber porta con sé.

La tempesta perfetta

È ormai un dato acquisito, confermato dalla nostra esperienza, che uno dei più importanti trend degli ultimi 20 anni è il progressivo spostamento della nostra vita nel dominio digitale. A partire dagli anni '90, con la diffusione di sistemi di accesso sempre più efficienti ed economici, prima su computer fissi, mediante linea telefonica tradizionale, poi più recentemente su cellulari e smartphone, l'utilizzo di servizi Web è diventato capillare, e sempre più persone utilizzano questo medium per attività che normalmente richiedevano un'interazione "fisica".

Il successo e la diffusione di reti di accesso sempre più ramificate e ubique, accompagnata alla crescente miniaturizzazione dei dispositivi di accesso, hanno permesso di estendere rapidamente il numero e la varietà dei dispositivi connessi. Questa esplosione nel numero di dispositivi e di "casi d'uso" ha generato una più che proporzionale crescita dell'utenza (interna ed esterna) sempre più distribuita e contemporaneamente dei dati generati, trasmessi, scambiati, memorizzati, correlati, che nascondono un valore, potenzialmente molto elevato, per chi questi dati è in grado di raccogliere e filtrare.

Assistiamo ora alla contemporanea e repentina accelerazione di questi fenomeni: l'esplosione del volume dei dati, la decentralizzazione delle architetture logiche e tecnologiche, la natura nativamente digitale dei nuovi processi di business e il boom dei dispositivi.

In questo scenario, l'emergenza di tre tecnologie apparentemente distinte, ma in realtà strettamente correlate, non è casuale: lo sviluppo e la rapida diffusione di oggetti interconnessi, capaci di elaborazione propria, la contemporanea espansione di algoritmi e tecniche di Intelligenza Artificiale e, infine, l'avvento di soluzioni "cloud" caratterizzate da rapida scalabilità verso l'alto sia della capacità elaborativa, sia dello spazio di storage. Fra queste tecnologie esiste un evidente legame: la mole enorme di dati generati dai dispositivi IoT richiede da un lato l'uso di algoritmi che siano in grado di estrarre efficacemente valore, sia per l'utilizzatore, sia per chi utilizza i dati per la vendita di prodotti e servizi. Dall'altro, la raccolta di questi dati e l'utilizzo di algoritmi di machine learning e di intelligenza artificiale, peraltro in continua evoluzione, si adattano perfettamente al modello "elastico" e scalabile offerto dal Cloud.

Va sottolineato inoltre che le capacità introdotte dall'Intelligenza Artificiale costituiscono un abilitatore di comportamenti autonomi e di capacità che contribuiscono a facilitare la diffusione e l'utilità dei sistemi IoT, seppure spesso appoggiandosi, per le computazioni più complesse, a sistemi in cloud.

Per le strutture che si occupano di sicurezza informatica, il governo e la protezione dei dati e dei sistemi, sia per quanto attiene alle caratteristiche proprie di ciascuno dei tre elementi, sia alle loro interazioni, è dunque una sfida centrale.

Due sono le direzioni di indagine che ci interessa approfondire in questa sede.

La prima, è la possibilità di utilizzare tecniche ed algoritmi di intelligenza artificiale per rafforzare le difese di un'organizzazione.

La seconda, speculare alla prima, affronta invece la possibilità che l'intelligenza artificiale venga utilizzata per rendere più efficaci o più estesi gli attacchi.

Sicurezza e Intelligenza Artificiale

Il ruolo crescente che la tecnologia ha nelle nostre vite quotidiane nei luoghi di lavoro, la crescita del cloud e delle tecnologie IoT e mobili hanno innescato una sorta di reazione a catena in termini di rischi per la sicurezza. Il numero enorme e crescente di dispositivi collegati in rete rappresenta uno scenario da sogno per i cyber criminali, con nuovi e abbondanti punti di accesso a disposizione, spesso scarsamente protetti.

Per le imprese, il desiderio di beneficiare dei vantaggi legati all'utilizzo di sistemi IoT è temperato dai timori generati dalle continue notizie di violazioni della sicurezza, con conseguenti titoli ad effetto sui giornali, che spingono le aziende a ricercare una maggiore protezione contro questo tipo di eventi. Le tecnologie e i metodi per la protezione delle informazioni usate tradizionalmente nelle industrie diventano però rapidamente proibitive, in termini di risorse economiche e umane richieste, al crescere del numero di dispositivi da

proteggere e della mole di dati trattati. Si palesa dunque la necessità di affiancare o integrare i metodi tradizionali, in ultima analisi incentrati sull'impiego di specialisti umani, con sistemi automatici basati sull'intelligenza artificiale, che possano aumentare la capacità di analisi degli specialisti in alcune delle fasi di gestione degli incidenti di sicurezza informatica, quando non automatizzandola del tutto.
Senza entrare in dettagli molto tecnici, un attacco informatico può essere suddiviso nelle fasi di ricognizione dell'obiettivo, realizzazione dell'attacco, violazione dei sistemi e esecuzione dell'attacco[1].

Figura 1 - *Le fasi di un attacco, semplificazione da Cyber Kill Chain®*

La capacità di riconoscere e identificare le diverse fasi di un attacco informatico è un fattore chiave nella protezione degli asset informatici. Tradizionalmente ciò viene effettuato per mezzo di sistemi in grado di individuare alcuni tipi di minaccia, bloccandoli, per mezzo di "sensori" o sonde che rilevano le attività in corso sui sistemi e identificano le anomalie, e da personale altamente specializzato in grado di interpretare i segnali provenienti dai sistemi per riconoscere potenziali situazioni di rischio, indagarle e, nel caso, reagire per arrestare l'attacco. Questo modo, per così dire "tradizionale" di procedere, sta però entrando in crisi a causa dell'enorme aumento dei sistemi da proteggere, anche dovuto alla progressiva introduzione di sistemi IoT e della crescente sofisticazione dei mezzi a disposizione degli attaccanti, che hanno possono usare numerose tecniche per superare le barriere tradizionali fornite ad esempio dagli Antivirus. Per fronteggiarle sarebbe necessario aumentare il numero di addetti alla sicurezza, ma ciò non è evidentemente possibile al di sopra di una certa soglia, per problemi di costi da un lato, e di carenza di risorse adeguatamente preparate dall'altro.

In questo scenario, l'introduzione di sistemi basati sull'intelligenza artificiale per affiancare gli specialisti umani comporta evidenti benefici, legati alla capacità di trattare volumi di dati più elevati e alla maggiore velocità nell'esecuzione di attività di risposta all'attacco. Possiamo identificare tre aree in cui l'impiego di metodi basati su algoritmi di intelligenza artificiale possono aiutare a rinforzare la gestione della sicurezza informatica.
La prima area è costituita dai sistemi di rilevazione di situazioni anomale potenzialmente

[1] Esistono varie definizioni delle fasi di un attacco informatico (cyber kill chain). L'analisi qui riportata si basa liberamente su una delle più utilizzate, la Killer Cyber Chain© proposta dalla Lockheed Martin, della quale costituisce una semplificazione. Si veda www.lockheedmartin.com per maggiori informazioni.

pericolose. La sicurezza informatica è un settore nel quale la mole di dati generati è elevatissima, e contiene informazioni su chi o che cosa si collega ai sistemi da proteggere, gli accessi ai dati, informazioni sulle connessioni verso siti esterni, cambiamenti apportati ai sistemi, informazioni o segnalazioni generate dagli stessi sistemi di sicurezza. Insomma, una mole vastissima di dati eterogenei, che vanno interpretati e confrontati tra loro per individuare quelle situazioni "anomale" che possono indicare un potenziale attacco in corso, ovvero esattamente il tipo di situazioni nelle quali gli algoritmi di intelligenza artificiale si mostrano più efficaci. Applicazioni in tal senso hanno già lasciato l'ambito della sperimentazione e sono disponibili sul mercato. Il loro compito è identificare quegli eventi, o insiemi di eventi, che collettivamente possono identificare una deviazione sospetta rispetto ai comportamenti "medi" riscontrabili all'interno dell'organizzazione che si vuole proteggere. In questo ambito, la capacità di "apprendere" mostrata dai sistemi di intelligenza artificiale, quali ad esempio le reti neurali, è particolarmente importante. Un sistema di questo tipo può infatti discriminare fra la normale operatività dei sistemi informatici e il manifestarsi di comportamenti anomali.

Sistemi di questo tipo possono essere usati per collaborare con esperti umani, arrivando ad individuare l'85% degli attacchi e a ridurre fino a ad un quinto il numero di falsi positivi, ovvero le segnalazioni di attacco che poi, ad una analisi più approfondita, si rivelano innocue[2]. Con il loro impiego è quindi possibile aiutare gli esperti umani a tenere sotto controllo un numero di sistemi molto più elevato di quanto sarebbe possibile ricorrendo solo a tecniche tradizionali. Inoltre, tali sistemi possono essere continuamente aggiornati per identificare correttamente anche le nuove tipologie di attacco che via via si manifestano.
Una seconda area è quella del supporto decisionale per mezzo dei sistemi esperti, ovvero dei sistemi composti da una base informativa e da un motore inferenziale, usato per elaborare risposte adatte alle situazioni che vengono presentate, sulla base delle informazioni già note. Sistemi di questo genere, peraltro già ampiamente utilizzati anche in altri ambiti, ad esempio negli help desk telefonici per aiutare gli operatori a fornire risposte ai problemi degli utenti, sono impiegati con successo anche nell'ambito della sicurezza informatica. Grazie a loro, è possibile velocizzare e standardizzare l'analisi di determinati eventi, per stabilire se si tratti o meno di incidenti di sicurezza, e mettere in atto delle procedure uniformi di risposta. In questo modo le organizzazioni possono più facilmente disseminare le informazioni, elevare uniformemente le capacità dello staff di esperti di sicurezza e rendere più rapide le attività di rilevazione e risposta agli incidenti.

[2] "AI2: Training a big data machine to defend", Veeramachaneni, Arnaldo, Alfredo Cuesta-Infante, Vamsi Korrapati, Costas Bassias, Ke Li. Articolo reperibile in: http://people.csail.mit.edu/kalyan/AI2_Paper.pdf. Il sistema è composto di quattro elementi: Una piattaforma di analisi comportamentale, un "motore" in grado di identificare scostamenti dalla normalità, un meccanismo per ricevere feedback dagli analisti di sicurezza e infine un sistema di apprendimento supervisionato.

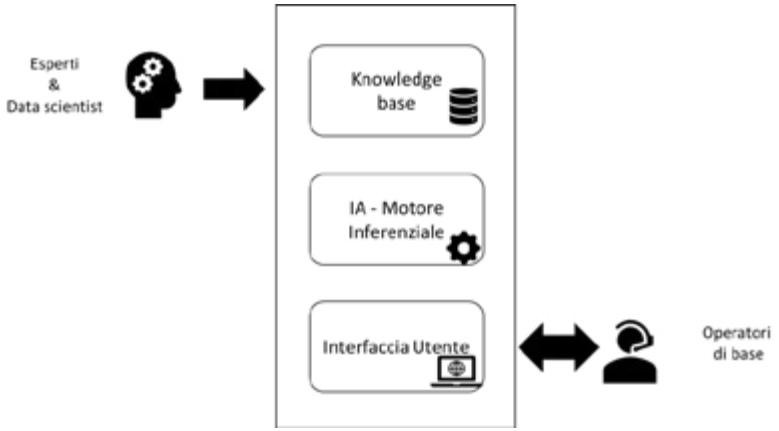


Figura 2 - *Il ruolo dell'AI nel potenziamento dei processi decisionali*

Un'ultima area di ricerca, a cavallo fra gli ambiti civili e militari, è quella dei cosiddetti agenti intelligenti. Gli agenti intelligenti sono componenti software che possiedono alcune caratteristiche di comportamento intelligente: proattività, la comprensione di un linguaggio di comunicazione fra agenti (Agent Communication Language - ACL), reattività (capacità di prendere alcune decisioni e di agire autonomamente).
Essi possono avere capacità di pianificazione, di riflessione e mobilità. Nel caso della sicurezza informatica, gli agenti intelligenti sono costituiti da sistemi software, autonomi o inseriti all'interno di piattaforme più tradizionali (firewall, sistemi antintrusione, router ecc.), che hanno diverse capacità: monitoraggio dell'attività in corso sui sistemi informatici, analisi, rilevazione di situazioni di attacco, risposta. I sistemi sono distribuiti sulla rete che si desidera proteggere e possono comunicare tra loro per mettere in relazione le informazioni raccolte separatamente e mettere in atto una strategia di difesa, con minima o nulla supervisione da parte di specialisti umani. Questi sistemi hanno un doppio interesse, civile[3] e militare[4], dove nel secondo caso si valuta anche la possibilità di dotarli della capacità di contrattaccare.

[3] G. Preetha, B. S. Kiruthika Devi, and S. Mercy Shalinie: "Autonomous Agent for DDoS Attack Detection and Defense in an Experimental Testbed". International Journal of Fuzzy Systems, Vol. 16, No. 4, December 2014

[4] A. Guarino: "Autonomous Intelligent Agents in Cyber Offence". 2013 5th International Conference on Cyber Conflict

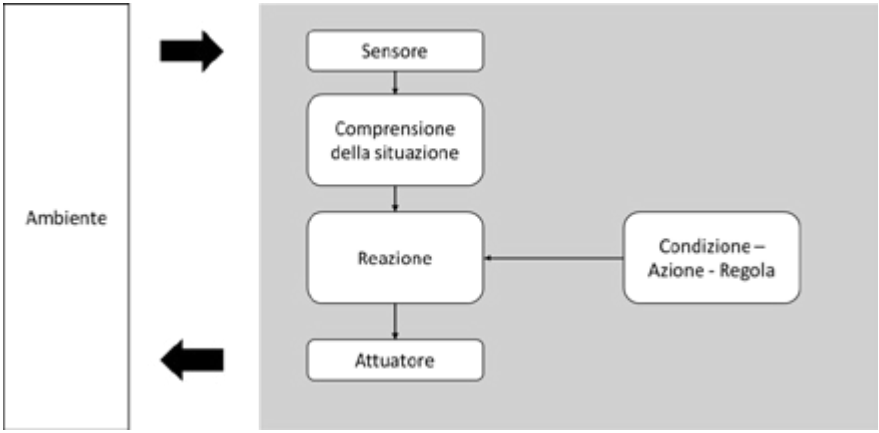


Figura 3 - *Rappresentazione schematica di un agente intelligente*

Nel mondo dei prodotti e dei servizi sicurezza è già oggi onnipresente la dichiarazione "powered by AI techniques". Dall'antivirus al firewall, dal sistema di accesso ai servizi SOC, l'utilizzo di sistemi di intelligenza artificiale per aumentare la capacità dei sistemi di identificare attività malevole e potenzialmente fraudolente è il nuovo trend.
L'adozione di queste tecniche, un fatto positivo in se, non deve però indurre ad abbassare la guardia: le stesse tecniche di intelligenza artificiale messe a guardia dei nostri sistemi, non sono immuni dall'essere vulnerabili loro stesse[5]. Molte di queste tecniche, infatti, utilizzano la tecnologia di apprendimento supervisionato (supervised learing) per apprendere a distinguere situazioni normali da situazioni anomale, e questo apre il tema dell'affidabilità originaria dei dati, o della loro sicurezza. L'utilizzo per l'apprendimento di basi di dati di bassa qualità o, peggio, corrotte, può comportare un funzionamento errato degli algoritmi di AI, che saranno quindi incapaci di riconoscere determinati tipi di attacchi.
Diversi studi poi mostrano che i sistemi di riconoscimento di questo tipo possono essere aggirati utilizzando tecniche di adversarial machine learning, nelle quali un'Intelligenza Artificiale viene usata proprio per costruire "casi" che porteranno ad un falso negativo, permettendo così di camuffare, ad esempio, file malevoli in modo che l'algoritmo che dovrebbe riconoscerli non sia in grado di farlo. Infine l'approccio "black box" di sistemi quali, ad esempio, le reti neurali profonde (deep neural network) potrebbe costituire un ostacolo nell'interpretazione dei risultati forniti da un sistema "powered by AI".

In questo momento l'intelligenza artificiale costituisce senz'altro un importante e, direi, necessario strumento per coadiuvare i responsabili della sicurezza nel compito di fronteggiare il numero sempre crescente di attacchi, ma non va considerato come uno strumento risolu-

[5] M. Giles: "AI for cybersecurity is a hot new thing—and a dangerous gamble", 22 agosto 2018, MIT Technology Review.

tivo e autonomo, ma semplicemente come un altro strumento nell'arsenale di chi difende, che richiede anche lui una supervisione ed una verifica dei risultati che ottiene.

L'intelligenza Artificiale come strumento di attacco cyber

Accanto al tema dell'utilizzo dell'intelligenza artificiale come strumento per accrescere le capacità di difesa informatica, è necessario considerare il "dark side" dell'intelligenza artificiale, ovvero il possibile utilizzo di queste tecnologie per affinare i metodi e l'estensione degli attacchi informatici. Nei due decenni scorsi abbiamo assistito ad un importante cambiamento di paradigma nel rapporto tra dato ed algoritmo: il crescente utilizzo di algoritmi di intelligenza artificiale, reti neurali, deep learning eccetera, ha spostato il vantaggio competitivo per le aziende dalla conoscenza (e segretezza) dell'algoritmo alla disponibilità dei dati, prerequisito fondamentale questi ultimi per addestrare i sistemi neurali e metterli in grado di eseguire attività in qualche modo monetizzabili, quali riconoscere immagini, decodificare il parlato, fare ricerche testuali. Per questa ragione già da alcuni anni, numerosi framework di programmazione per lo sviluppo di sistemi basati su tecniche dell'Intelligenza Artificiale sono stati resi gratuitamente disponibili: TensorFlow di Google, Microsoft CNTK o Caffe, per citarne solo alcuni, rendono relativamente semplice lo sviluppo di applicazioni basate su tecniche di machine learning o deep learning, democratizzandone l'impiego. Data la continua escalation fra attacco e difesa cyber, è ragionevole ritenere che queste tecniche possano venire utilizzate dai "bad actors" per potenziare i propri attacchi, con tre prevedibili effetti sulle minacce di tipo informatico: l'espansione delle minacce esistenti, l'introduzione di nuovi tipi di minaccia ed infine un cambiamento o evoluzione delle minacce stesse[6].

Espansione delle minacce esistenti. I costi degli attacchi potrebbero ridursi grazie alla scalabilità offerta dai sistemi di intelligenza artificiale, utilizzata per completare le attività che altrimenti richiederebbero l'impiego di persone. Un possibile effetto sarebbe quello di accrescere il numero di attori che possono effettuare attacchi, la velocità con cui questi attacchi possono essere eseguiti e l'insieme dei potenziali obiettivi.

Introduzione di nuove minacce. Nuovi tipi di attacco potrebbero essere lanciati con l'aiuto di sistemi di intelligenza artificiale per eseguire attività che sarebbero altrimenti poco pratiche o troppo dispendiose per l'uomo. L'IA permetterà inoltre di aumentare l'efficacia di attacchi che sfruttino le vulnerabilità umane, ad esempio attraverso l'uso di sistemi in grado di riprodurre la voce o l'immagine delle persone (si pensi ai deep fake). Infine, gli attori malevoli potrebbero sfruttare le vulnerabilità dei sistemi di intelligenza artificiale schierati dai difensori, come mostriamo in un successivo articolo.

Evoluzione delle minacce esistenti. È lecito attendersi che l'uso di sistemi di intelligenza artificiale possa rendere le minacce già esistenti più efficaci, più mirate e più difficili da

[6] Cfr. The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation, AA.VV. Feb. 2018

attribuire. L'uso dell'IA per automatizzare le attività necessarie alla realizzazione di attacchi informatici cambierà il compromesso esistente fra la scala e l'efficacia degli attacchi. In questo modo potrebbe estendersi la minaccia associata agli attacchi informatici che richiedono uno studio intenso dell'obiettivo, come è il caso dello spear phishing. In pratica il rischio è che sia possibile, per un attaccante, realizzare campagne di phishing su larga scala costituito da e-mail in qualche modo. personalizzate.

Figura 4 - *Direttrici di attacco potenziabili con l'intelligenza artificiale*

La presenza di fenomeni quali il Malware as a Service (MaaS), dove un team di esperti "produce" malware, sviluppa exploits e si occupa della loro ricerca e sviluppo, mentre una catena di distributori si occupa di procacciare i clienti, rende questi scenari ancora più attuali. Questo modello, che somiglia più ad una normale azienda di tecnologia che al bricolage che ha caratterizzato i primi anni del cybercrime, con la possibilità di accentrare le capacità tecniche rende più facile l'assorbimento di tecnologie innovative come l'IA per lo sviluppo o il potenziamento dei metodi di attacco.
Con riferimento alle fasi tipiche di un attacco informatico citate nel capitolo precedente[7], vediamo dove è possibile prevedere che gli hacker possano mettere a frutto le tecniche dell'Intelligenza artificiale, ed in che modo.

[7] Esistono varie definizioni delle fasi di un attacco informatico (cyber kill chain). L'analisi qui riportata si basa liberamente su una delle più utilizzate, la Killer Cyber Chain© proposta dalla Lockheed Martin, della quale costituisce una semplificazione.
Si veda www.lockheedmartin.com per maggiori informazioni.

Fase di ricognizione: Uno dei vantaggi offerti dall'Intelligenza Artificiale è il rapido riconoscimento di pattern. Questa capacità può essere impiegata nella fase di ricognizione, per automatizzare la scansione di vulnerabilità, introducendo maggiore flessibilità rispetto alla semplice ripetizione di una chek list. L'IA può inoltre aiutare a selezionare il malware più idoneo a penetrare un particolare sistema, applicazione, infrastruttura o ambiente. L'IA può infine facilitare l'adattamento di un exploit al particolare ambiente-bersaglio più rapidamente di un essere umano, generando e testando velocemente numerose varianti dello stesso. Alcuni autori, inoltre, mettono in guardia dalla possibilità che i malware del futuro possano essere dotati di sistemi di riconoscimento automatico che potranno attivare automaticamente un certo attacco in presenza di caratteristiche specifiche: una certa configurazione del computer o della rete, una posizione geografica o il riconoscimento di specifici pattern vocali[8]. Non si tratta di mere speculazioni, come ha dimostrato una ricerca presentata alla conferenza Black Hat USA nel 2018 dove è stata dimostrata la fattibilità di un attacco che sfruttava tecniche di riconoscimento del volto per scaricare un malware, nascosto all'interno di un programma di videoconferenza, solo sulla macchina di una specifica persona.

La **fase di realizzazione** dell'attacco, ovvero il download del mailware per infettare una prima macchina, è spesso effettuata mediante e-mail che invitano l'utente a scaricare un file, a clickare su un link o a rivelare dati riservati, come ad esempio la propria password. Gli attacchi di phishing per riuscire richiedono una buona conoscenza del bersaglio ottenibile attraverso una preparazione meticolosa: gli hacker possono trascorrere mesi a studiare i loro obiettivi e a raccogliere informazioni.
L'Intelligenza Artificiale può ridurre considerevolmente questi tempi, automatizzando gran parte del processo, raccogliendo informazioni dai social media e da fonti online, individuando le correlazioni pertinenti che aiuteranno gli attaccanti a migliorare l'inganno. In questo scenario le tecniche di Intelligenza Artificiale che si occupano dell'elaborazione del linguaggio naturale possono venire sfruttate dagli hacker per analizzare rapidamente grandi moli di dati non strutturati (articoli online, pagine web e social media post), estraendone informazioni utili, quali le abitudini e le preferenze del bersaglio di un attacco, che possono poi essere utilizzate per comporre mail di phishing estremamente dettagliate e su larga scala.
In aggiunta a questi scenari, vanno considerati anche gli utilizzi di sistemi di adversarial machine learning per sviluppare rapidamente messaggi di pishing in grado di superare i sistemi antiphishing.

Per esempio, è stata dimostrata la possibilità di utilizzare un sistema, basato su algoritmi di machine learning, in grado di generare URL di phishing capaci di superare i sistemi di sicurezza. Il sistema utilizza il database phishtank (www.phishtank.com), un database aperto che permette di verificare se una URL è legittima o meno come base per l'apprendimento. I ricercatori hanno creato un software per l'apprendimento automatico (DeepPhish), in

[8] Si veda l'articolo "How weaponized AI creates a new breed of cyber-attacks", pubblicato su TechRepublic ad Agosto 2018.

grado di creare URL per pagine Web che sembrano essere legittime pagine di accesso per i siti Web reali. In realtà queste URL possono ingannare gli strumenti di sicurezza, pur se nascondono pagine Web in grado di raccogliere le credenziali di accesso - nome utente password – di utenti ignari[9].
Fase di esecuzione: le capacità dell'Intelligenza Artificiale possono essere utilizzate anche nella fase di esecuzione, nella quale l'attaccante cerca di estendere la propria presenza sulla rete. All'inizio del 2017, la società di sicurezza informatica Darktrace sosteneva di avere individuato un attacco di nuovo tipo ai danni di una società Indiana. L'attacco utilizzava rudimentali tecniche di machine learning per osservare ed apprendere l'andamento del traffico di rete. Il software ha quindi imitato, nelle sue comunicazioni verso l'esterno i flussi di traffico appresi, probabilmente per meglio confonderli e rendere più difficile l'individuazione[10]. Questo tipo di analisi automatizzata può aiutare nella fase di espansione, permettendo ad esempio di mascherare le azioni utilizzate per attaccare altre macchine con il traffico che legittimamente si genera sulla rete, oppure per identificare rapidamente i bersagli più interessanti dal punto di vista dell'attaccante, ed infine per meglio nascondere il traffico di esfiltrazione dei dati all'interno di pattern di traffico legittimo.

Infine è necessario citare rapidamente un ulteriore tema, quello della falsificazione della voce o delle immagini di persone reali (i cosidetti "deepfake") che potrebbero essere utilizzati per rendere ancora più efficienti gli attacchi di social engineering, ad esempio chiamando un help desk o un collega con la voce stessa del proprio bersaglio, per convincere la persona all'altro lato del telefono a rivelare informazioni o eseguire un reset password.

9 "AI Creates Phishing URLs That Can Beat Auto-Detection", IT West blog https://www.itwest.co.uk/ai-creates-phishing-urls-can-beat-auto-detection/

10 "Era of AI-Powered Cyberattacks Has Started", The Wall Street Journal, Nov 2017

Conclusioni

Benché gli esempi effettivi di attacchi che utilizzano tecnologie IA siano per ora limitati principalmente ad attività di ricerca, più che attacchi veri e propri, è lecito attendersi una crescita del fenomeno. Questo comporterà necessariamente la necessità di evolvere i sistemi di sicurezza tradizionale e di adottare sistemi di difesa che, a loro volta, siano muniti di sistemi di intelligenza artificiale capaci di rispondere con la necessaria flessibilità e rapidità alle minacce di nuovo tipo.
Assisteremo quindi, nei prossimi anni, ad una rinnovata escalation fra attacco e difesa cyber, nel quale entrambe le parti utilizzeranno tecniche di intelligenza artificiale per, rispettivamente, superare le difese o identificare ed arrestare gli attacchi. Un settore di ricerca molto attivo in questo ambito è rappresentato dall'Adversarial Machine Learning, dove un sistema di IA è disegnato per produrre dei risultati che possano ingannare un secondo sistema di IA.[11]

Questa prospettiva impatterà probabilmente non solo sul disegno dell'infrastruttura tecnologica di difesa, che dovrà essere adeguata ai nuovi scenari di minaccia, ma anche sull'organizzazione della sicurezza e sulla formazione delle persone, che dovranno saper riconoscere modalità di attacco più sofisticate e "personalizzate". Per contrastare efficacemente questo particolare tipo di minaccia, sarà necessario estendere lo scambio di informazioni di sicurezza per segnalare tempestivamente l'apparire di, ad esempio, sofisticate tecniche di phishing "potenziato" grazie ad informazioni raccolte su questo o quel social network, o attacchi che includono messaggi vocali "di sintesi", per permettere alle organizzazioni di allertare tempestivamente i propri dipendenti o i propri clienti. In questo ambito i CERT (Computer Emergency Response Team), opportunamente potenziati, potrebbero giocare un ruolo molto importante.
L'espansione di questi fenomeni è probabilmente destinata ad esercitare un'ulteriore pressione sul già evidente skills shortage in ambito cybersecurity. Con tutta evidenza questo è un tema di cui non possono farsi carico, autonomamente, le singole organizzazioni, ma necessiterebbe di un intervento a livello nazionale o sovranazionale per reperire ed indirizzare le risorse economiche necessarie a preparare, sin d'ora, i futuri esperti di sicurezza ed IA che saranno senza dubbio necessari nei prossimi anni.

La sfida di costruire una cybersecurity di nuova generazione con potenzialità e finalità espanse correlate all'AI ed alla gestione del fenomeno dei Big Data, è già aperta.

[11] B. Biggio, F. Roli, "Wild Patterns: Ten Years After the Rise of Adversarial Machine Learning", 2018, Pattern recognition

Tutto ebbe inizio alle 18:05 del 3 Gennaio 2009.
È proprio in quel momento che Satoshi Nakamoto rilasciò su Sourceforge il Blocco Zero, meglio noto come **Genesys Block**. Un blocco che contiene 50 bitcoin non spendibili e un messaggio che, facendo riferimento al salvataggio delle banche voluto dal governo inglese, mette in discussione proprio il ruolo di intermediario del sistema bancario.

La blockchain nasce proprio con l'idea di sostituire la fiducia riposta in intermediari noti e blasonati quali banche e istituzioni con la fiducia in un algoritmo.
Nel corso di questi 10 anni abbiamo compreso come la Blockchain - andando ben oltre i bitcoin – possa essere utilizzata per creare strutture dati più resilienti, sicure e distribuite di quanto si potesse immaginare sino a ora.
Combinata all'utilizzo di *Smart Contract* e altre nuove tecnologie come l'Intelligenza Artificiale, la Blockchain sarà in grado nei prossimi anni di introdurre nuovi modelli di business e al contempo di trasformare radicalmente i modelli attualmente predominanti, come ad esempio i processi di Supply Chain.

Si tratta di un'innovazione paragonabile a Internet o persino all'introduzione dell'energia elettrica presso le nostre case. Sarà ovviamente necessario del tempo per chiarire questioni ancora aperte o definire le migliori strategie di diffusione, ma nessuno può escludere che nei prossimi 10 o 20 anni useremo la tecnologia Blockchain così come oggi utilizziamo l'energia elettrica, senza neanche rendercene conto e dando per scontato che sia sempre presente.
Gli asset crittografici diventano così una nuova modalità di rappresentazione del valore completamente sganciata dal concetto di fiducia e come tali inseriscono nuove e interessanti sfide per i professionisti della sicurezza informatica. In primis la corrispondenza biunivoca tra le chiavi crittografiche e gli asset per cui la perdita delle prime si traduce automaticamente in una perdita economica in genere non recuperabile.

Blockchain & Supply Chain: una catena del valore sicura, distribuita e trasparente

[A cura di Guido Sandonà e Federico Griscioli]

Una delle modalità più efficaci a disposizione delle aziende per affermare il proprio vantaggio competitivo è legata da un lato alla capacità innovativa e dall'altro alla capacità di creare relazioni strategiche e complementari con altre aziende. Sono entrambi aspetti peculiari di qualsiasi processo di supply chain management che abbia l'obiettivo di ottimizzare l'intera filiera produttiva, partendo dall'approvvigionamento della materia prima fino ad arrivare al cliente finale. Tra le numerose definizioni di Supply Chain riteniamo utile ricordare quella di Lamber e Cooper in base alla quale *"si tratta dell'integrazione di processi aziendali chiave dal cliente finale per arrivare ai fornitori, i quali generano valore aggiunto per il cliente stesso o per gli stakeholder interessati fornendo prodotti, servizi e informazioni"*. Si tratta di continue interazioni tra moltissimi operatori che a vario titolo intervengono lungo una catena che prevede innumerevoli fasi, nonché siti geografici tra i più disparati. Culture e legislazioni diverse non contribuiscono a rendere fluido e trasparente l'intero processo. Inoltre, i diversi attori della catena di distribuzione hanno interessi e priorità spesso contrastanti tra loro, che rendono difficile e oneroso instaurare meccanismi di fiducia. Non va dimenticato come tali interazioni comportino in ultima analisi il perfezionamento di numerosi contratti, lo scambio di documenti ed informazioni digitali e di pagamento.
Una catena di interazioni e passaggi così articolata, rende non semplice conoscere il reale valore dei prodotti. In modo simile, è estremamente difficile indagare sui processi di supply chain quando vi sia il sospetto di pratiche illegali o immorali. Tematiche del genere portano con sé problemi di trasparenza, e fiducia tra i vari attori, che quando degenerano si traducono in frodi, contraffazione nonché condizioni di lavoro eticamente discutibili. Nessuna azienda può permettersi di sottovalutare o peggio trascurare tali evenienze, poiché attenzione alla sostenibilità dell'ambiente, rispetto dei diritti umani e dei lavoratori, costituiscono fattori vitali per il sostentamento dell'organizzazione, soprattutto in quei casi in cui il business è fortemente sorretto dalla reputazione del brand.
Gli innumerevoli tentativi di eliminare alla radice tali rischi hanno vissuto fasi alterne – spesso in base ai settori merceologici nonché agli *hype* delle diverse tecnologie - senza tuttavia mai raggiungere l'obiettivo nella sua interezza. Di certo si può dire che i processi di supply chain nel frattempo si sono arricchiti – per utilizzare un eufemismo – di controlli, audit, sistemi informatici etc... aumentando costi e tempi.

Da più di 30 anni ormai supply chain e tecnologia sono strettamente collegati. La tecnologia ha reso le relazioni tra clienti e fornitori veloci e flessibili; ha decisamente migliorato efficienza ed integrazione nei rapporti tra le aziende senza tuttavia riuscire a risolvere completamente i problemi di fiducia, concentrazione e sicurezza dell'informazione che tuttora affliggono i processi di supply chain. La quarta rivoluzione industriale ha amplificato tale

interdipendenza grazie a tecnologie quali *Internet Of Things, Big Data* e non ultimo l'Intelligenza Artificiale. Ma è soltanto tramite l'utilizzo della tecnologia Blockchain che sarà possibile instaurare fiducia senza bisogno di intermediari, garantire sicurezza e univocità di documenti e pagamenti, nonché ridurre i problemi di concentrazione che spesso influenzano negativamente la catena del valore dei prodotti.

La Blockchain nata come strumento per realizzare un sistema decentralizzato e disintermediato di pagamento, ha dimostrato nel corso degli ultimi anni di poter svolgere numerose altre funzioni. Può essere utilizzata per gestire qualsiasi scambio, contratto, accordo, per tracciare ed ovviamente per pagare. Ogni volta che un prodotto viene movimentato la transazione può essere documentata, creando una storia permanente del prodotto stesso, dalla produzione alla vendita. Ciò potrebbe ridurre drasticamente i ritardi di tempo, i costi aggiuntivi e l'errore umano che oggi affliggono i processi di supply chain. In **Figura 1** l'*hype* della Blockchain nel tempo.

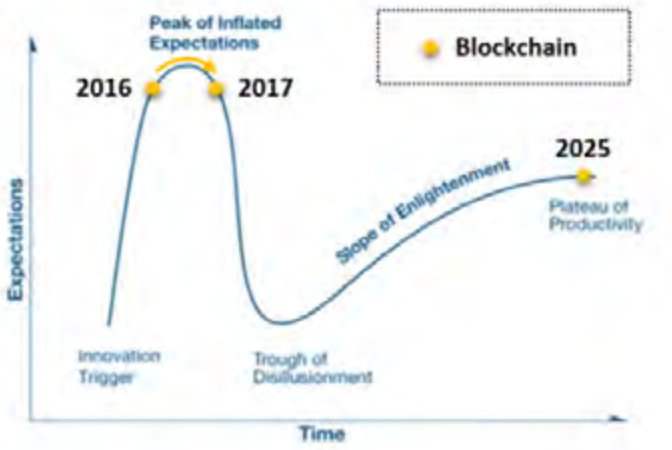


Figura 1 - *Hype del ciclo della Blockchain - Gartner (rielaborato QuanTek)*

La Blockchain combina in maniera articolata e logica al tempo stesso tecniche da tempo in uso nel campo dell'Information Technology. Si tratta di un'infrastruttura condivisa basata su complessi ed affidabili algoritmi di crittografia che rientra nella più ampia categoria dei database distribuiti. La presenza di un meccanismo di consenso (*Consensus Mechanism*) elimina la necessità di soggetti intermediari ma garantisce nello stesso tempo affidabilità e consistenza dei dati e dell'intera infrastruttura. Il database o registro è organizzato in blocchi legati sequenzialmente tra di loro. I blocchi, a loro volta, sono un insieme di transazioni le quali contengono i dati. Il blocco rappresenta la singola unità della struttura ed è formato da un insieme di transazioni. I blocchi vengono inseriti all'interno della struttura in accordo

al *Consensus Mechanism* e, una volta inseriti, non possono più essere eliminati (proprietà dell'immutabilità). Il fatto che i blocchi siano legati sequenzialmente tra di loro per mezzo di una hash crittografica (per semplicità chiamata nel seguito hash) garantisce l'integrità del dato. L'hash è un algoritmo matematico che riceve in ingresso una stringa di qualsiasi lunghezza e fornisce in uscita una stringa di lunghezza fissa. È un processo unidirezionale, nel senso che, avendo a disposizione la stringa in uscita, non è possibile ricostruire la stringa in entrata. La natura distribuita è data dal fatto che, potenzialmente, tutti i partecipanti alla Blockchain possono avere un esemplare del database o registro. Questo tipo di partecipanti prende il nome di *full-node*. In relazione a ciò, la Blockchain diventa robusta agli attacchi di tipo *Denial of Service*1 in maniera esponenziale rispetto al numero di *full-node*. Il numero di partecipanti impatta anche sull'affidabilità di tutta la struttura. Più precisamente, a seguito del meccanismo di consenso, l'affidabilità della Blockchain cresce esponenzialmente con i partecipanti che, potenzialmente, possono contribuire a validare un blocco.
Ogni partecipante che opera sulla Blockchain è identificato da una chiave privata e una chiave pubblica (crittografia asimmetrica). Mentre la chiave pubblica è conosciuta da tutti, la chiave privata è il "segreto" viene utilizzata per provare la propria identità. L'utilizzo della criptografia asimmetrica garantisce il rispetto del principio di *non-ripudio*, secondo il quale, una volta che un certo soggetto ha svolto una certa azione (per esempio una transazione), non è possibile negarne la paternità.
Grazie al meccanismo di consenso e agli algoritmi di crittografia utilizzati, la Blockchain affronta il tema della *Digital Scarcity,* ovvero la capacità di rendere non riproducibili informazioni digitali come file o pagamenti. Ciò avviene tramite l'adozione dei cosiddetti *Security Tokens* ai quali legare files, scambi dati ed ovviamente pagamenti (alla stregua di quanto oggi avviene nella rete Bitcoin)

Esistono varie tipologie di blockchain distinte in base alla modalità di riconoscimento dei partecipanti, al meccanismo di accesso, ma soprattutto in base al meccanismo di consenso adottato. Tuttavia, ognuna di esse ricade in una di queste tre grandi tipologie:

- **Pubblica:** ogni partecipante o nodo può accedere alla blockchain e validare le transazioni, per cui il meccanismo di consenso è aperto a tutti. È necessario semplicemente un wallet che abiliti il soggetto a ricevere, inviare o memorizzare asset digitali. Si tratta del modello su cui si basa la Blockchain Bitcoin
- **Privata:** solo i soggetti abilitati che tra loro si conoscono ed hanno un rapporto fiduciario già in essere possono leggere e validare le transazioni e le autorizzazioni di scrittura e lettura vengono gestite da uno o più soggetti determinati. Si tratta di una blockchain non accessibile pubblicamente.
- **Ibrida:** è la combinazione tra pubblica e privata. Il meccanismo di consenso è controllato da una serie di nodi preselezionati i quali decidono quali transazioni possono essere incluse nei blocchi, nonché i diversi livelli autorizzativi all'interno della blockchain.

L'adozione della tecnologia Blockchain è in grado di generare trasparenza e assicurare l'adempimento ad esempio dei contratti di trasporto, grazie all'utilizzo degli *Smart Contract*.

Proprio gli Smart Contract – ovvero contratti intelligenti capaci di eseguire automaticamente delle transazioni – insieme alla natura immutabile della Blockchain potrebbero introdurre alcuni automatismi ma soprattutto incentivi per aumentare integrità e sicurezza della supply chain anche nel caso in cui non vi sia un rapporto fiduciario o di conoscenza tra due o più contraenti. Si pensi al caso di uno Smart Contract che leghi pagamento e consegna della merce. In questo caso si potrebbero ridurre tempi e costi collegati al contratto e soprattutto si potrebbero ridurre i contenziosi poiché essendoci maggiore certezza sulle condizioni, l'interpretabilità di un contratto digitale è ridotta. Allo stesso modo la gestione dei documenti accompagnatori del prodotto potrebbe avvenire in maniera più distribuita e con il minimo rischio di smarrimento e falsificazione.

Rendendo certo e non ripudiabile il monitoraggio, il tracciamento dei prodotti e la tracciabilità dei trasporti, la blockchain potrebbe rendere più efficace ed efficiente il processo di certificazione riducendo costi e tempi, e aumentando l'affidabilità del dato (Baker, 2015). I processi di audit e di controllo qualità beneficerebbero in maniera significativa della natura immutabile e basata su crittografia della Blockchain (Dickson, 2016). Il suo utilizzo può anche semplificare la (Dickson, 2016) gestione dei resi, per reperire le informazioni collegate al prodotto reso, in modo da essere certi ad esempio che non tratti di un falso ma anche per identificare più facilmente in quale momento del processo produttivo si è originato il problema che può aver generato l'azione di reso.
La tecnologia Blockchain se implementata senza distorcere i suoi principi fondanti descritti da Satoshi Nakamoto nel paper *"Bitcoin: A Peer-to-Peer Electronic Cash System"* quali immutabilità, trasparenza ed infrastruttura distribuita, è in grado di aggiungere valore al processo di Supply Chain cosi come lo conosciamo oggi, rendendo l'intero processo più semplice, efficiente ma in assoluto più trasparente e sicuro. Non è un caso che come mostrato nel grafico di **Figura 2,** nei prossimi anni sia prevista un'adozione crescente di tecnologie Blockchain all'interno della supply chain.

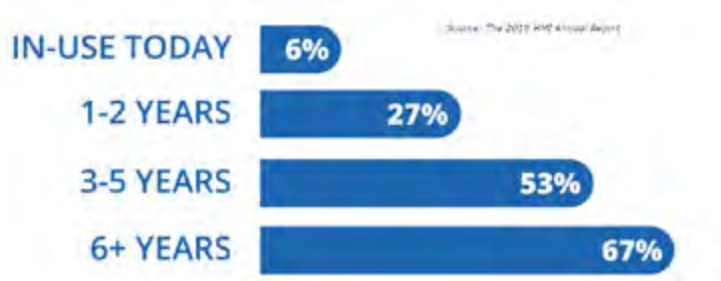


Figura 2 - *Trend nell'adozione della Blockchain all'interno della supply chain a partire dal 2018*

Dal Fisico al Digitale

Nel prossimo futuro la tecnologia Blockchain ci offrirà la possibilità di contrastare in maniera definitiva anche il fenomeno della contraffazione.
Ad oggi una delle modalità per combattere i fenomeni di contraffazione consiste nel combinare la serializzazione dei prodotti ai cosiddetti processi di *"track & trace"* - basati su tecnologia bar code o RFID – in modo monitorare e verificare i prodotti lungo le diverse fase della supply chain. Purtroppo, tali sistemi si accompagnano a difficoltà di integrazione tra diverse aziende e soprattutto presentano debolezze intrinseche che non impediscono fenomeni di frodi di contraffazione. Le etichette con tag RFID potrebbero essere clonate mentre per le etichette con bar code è sufficiente una foto con qualsiasi smartphone. Parlando proprio di smartphone, un recente rapporto dell'OECD ci ricorda che un telefono su cinque è falso.
Affinché la tecnologia Blockchain possa dare un contributo determinante a contrastare tale fenomeno è necessario associare univocamente l'oggetto fisico al suo alter ego digitale. Tutto ciò potrebbe essere possibile integrando Blockchain con tecnologie innovative quali Intelligenza Artificiale e IoT in grado di combinare oggetti fisici e sicurezza digitale.
Nel mese di gennaio di quest'anno (Group, s.d.) – un'importante multinazionale del settore farmaceutico – ha brevettato una nuova procedura di sicurezza che collega l'intelligenza artificiale (AI) e la tecnologia blockchain, tramite la creazione di *crypto objects*. Questa nuova procedura utilizza le tecnologie di Machine Learning per collegare oggetti fisici a una Blockchain tramite i propri identificatori univoci. Qualsiasi caratteristica unica può essere utilizzata come impronta digitale, ad esempio una firma chimica, DNA o immagini del prodotto.
L'applicazione di tale metodologia sarà in grado di costituire un vantaggio competitivo tangibile per tutti quei settori industriali che hanno nell'autenticità ed affidabilità del prodotto un elemento fondante del proprio business, partendo dal settore farmaceutico - dove nasce il brevetto appunto – al settore alimentare, senza però dimenticare ad esempio il settore manufatturiero. Saremo sempre in grado di rispondere alla domanda cosa viene consegnato, quando e come.

Implementare una Blockchain sicura

Nell'implementazione di una tecnologia blockchain è opportuno porre particolare attenzione ad alcuni aspetti che potrebbero impattare sul processo di supply chain stesso, o addirittura far venire meno l'esigenza di utilizzare una rete Blockchain.
La governance è il primo elemento da valutare con estrema attenzione ogni qualvolta un'azienda si appresta ad implementare o aderire ad una rete Blockchain. Informazioni distribuite e mancanza di un intermediario, non implicano mancanza di regole del gioco. Governance in sostanza vuol dire stabilire il meccanismo di validazione delle informazioni (ovvero il consenso), nonché le regole di accesso alle informazioni stesse. È più verosimile – ed oltretutto in linea con quanto osservato negli ultimi 2 anni – che le Blockchain Ibride siano le più adatte ad ospitare i processi di supply chain.
Ad esempio, grandi società di logistica come MAERSK, DHL, UPC hanno molti partner,

subappaltatori e clienti. Ciò crea una rete aziendale ma anche extra-aziendale complessa e spesso mutevole che costringe le aziende a mettere in atto strategie per affrontare e beneficiare di tale complessità. Fiducia, sicurezza e integrazione, sono i concetti cardine su cui costruire tale strategia. In questo caso la parte privata di una soluzione di blockchain ibrida può essere utilizzata per le transazioni tra i maggiori partner; avrà una classica configurazione basata sul principio del *Need to Know,* in cui i partecipanti possono visualizzare, effettuare transazioni e apportare modifiche in base ai permessi a loro assegnati. Questa parte di rete è veloce, scalabile e ragionevolmente sicura. Tuttavia, aggiungere altri partecipanti tramite un processo di *vetting*2 che ne certifichi l'identità è sicuramente più dispendioso rispetto a una blockchain pubblica. La parte pubblica di una soluzione blockchain ibrida conterrà quindi un ampio elenco di subappaltatori e piccoli partner (ad esempio i fornitori di servizi di trasporto locali) che saranno in grado di apportare modifiche a una rete pubblica, con un processo più semplice di costituzione della fiducia.

Quanto sopra ci fa capire come nel caso di Blockchain ibride sia di fondamentale importanza prestare attenzione al concetto di interoperabilità in modo che la comunicazione tra diverse blockchain e quindi tra diversi gruppi di aziende o consorzi sia sempre garantito.

Altrettanta attenzione va posta alla standardizzazione di dati e informazioni veicolate dalla Blockchain. È necessario un'attività di riconciliazione per far comunicare tra loro i sistemi informatici già in uso presso i diversi partecipanti.

Proprio l'integrazione di tutti questi sistemi legacy rappresenta la sfida che dovrà essere vinta affinché la Blockchain possa essere davvero integrata su larga scala nella gestione dei processi di supply chain. Si tratta di sistemi tra i più svariati, spesso sviluppati *"in casa",* non paragonabili tra loro nemmeno nelle logiche di programmazione. La sicurezza informatica per tal sistemi non è mai stato un punto di partenza né tanto meno un obiettivo. Alcuni di essi sono talmente datati che aggiornarli equivarrebbe a ripensarli da capo. È plausibile pensare che una vulnerabilità su uno di tali sistemi potrebbe avere impatti sulla Blockchain cui sono collegati abilitando azioni indesiderate, oppure rendendo più complesso il meccanismo di consenso, o infine ponendo dubbi sull'origine stessa dei dati. Se inoltre consideriamo il carattere immutabile della Blockchain, ci si rende conto di come la progettazione con cura della nuova tecnologia con processi e sistemi già esistenti, diventa nel nostro caso il punto da cui partire.

È buona prassi eseguire una validazione del codice in modo da eliminare possibili falle di sicurezza che possono essere sfruttate da un attaccante. Nel contesto Blockchain, definire un processo di *patch management* può risultare complicato. Nel caso peggiore, ci si potrebbe trovare nel caso di un *hard fork*3, causata dalla non compatibilità del vecchio codice con il nuovo. Nel caso degli smart contract la situazione è ancora più delicata. Generalmente una volta che un contratto è stato pubblicato non è più possibile invertire questo processo. Questo diventa particolarmente rilevante se si considera uno smart contract a tutti gli effetti un contratto legale che vincola le parti che "lo sottoscrivono". In questo caso, l'ideale sarebbe definire un processo di *assessment* del codice sia relativo alla sicurezza – se contiene falle di sicurezza – che relativo alla sua funzionalità – se cioè realizza il comportamento voluto.

Non bisogna inoltre sottovalutare la sicurezza dei *client* 4. In questo caso l'approccio processi di *security assessment* che *patch management* sono piuttosto facili da implementare visto che è possibile usare lo stesso approccio solitamente adottato per codice tradizionale. Il processo di identificazione dei partecipanti – il cosiddetto *vetting* - è l'ultimo aspetto da considerare per implementare un'infrastruttura Blockchain in maniera sicura. Di fatto si tratta del punto di ingresso al nostro database distribuito e per tale motivo va sempre presidiato con attenzione. Allo stesso modo va presidiata la modalità con la quale i partecipanti hanno cura della propria identità, ovvero della propria chiave privata. È indubbio che la perdita o il furto dell'identità digitale che rappresenta il partecipante all'interno dell'infrastruttura, può equivalere per lo meno a un disservizio e un'inefficienza più o meno grave nella catena del valore.
Nulla di tutto ciò può essere lasciato al caso, poiché in ultima analisi rischio è quello di vanificare le caratteristiche di sicurezza connaturate nella Blockchain.

Conclusioni

Attorno ai principi di Confidenzialità, Integrità, Disponibilità e Tracciabilità si costruisce la sicurezza di qualsiasi sistema informatico. Sono gli stessi quattro principi che nei prossimi anni faranno diventare la Blockchain un *Game Changer* per il mondo della supply chain. Come sostiene Paul Brody *"al suo livello più elementare, la logica fondamentale della blockchain significa che nessun pezzo di inventario può esistere nello stesso posto due volte";* basterebbe questo per convincerci che la supply chain sarà uno dei più interessanti ambiti di utilizzo per la Blockchain – con le sue intrinseche caratteristiche di sicurezza - nei prossimi anni. Se davvero ciò accadrà, a beneficiarne sarà l'intero sistema in termini di concorrenza, efficienza e sicurezza delle informazioni. Dovremo tutti essere vigili per non iniettare nel nuovo modello le vulnerabilità dei precedenti sistemi e ancora di più per non tradire lo spirito del Blocco Zero e della tecnologia che Satoshi ci ha lasciato in eredità senza nulla chiedere in cambio.

Bibliografia

- Baker, J. a. (2015). *Blockchain: the solution for transparency in*. Retrieved from https://www.provenance.org/whitepaper
- Dickson, B. (2016). Blockchain has the potential to revolutionize the supply chain. *Aol Tech*.
- Group, M. (n.d.). Retrieved from https://www.merckgroup.com/en/news/us-patent-blockchain-30-01-2019.html
- Fulvio SARZANA di S. IPPOLITO, Massimiliano Nicotra. Diritto della Blockchai, Intelligenza Artificiale
- Nadia Di Paola. *Blockchain e Supply Management*
- Paul Brody. *How Blockchain is revolutioning supply chain management*

Aspetti di sicurezza legali e tecnici sugli smart contract

[A cura di Alessio L.R. Pennasilico e Piero Bologna]

Caratteristiche e vantaggi

Chi si occupa di blockchain e temi ad esso collegati si è certamente imbattuto in una delle (oramai) tante definizioni di smart contract: a seconda dei casi o degli studi compiuti avrà letto definizioni tipo "*contractual type arrangement embedded in software*", oppure altre come "*protocollo informatico in grado di eseguire determinati termini contrattuali*", in altre ancora "*una forma avanzata della funzione "if-then" scritta in un linguaggio informatico*".

Le definizioni sono molte e, partendo da quella elaborata dal celebre Nick Szabo ancora negli anni '90, notiamo che uno smart contract può essere: "*[…] a set of promises, specified in digital form, including protocols within which the parties perform on these promises.*"

Il concetto di smart contract come sopra descritto è risalente nel tempo ed è infatti conosciuto in ambito informatico da (oramai) decenni.

Potremmo, in modo molto sintetico, vedere in uno smart contract una sorta di "*ibrido*" tra codice e contratto, tra informatica e diritto. Una realizzata possibilità di coniugare la certezza e automaticità di una condizione preimpostata a livello informatico (*if-then*) con un effetto giuridico che si sostanzia tra due parti contrattuali.

Quando uno smart contract viene inserito all'interno di una blockchain, a questo particolare "*meccanismo*" viene aggiunta la caratteristica dell'**immutabilità** e della sua "**distribuzione**" quasi simultanea in questo registro distribuito.

Tale inserimento permette di ottenere notevoli vantaggi i quali sono legati all'esecuzione pressoché automatica dei termini contrattuali inseriti nello smart contract e la possibilità di avere un "*record o prova*" di una transazione o di un particolare "fatto" che rimane registrato in modo immutabile (o quantomeno la cui falsificazione/ alterazione, per la struttura della blockchain e le regole sul consenso, rende di fatto totalmente anti-economico attuare cambiamenti ex post).

Va inoltre notato che inserire uno smart contract all'interno di una blockchain, esaurito l'effort iniziale (non banale) di trasposizione dei concetti giuridici e delle reciproche obbligazioni contrattuali in linguaggio informatico, poi potrebbe permettere uno snellimento delle procedure per la tenuta amministrativa e burocratica nonché un abbattimento dei costi di gestione del contratto stesso.

Non da ultimo, anzi, se vogliamo è di primaria importanza il fatto che una tale tecnologia permette di ottenere un ambiente in cui vige una fiducia nella tecnologia stessa senza il bisogno di avere intermediari o soggetti terzi fidati i quali garantiscono il regolare svolgimento (o il c.d. *enforcement*) delle obbligazioni contrattuali. Tale particolare impostazione permetterebbe a soggetti estranei e tra cui non è presente alcun tipo di fiducia reciproca, di

porre in essere delle transazioni; in questo caso, infatti, si parla di "*trust in computer code*".
Ma allora uno smart contract è effettivamente un contratto?
Ad oggi vi sono parecchi studi ed articoli specialistici che trattano il tema alla luce dei vari diritti nazionali che si scelgono come modello.
In ambito italiano, non paiono esservi regole che ostacolino la formazione di un contratto a livello digitale/ informatico ed è inoltre stato recentemente promulgato dal legislatore (legge n. 12/2019 che ha convertito il decreto legge n. 135/2018) un importante articolo che disciplina tali aspetti e conferisce, fra gli altri, il **requisito della forma scritta** agli smart contract qualora la parti interessate vengano previamente identificate (la procedura per l'identificazione verrà prossimamente emanata dall'AGID – l'Agenzia per l'Italia Digitale).

Problemi legati a bug o errori o difetti dello smart contract

Come risolvere eventuali problemi legati ad errori dello smart contract stesso?
È plausibile utilizzare categorie giuridiche preesistenti o comunque applicate in altri settori?
Le domande sopra riportate sono ancora dibattute e non si è ancora giunti ad una soluzione uniforme delle stesse.
Le soluzioni giuridiche applicate in ambito software potrebbero permettere delle way-out a tali problematiche: per verificare le stesse vanno però fatti dei distinguo nel caso in cui si operi con smart contract inseriti su una blockchain pubblica o su una privata.
Nel caso ci si trovi all'interno di una **blockchain privata** la soluzione che appare più semplice ed efficiente è quella di attribuire la responsabilità per eventuali bug o errori di vario tipo al provider della blockchain stessa.
Lo stesso provider però potrebbe argomentare (o difendersi) dicendo che gli errori nell'esecuzione di obbligazioni contrattuali è invece attribuibile solamente al programmatore dello smart contract (a cui lui non è collegato o unito).
In tal caso, se effettivamente tale "catena di responsabilità" venisse correttamente ricostruita a livello probatorio, pare sicuramente praticabile attribuire la responsabilità al programmatore dello smart contract.
Altra tematica di particolare complessità subentra per il fatto che lo smart contract inserito su una blockchain è di per sé immutabile e paiono al momento non praticabili dei meccanismi di eventuale sovrascrittura o annullamento dei blocchi.
Nel caso ci si trovasse in una **blockchain pubblica** invece i temi sopra evidenziati non sono di così "semplice" soluzione e al momento attuale, come e a chi attribuire la responsabilità per eventuali errori nello smart contract, non è ancora stata fornita una soluzione.
In questo specifico ambito potrà essere necessario l'intervento del legislatore, il quale potrà tenere in considerazione gli enormi vantaggi di questa tecnologia e quindi incentivare gli operatori del settore con norme certe.

Aspetti di sicurezza da prendere in considerazione

Lo smart contract è a tutti gli effetti un software, un programma, prono quindi a tutti gli errori tipici di questa categoria, nonché ad una serie di attacchi tecnologici da tenere in considerazione.
Esistono alcuni aspetti noti e scontati legati alla tipicità dell'infrastruttura su cui il contratto viene eseguito: prendere il possesso di oltre il 51% dei nodi, ad esempio, potrebbe permettere di manipolare il meccanismo di consenso. Tuttavia, volendo ignorare ile possibili vulnerabilità "infrastrutturali", restano diverse minacce specifiche da prendere in considerazione.

Al fine di assicurare la corretta qualità del codice è necessario adottare un processo di sviluppo solido e robusto, basandosi sulle best practice di mercato oggi disponibili, pur tenendo presente le peculiarità specifiche. Se sono certamente da adottare tutte le tecniche note di secure coding e di code review, non è detto che le linee guida disponibili oggi coprano tutte le necessità legate all'esecuzione del codice in un ambiente quale la blockchain.
Anche la creazione e la gestione di ambienti di sviluppo e test è ovviamente un argomento sul quale, per certo, sono ancora da definire delle linee guida consolidate.
Resta poi il tema degli update da gestire, non essendo sostituibile il codice precedentemente aggiornato.

Grande interesse, inoltre, suscita la possibilità di utilizzare fonti esterne alla blockchain adottata, gli oracoli, per alimentare lo smart contract e scatenarne o influenzarne l'esecuzione. Relativamente agli oracoli, potendo essere fonti informative di ogni genere, dalla API di un sito fino all'output di un oggetto IoT, si pongono diversi problemi. Uno riguarda per certo l'autorevolezza della fonte. Come si può essere certi di avere scelto la fonte corretta, la più adatta a fornire l'informazione voluta, nei tempi adatti? Come è possibile garantire eventuali manipolazioni della fonte?

Esempio: *se venisse utilizzato uno smart contract per stipulare una polizza assicurativa che liquida un danno "a forfait" in caso di grandine nel Cap di riferimento, come essere certi che nessuno abbia violato la sicurezza del sito da cui vengono attinte le informazioni sulle condizioni atmosferiche? La singola violazione di quel sito, ad esempio, per la compagnia di assicurazione significherebbe il liquidare erroneamente, e purtroppo automaticamente, magari migliaia di sinistri.*

Come è possibile essere certi che l'informazione autorevole scelta non venga manipolata durante la comunicazione? Si pensi al variarne il contenuto in transito ma anche al banale non far giungere l'informazione, evitando di far godere di un diritto ad un sottoscrittore del contratto.
Si tenga in considerazione, inoltre, che, essendo lo smart contract, uno strumento pensato per generare "fiducia tra sconosciuti", è estremamente probabile che una delle parti interessate possa essere fisicamente in possesso dell'oracolo (es. sensore IoT) e nella possibilità di

riprogrammarlo o manometterlo, al fine di ottenere un vantaggio personale.
Questa classe di problemi, legata al richiamo di informazioni esterne, è nota anche come reentrancy e sarà uno dei principali temi a cui fare attenzione nell'uso degli smart contract.
Anche il problema tempo, nella blockchain, è tutt'altro che trascurabile. Poiché la scrittura di un blocco non è immediata, è di fatto possibile conoscere quali azioni saranno eseguite prima che esse vengano formalizzate.
Restano, inoltre, validi tutti i temi legati all'overflow, ai DoS, e così via: minacce e vulnerabilità che da sempre possono affliggere programmi e servizi accessibili on-line.

Esempio: *nel caso di smart contract legati a pagamenti, aste, crowdfunding, ad esempio, potrebbe essere possibile influenzare il meccanismo di valutazione delle offerte o di rimborso; questo potrebbe condurre alla sottrazione di denaro al legittimo destinatario, ad esempio impedendo l'esecuzione di un rimborso*

Quelli elencati non sono solo plausibili scenari futuri, ma le cause di incidenti già avvenuti. In particolar modo si pensi, ad esempio, a quanto avvenuto agli utilizzatori di Parity, un ethereum wallet, di PoWHCoin o di DAO nei mesi passati, i cui dettagli sono disponibili in bibliografia.

A sottolineare la necessità della corretta gestione del codice sono anche la attuale disponibilità di diversi strumenti per la verifica ed il monitoraggio degli smart contract, molti dei quali elencati in bibliografia, o di programmi di bug bounty (riconoscimenti in denaro offerto dal produttore per chi riesce a scovare un bug nel proprio programma).

Bibliografia

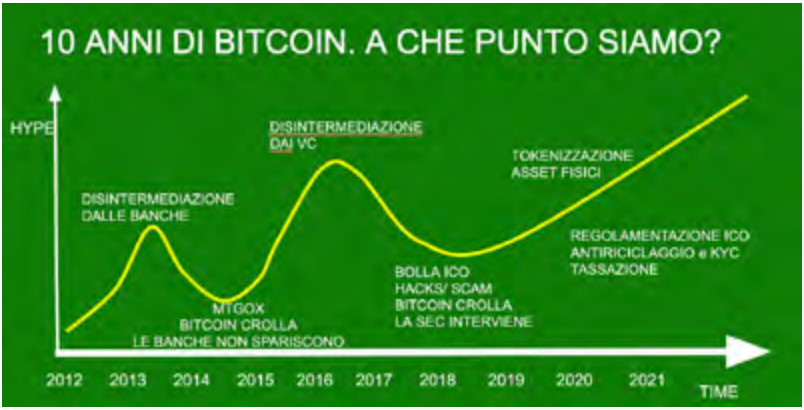
- **Paper BCE:** https://www.ecb.europa.eu/pub/pdf/scplps/ecb.lwp16.en.pdf?344b9327fec917bd7a8fd70864a94f6e
- **Smart contract alliance**: https://digitalchamber.org/smart-contracts-whitepaper/
- **Harvard paper**: https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/#3b
- **Nick Szabo**: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html
- **Gazzetta Ufficiale** italiana – legge 12/2019: http://www.gazzettaufficiale.it/eli/id/2019/02/12/19G00017/SG
- **Differenze tra blockchain pubblica e privata**: https://www.zerounoweb.it/software/blockchain/differenza-tra-blockchain-pubbliche-e-private/
- **Analyzing Safety of Smart Contracts** http://wp.internetsociety.org/ndss/wp-content/uploads/sites/25/2018/02/ndss2018_09-1_Kalra_paper.pdf
- **Ethereum Smart Contract Best Practices – Known Attacks** https://consensys.github.io/smart-contract-best-practices/known_attacks/
- **Ethereum Smart Contract Best Practices – Security Tools** https://consensys.github.io/smart-contract-best-practices/security_tools/
- **Incidenti negli smart contract** https://medium.com/new-alchemy/a-short-history-of-smart-contract-hacks-on-ethereum-1a30020b5fd

Il 2018 dei Crypto Exchange

[A cura di Davide Carboni]

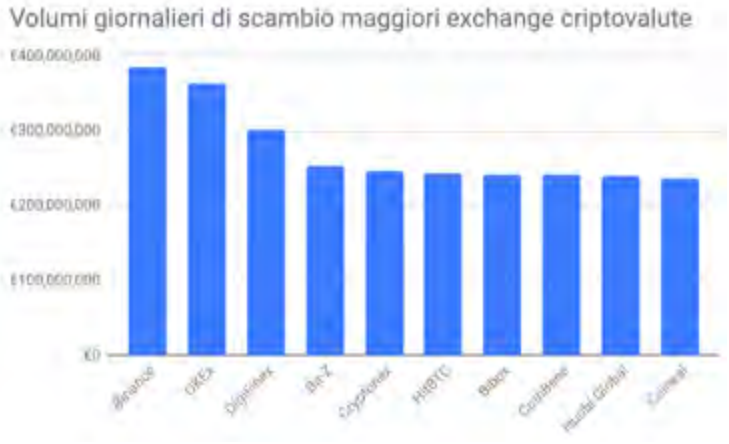
A 10 anni dalla nascita di Bitcoin è giusto fare una piccola analisi dell'evoluzione che questo nuovo settore ha rapidamente attraversato ed in particolare analizzare le nuove problematiche di sicurezza che in questo campo sono aggravate dal fatto che le intrusioni informatiche e le frodi si traducono direttamente una perdita finanziaria vista la irrevocabilità e disintermediazione delle transazioni in blockchain.

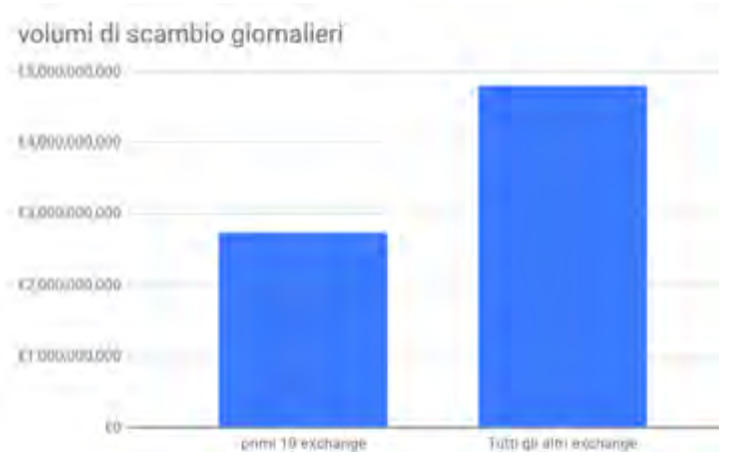
La febbre del 2017 è alle nostre spalle e il 2018 è stato un bagno di umiltà per tutto il settore, e probabilmente anche un periodo di filtro dove i progetti senza valore aggiunto si sono dissolti quasi da soli, lasciando però sul campo investitori che ancora si leccano le ferite e un generale senso di disillusione. Ma come al solito non bisogna buttare il bambino con l'acqua sporca e così come non bisogna sopravvalutare una tecnologia nel breve termine non bisogna neanche sottovalutarla nel lungo termine. I buoni progetti ci sono e sicuramente emergeranno.



In questo mercato ribassista un settore che comunque non conosce ancora crisi è quello degli exchange di criptovalute. Pur essendo questo un ambiente affollato, il business model è tanto semplice quanto profittevole. Gli utenti si registrano, comprano criptovaluta in cambio di moneta euro o dollaro e fanno trading. Ogni operazione viene tassata dall'exchange (tranne il deposito in genere). Inoltre i progetti che oggi fanno ICO e domani faranno STO (Security Token Offering) hanno bisogno di spazio e visibilità e quindi pagano per essere listati in un exchange perché poi i grandi hub di informazione come Coinmarketcap o Cryptocompare rilancino a livello globale l'andamento dei token, funzionando da listini globali cross-exchange.

Gi exchange sono anche il punto di maggior centralizzazione di tutto l'ecosistema crypto, come tale sono pochi (centinaia in effetti ma pochi quelli hanno volumi giornalieri di scambio superiori ai cento milioni di dollari[1]), gestiscono cospicue somme (hanno grandi liabilities) e non godono integralmente della sicurezza della blockchain in quanto sono sostanzialmente dei grossi wallet le cui chiavi private sono gestite all'interno del processo aziendale che come al solito è un mix di operazioni umane e programmi informatici che espongono varie superfici di attacco.





[1] https://coinmarketcap.com/it/rankings/exchanges/

Funzionamento di un exchange centralizzato

Prima di esaminare il 2018 dei crypto exchange facciamo una brevissima introduzione sul loro funzionamento. Un exchange "centralizzato" altro non è che che un sistema informatico che attraverso un'applicazione web o mobile, permette a degli utenti di registrarsi attraverso una procedura di sign up, di creare un profilo personale che a seconda dei casi richiede diversi livelli di verifica dell'identità e di comandare il sistema nella gestione di asset crittografici tra i quali criptovalute e valute nazionali. Quest'ultima possibilità non è scontata, in quanto la possibilità di gestire valute a corso legale per conto di un cliente è una pratica soggetta ad autorizzazioni di tipo "parabancario" che saranno più o meno impegnative a seconda della giurisdizione in cui opera l'exchange.

Quello che dunque in genere l'utente può fare mentre utilizza un exchange consiste in tre operazioni fondamentali:

- depositi in criptovaluta o in moneta a corso legale.
- Prelievi in criptovaluta o in moneta a corso legale.
- Ordini di trading, ovvero la richiesta di vendere o comprare una determinata parte dei propri asset in cambio di altri presenti sul mercato dell'exchange

La caratteristica fondamentale di un exchange centralizzato, come dice il nome, è che questo gestisce gli asset in nostro nome e per nostro conto. Questo si traduce nel fatto che è l'exchange a possedere le chiavi private per poter movimentare i fondi dall'exchange verso altri indirizzi della blockchain. Mentre le operazioni di trading e i relativi aggiornamenti dei saldi sono gestiti attraverso transazioni interne nel database dell'exchange senza transazioni in blockchain. Questo significa una grossa semplificazione per l'utente ed una grande rapidità di esecuzione degli scambi, ma in pratica significa anche che in caso di downtime, attacco informatico o altro incidente di sicurezza a danno dell'exchange che i fondi di tutti i clienti sono bloccati o compromessi. In questo senso un furto in un exchange di criptovalute è persino peggio di un furto informatico in una banca, infatti mentre le transazioni di moneta elettronica fiat sono più facilmente revocabili attraverso azioni delle pubbliche autorità, un furto di chiavi private e conseguente transazione in blockchain a beneficio di un criminale è praticamente impossibile da impedire e revocare, sebbene in molti casi le transazioni in blockchain sono facili da seguire e i relativi fondi tracciati ("tainted coins").

Funzionamento di un exchange decentralizzato

Al contrario del precedente, un exchange decentralizzato è in genere costituito da un protocollo di partecipazione che prevede che gli utenti gestiscano direttamente le chiavi private dei loro fondi, e impegnino durante il trading tali fondi in smart contract che poi possono autonomamente e senza l'intervento di un sistema centralizzato realizzare le stesse funzioni di matching di un order book. In questo caso gli utenti sono responsabilizzati nella gestione dei loro asset, non hanno a disposizione un meccanismo di "password recovery" e se smarriscono i loro segreti crittografici di fatto smarriscono i loro fondi. Non esiste un'architettura

unica per questo genere di exchange e non tutti fanno uso di smart contract. L'unica caratteristica che li contraddistingue è l'assenza di un gestore incaricato di gestire i fondi dei vari partecipanti. Solitamente questi exchange sono più complessi per quanto riguarda l'utilizzo. Il vantaggio per l'utente nell'uso di tali exchange decentralizzati è che non esistendo un sistema centrale di gestione dei fondi è praticamente esente dalle tipologie di attacco che affliggono gli exchange centralizzati. Tuttavia decentralizzazione non significa invulnerabilità. Implementazioni scorrette del protocollo, vulnerabilità degli smart contract e tecniche di ingegneria sociale possono sempre essere sfruttate dagli hacker per eventuali attacchi.

Attacchi del 2018

Il primo o per lo meno il più importante incidente per un exchange risale al collasso di MtGox nell'ormai lontano 2014. Tale exchange all'epoca aveva un volume di scambi pari a circa l'70% di tutti gli scambi in bitcoin[2]. Si può dire che l'incidente di MtGox ha letteralmente creato il genere e con questo incidente sono anche state messe in pratica e affinate per la prima volta le tecniche investigative e di blockchain intelligence che oggi sono a disposizione di istituzioni, banche e blockchain companies.

Il 2018 non è stato un anno idilliaco e ci sono state truffe e hack in una misura superiore a quanto mai visto in passato. Anche le modalità usate dai criminali e dai truffatori come al solito sono molteplici. Ad esempio un giovane truffatore è riuscito a sottrarre $1 milione dall'account Coinbase di un utente di San Francisco attraverso la tecnica del SIM swapping, ovvero convincendo l'operatore mobile a far assegnare alla propria SIM il numero che al momento era in possesso della vittima. Con questo trucco[3] il truffatore ha potuto sfruttare la procedura 2FA e accedere con relativa facilità all'account della vittima.

Nel 2018 sono state trafugate tra furti e truffe circa $1.7B[4] dei quali una buona parte è ancora in circolo sotto forma di criptovaluta in cerca di una qualche soluzione di riciclaggio. Di questi $1.7B, circa $950 milioni sono stati trafugati da exchange e infrastruttura (ovvero wallet e blockchains). Circa 3.6x volte quanto accaduto nel 2017.

2 https://blogs.wsj.com/briefly/2014/02/25/5-things-about-mt-goxs-crisis/?mg=prod/accounts-wsj

3 https://www.cnbc.com/2018/11/21/hacker-lifts-1-million-in-cryptocurrency-using-mans-phone-number.html

4 https://ciphertrace.com/crypto-aml-report-2018q4/

Tra gli incidenti degni di nota del 2018[5] ricordiamo l'hack di circa $500 milioni di controvalore in criptovaluta NEM subìto dalla piattaforma giapponese Coincheck. Nessun dettaglio è stato fornito dai gestori del servizio che semplicemente respingono ogni accusa che si trattasse di una truffa orchestrata dal loro staff. Attraverso il tracciamento in blockchain delle transazioni Coincheck ha scoperto 11 indirizzi dove le criptovalute sottratte sono state "parcheggiate" in attesa di riciclaggio e tali indirizzi sono stati resi pubblici e marchiati con la label "coincheck_stolen_funds_do_not_accept_trades_owner_of_this_account_is_hacker".
Laddove molti exchange giustamente conservano una cospicua parte dei propri fondi in quelli che sono chiamati cold wallet, ovvero sistemi di gestione delle chiavi che normalmente sono offline e richiedono procedure multifirma e hardware dedicato per firmare le transazioni, a quanto pare Coincheck teneva tutti i suoi NEM (o meglio quelli dei suoi utenti) in hot wallet che invece sono dei software online pensati per un uso frequente e automatico della firma digitale e che espongono una superficie d'attacco molto più estesa.
Un altro importante incidente è avvenuto nell'exchange italiano BitGrail dove un controvalore di $195 milioni è improvvisamente scomparso. Anche in questo caso le responsabilità non sono chiare e da più parti è stato ipotizzato[6] che si sia trattato di una frode dell'exchange stesso piuttosto che un'intrusione informatica da parte di terzi.
Chiudiamo questa breve e non esaustiva rassegna degli hack 2018 con CoinRail[7], un exchange coreano che ha perso il 30% dei suoi asset per un ammontare complessivo di circa $40 milioni. Anche in questo caso l'account dell'hacker è facilmente visibile nella blockchain Ethereum[8] e rinominato con Fake_Phishing1432.

[5] https://freestartupkits.com/articles/technology/cryptocurrency-news-and-tips/worst-cryptocurrency-exchange-hacks-of-all-time-2018/

[6] https://ethereumworldnews.com/nano-bitgrail-hack-lawsuit-2018/

[7] https://www.startmag.it/fintech/monetevirtuali-coinrail/

[8] https://etherscan.io/address/0xf6884686a999f5ae6c1af03db92bab9c6d7dc8de#tokentxns

Il report di ICO RATING e ranking degli exchange

Alla luce di questi dati è interessante capire come i vari exchange affrontano il problema della sicurezza. Uno studio è stato realizzato da ICO Rating[9] e pur non trattandosi di un'analisi approfondita o estremamente rigorosa, e sulla quale si potrebbe obiettare perché sono stati scelti alcuni criteri piuttosto che altri, ha comunque il pregio di fornire un framework di valutazione semplice e di esibire il risultato della sua applicazione a circa 200 diversi servizi di exchange.

Le sezioni in cui il report analizza la sicurezza di un exchange sono: user security, DNS/Registrar security, Web security e DoS protection. Ad esempio nella sezione user security sono valutate la possibilità di creare password deboli, la conferma di ogni operazione rilevante da un punto di vista monetario attraverso la posta elettronica e la disponibilità di 2FA.

Sempre a titolo di esempio, per la sezione web security sono valutate caratteristiche come la presenza dell'header HTTP Strict-Transport-Security o tecniche per la prevenzione di Clickjacking attacks. Per una panoramica completa dei vari tipi di attacchi e contromisure elencate nel report si invita il lettore a consultare direttamente lo stesso.

Secondo il report i migliori exchange valutati secondo le categorie di attacco di cui sopra sono Kraken, Cobinhood e Poloniex. Coinbase si classifica solo in nona posizione dato che per questo sono state rilevate alcune criticità nella sezione Registrar e Domain security.

Scorrendo la classifica troviamo Binance solo al 34simo posto, non molto lusinghiero apparentemente, vista la grandissima popolarità che tale exchange ha raggiunto nel 2018. Il primo exchange italiano è The Rock Trading. Sempre come nota di curiosità, Cryptopia e QuadrigaCX che sono stati oggetto dei primi incidenti di sicurezza nel Gennaio 2019 si piazzano rispettivamente in 60sima e 51sima posizione.

È particolarmente curioso il caso di QuadrigaCX che in sostanza pare essere finito in una situazione di insolvenza causata dalla morte del suo fondatore[10] e conseguente perdita delle chiavi private che a quanto pare gestiva personalmente senza una adeguata procedura di recovery in casi diciamo eccezionali. Criteri come processi di trasmissione condizionale dei segreti crittografici e in generale di gestione dei cold wallet sembrano non essere adeguatamente contemplati in questo report, che magari per il 2019, aggiornerà la propria lista di criteri.

[9] https://icorating.com/report/exchange-security-report-v-20-update/

[10] https://cointelegraph.com/news/crypto-exchange-quadrigacx-missing-145-mln-after-death-of-founder

Conclusioni

In conclusione l'anno 2018 è stato sicuramente caratterizzato da numerosi incidenti nei sistemi di exchange di criptovalute, tuttavia non dimentichiamo che si tratta di un'industria emergente nella quale non sono ancora stati stabiliti degli standard internazionalmente riconosciuti per poter operare. $1.7B sono una cifra astronomica e per avere un termine paragone si tratta di una cifra comparabile con le transazioni fraudolente delle carte di credito di tutto il circuito SEPA i cui danni ammontano a circa €.8B all'anno[11]. Pur essendo le criptovalute una categoria di asset ancora limitata nel loro utilizzo ad una nicchia di utenti piuttosto esigua, visti questi numeri si comprende l'urgenza e la necessità di un significativo miglioramento della sicurezza dei servizi in questo settore.

Se oggi il furto di criptovaluta ha una certa diffusione in parte è anche dovuto ad una non omogenea normativa AML nel settore. Gli "attori" di questi attacchi informatici e frodi legate alla blockchain in generale cercano di riciclare i proventi delle loro attività attraverso giurisdizioni che non hanno una normativa antiriciclaggio restrittiva.
Tuttavia il 2018 è stato anche un anno in cui c'è stata una forte presa di coscienza dei legislatori rispetto al fenomeno delle criptovalute e ICO. In questo senso entro il 2019[12] la maggior parte delle giurisdizioni si doterà di una disciplina antiriciclaggio per il settore criptovalute.

[11] https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport201809.en.html

[12] https://www.financemagnates.com/cryptocurrency/regulation/financial-action-task-force-to-issue-its-crypto-guidelines-by-mid-2019/

Il mercato italiano della Sicurezza IT: analisi, prospettive e tendenze secondo IDC

Le statistiche degli attacchi informatici sono evidenziate dai principali operatori del mercato e dalle vicende pubblicate nei giornali quasi quotidianamente. La criminalità elettronica sta di fatto diventando una delle forme più diffuse di criminalità comune pur avendo poco a che fare, in termini di complessità e ingegno, con le forme più tradizionali di criminalità, poiché investe intensamente nella strumentazione tecnologica per avvantaggiarsi delle proprie vittime, eludere i propri avversari, sopravanzare in astuzia sia le imprese che le forze dell'ordine.

Nel 2019 la Sicurezza IT si confermerà come il campo di una intensa competizione tecnologica fra gli operatori, il cybercrime e gli stati. Dall'osservatorio internazionale di IDC emergono diverse tendenze che proseguiranno il proprio corso nell'anno a venire, e in particolare alcuni temi saranno al centro dell'attenzione internazionale, come ad esempio l'impiego sistematico del Machine Learning in diverse tipologie di attacchi, le tensioni politiche internazionali che daranno spazio a ulteriori scambi di accuse in merito alla "latente" guerra informatica globale, le sfide tecnologiche e organizzative che le imprese stanno affrontando nei processi di digitalizzazione dell'economia e della società, dalla Trasformazione Digitale fino all'Internet delle Cose.

Ogni anno IDC propone una breve panoramica che guarda alle tendenze internazionali più significative che andranno a incidere sull'orizzonte temporale di breve, medio e lungo termine nel settore della Sicurezza IT. Tra le tendenze tecnologiche più significative che verranno rappresentate in questa sezione, quest'anno è possibile ricordare la progressiva evoluzione dei Managed Security Services, la diffusione del Key Management as a Service, l'automazione dei processi di recovery & remediation attraverso l'Intelligenza Artificiale, il consolidamento della spesa per le soluzioni di encryption, l'affinamento tecnico-legale del concetto di identità digitale.

Fino a qualche decennio addietro, quando le imprese si rivolgevano ai Managed Service Providers, l'esigenza discendeva principalmente dalla necessità di gestire la complessità tecnica di alcuni dispositivi, come la configurazione di firewall, il monitoraggio dell'up-time dei servizi, l'aggiornamento e la gestione delle patch, il monitoraggio dei log degli eventi. Al crescere della complessità degli ambienti IT, sempre più eterogenei e sempre meno inclusi all'interno del perimetro aziendale, le esigenze di gestione diventano più complesse: dai tradizionali servizi gestiti focalizzati sulla gestione professionale di specifiche soluzioni tecniche il focus del mercato si sposta sulla gestione del ciclo di vita dei rischi e del malware, il Threat Life-Cycle Management. Secondo IDC, entro il 2024 circa il 90% dei clienti dei servizi gestiti adotteranno servizi per la gestione del ciclo di vita dei rischi IT.

Nel momento in cui gli ambienti ibridi e cloud diventano sempre più spesso una opzione comune nelle scelte infrastrutturali delle imprese, si palesa la crescente necessità di provvedere a una gestione più accorta delle chiavi di crittografia. Per rispettare gli obblighi di regolamenti e normative, nel trasferimento dei propri dati sulle nuove piattaforme, le imprese sono chiamate in molte occasioni a un processo oneroso e macchinoso di gestione e trasferimento delle chiavi di crittografia originali. Secondo IDC, la necessità di ovviare a queste incombenze aprirà maggiore spazio al Key-Management-as-a-Service: entro il 2021 l'adozione da parte del mercato crescerà di oltre venti punti percentuali a livello globale.
L'endemica carenza di personale nella cybersecurity, coniugandosi con l'industrializzazione massiva del malware e l'espansione degli ambiti di vulnerabilità di nuovi ambienti e infrastrutture (dalla Mobility all'IoT), apre una voragine nelle risorse disponibili per le attività di Security Intelligence, rendendo indispensabile l'impiego di forme di automazione intelligente basate su algoritmi di Predictive Analytics e Machine Learning. Entro il 2021, almeno il 50% degli allarmi di sicurezza dei SOC saranno gestiti attraverso l'automazione che porterà a misure di risposta automatica senza l'intervento diretto degli analisti di sicurezza.
Un effetto collaterale positivo dei processi di Trasformazione Digitale e di migrazione dei dati su piattaforme Cloud e Big sarà il consolidamento delle applicazioni di crittografia una volta presenti nei diversi silos aziendali. Le migrazioni verso i Data Lakes consentono alle organizzazioni di riconsiderare in una nuova prospettiva costi e benefici dei precedenti investimenti nelle soluzioni, che fino a pochi anni fa erano considerati troppo onerosi per la sostituzione e l'aggiornamento. Secondo IDC, entro il 2023 da questo processo di consolidamento sarà possibile razionalizzare circa un terzo dello spending per le soluzioni di crittografia.

Ultima previsione che si intende rappresentare in questa introduzione. La proliferazione di identità fittizie rischia di incidere negativamente sulla digitalizzazione dell'economia e della politica. Nel prossimo futuro le identità digitali saranno sempre più spesso forgiate ricorrendo al footprint digitale che arriva dai sensori dell'ambiente circostante, dai wearable fino all'IoT, determinando un pool variabile di informazioni sensibili che consentiranno una corretta identificazione personale e ridurranno al minimo il rischio di abusi. Nel breve termine, si andranno moltiplicando le authority nazionali (come ad es. Aadhaar) per la creazione di identità digitali univoche che siano riconducibili alle persone fisiche. Secondo IDC, entro il 2024, soltanto il 20% delle identità digitali saranno legalmente individuate rispetto a quelle giuridiche-personali, quindi il far-west dell'identità digitale durerà ancora tanti anni.

La Sicurezza IT in Italia: le previsioni di spesa aggregata

Nei paragrafi che seguono viene proposta una sintetica rappresentazione quantitativa dei principali segmenti della Sicurezza IT con riferimento al mercato italiano, in base alle tassonomie standard impiegate da IDC a livello internazionale. Le informazioni derivano dalla stima dei risultati dei principali operatori con riferimento ai ricavi di licenze, rinnovi, manutenzioni e sottoscrizioni a consumo di servizi rispetto al territorio nazionale. Le stime de-

rivano sia dalla *knowledge base* accumulata da IDC a livello internazionale sia dalla ricerca condotta a livello locale, dai contatti diretti con gli operatori e dall'analisi delle comunicazioni economico-finanziarie. IDC impiega tassonomie standard, neutrali rispetto alle denominazioni commerciali impiegate dagli operatori; per facilitare i processi di conciliazione dei dati, le informazioni raccolte durante le indagini vengono ricondotte nell'ambito di tali tassonomie standard, rispetto le quali vengono categorizzare e comparate le informazioni raccolte nelle varie geografie.

Il Software per la Sicurezza IT, segmentato nelle aree della Web Security, del Security & Vulnerability Management, della Network Security, dell'Identity & Access Management e dell'Endpoint Security, rappresenta in Italia un valore complessivo di circa 380 milioni di euro nel 2018 (***Fig. 1***). Con un $CAGR^{2018\text{-}2021}$ di sette punti percentuali, con una prospettiva di lieve ridimensionamento rispetto alle stime dello scorso anno, a trainare la crescita del comparto sono essenzialmente le applicazioni legate a Security & Vulnerability Management e Network Security, in alcuni casi con tassi di crescita che arrivano a due cifre, mentre le altre aree esprimono tendenziali consistentemente inferiori. Si conferma la rilevanza strategica dell'area SVM nell'interpretare la necessità di rinnovamento delle imprese italiane con una progressiva migrazione verso tecnologie sempre più comunemente fondate su analisi di dati e intelligence nella valutazione del rischio malware.

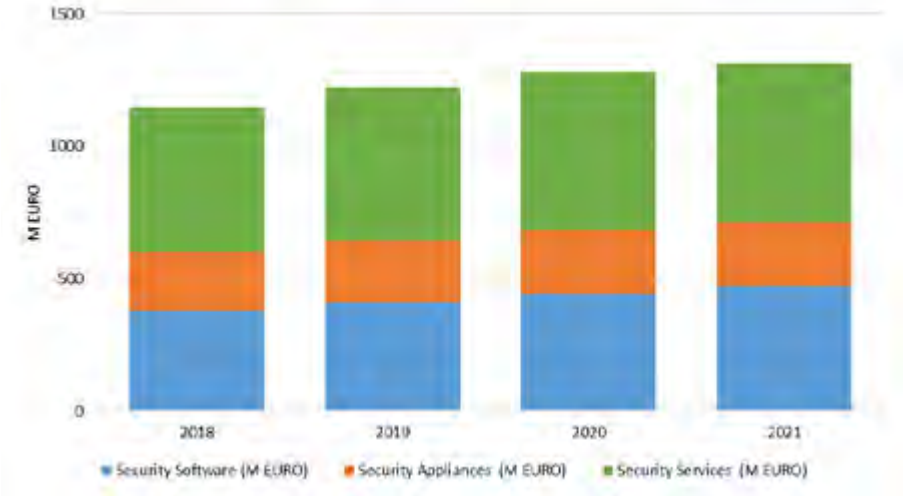


Figura 1 - *La Sicurezza IT, i principali segmenti del mercato italiano (Software, Appliance e Servizi). Fonte: IDC Italia, 2019*

In merito alla categoria delle Appliances per la Sicurezza IT, IDC segmenta il mercato in cinque aree principali (VPN, Firewall, IDP, Unified Threat Management, Content) che nel 2018 hanno espresso un valore complessivo di circa 220 milioni di euro (***Fig. 1***).
Con un $CAGR^{2018\text{-}2021}$ stimato in circa quattro punti percentuali, IDC propone un limitato ridimensionamento nelle sue stime di medio termine: la maggiore intensità di crescita nell'orizzonte previsionale considerato è riconducibile all'area VPN, nell'ambito della quale si prevede un tasso di crescita consistentemente superiore alle due cifre nel medio termine.
I Servizi per la Sicurezza IT rappresentano il comparto caratterizzato dalla maggiore dinamicità in termini di continuo rinnovamento delle proposizioni dei principali operatori, con una articolazione sempre più profonda dei servizi proposti al mercato. Proponendo una tassonomia generale e neutrale rispetto al mercato, IDC stima la dimensione del comparto in base alla ripartizione tra servizi di IT Consulting e servizi di System Integration/ Implementation. Con un $CAGR^{2018\text{-}2021}$ attorno ai tre punti percentuali, in sostanziale continuità rispetto alle previsioni dello scorso anno, i servizi hanno un valore superiore ai 500 milioni di euro nel 2018.

Opportunità e sfide secondo le imprese italiane

Nella sezione seguente verranno evidenziati i principali risultati di una indagine condotta da IDC sul mercato italiano che ha coinvolto circa 300 imprese nel segmento delle Medie e Grandi Imprese, rappresentando gran parte della struttura imprenditoriale del Paese (dal manifatturiero ai servizi, dal commercio alla pubblica amministrazione, dalle utilities fino ai trasporti e alle comunicazioni).
Lo strumento di indagine, composto da circa una ventina di quesiti di approfondimento con domande a risposta chiusa e a risposta multipla, ha indagato i fattori che indirizzano la spesa in Sicurezza, le priorità principali dell'impresa, sia lato business che technology, la rilevanza della Sicurezza rispetto a diversi paradigmi tecnologico-organizzativi (in modo particolare rispetto alla Trasformazione Digitale). Il questionario è stato somministrato a un campione che comprende sia le figure apicali dell'IT aziendale (CIO/ Directors/ etc.), sia figure più specializzate che danno una centralità di rappresentanza al tema della Sicurezza IT (Chief Information Security Officer/ IT Security Manager/ etc.), sia figure di middle management più generaliste per cui la Sicurezza IT rappresenta un compito comunque imprescindibile (IT Manager/ Responsabili IT/ etc.).
Il dato campionario è stato estrapolato all'universo delle imprese in base a elaborazioni IDC dei dati ISTAT così da dare una rappresentazione del fenomeno della Sicurezza IT rispetto a un universo aggregato di circa 25.000 imprese in Italia.

Tendenze di spesa e investimento del mercato italiano

Dalle ultime indagini condotte sul segmento delle imprese sopra i 50 addetti in merito alle previsioni di investimento in area ICT, emergono prospettive positive per il 2019: circa il 30% prevede una sostanziale espansione del budget rispetto all'anno precedente, circa il 60% delle imprese annuncia un budget stabile, mentre soltanto il 10% segnala una po-

tenziale riduzione. Rispetto a queste dinamiche di fondo, le imprese italiane procedono all'allocazione degli investimenti destinati alla Sicurezza IT: il 32% delle imprese dedica alle tecnologie per la sicurezza fino al 3% del budget ICT, il 26% tra il 3 e il 10%, soltanto il 4% investe oltre il 10% del proprio budget ICT. Le tendenze generali del budget ICT rappresentano ancora un fattore essenziale nella determinazione del budget rate per la Sicurezza IT: quando il budget ICT è in espansione, le imprese con un budget rate superiore al 10% salgono al 9,6%, mentre quando è in contrazione lo stesso dato scende allo 0,3%. Così come la congiuntura economica generale ha un impatto determinante nella definizione del budget ICT, allo stesso modo le dinamiche del budget ICT determinano in modo diretto gli investimenti disponibili per la Sicurezza IT, con un raggio di variazione da un decimo fino al doppio della media.

Un ulteriore fattore che incide in misura importante nella definizione del budget destinato alla Sicurezza IT è dato dalla specifica considerazione attribuita a tali tecnologie come autonome voci di spesa tra i capitoli di investimento del budget ICT: oltre il 40% delle imprese indica la Sicurezza IT come un investimento strategico per abilitare nuovi modelli, circa il 30% la indica come una semplice voce di spesa corrente come molte altre, circa il 10% la considera niente di più di un costo del tutto contingente. Nel complesso le imprese di media e grande dimensione prestano una certa attenzione rispetto alla necessità di tutelare i dati aziendali. L'effetto di questa maggiore sensibilità si riflette in modo immediato e diretto nell'ampiezza del budget rate destinato alla Sicurezza IT (***fig. 2***): nel momento in cui le tecnologie per la sicurezza assumono una sempre maggiore rilevanza strategica per i progetti aziendali, la curva che rappresenta la distribuzione dell'intensità dei budget cresce nella sua estremità a destra: la *thin tail* si trasforma progressivamente in una *fat tail*, aumenta in modo sostanziale la frequenza di imprese con un budget rate compreso approssimativamente tra il 7 e il 12%.

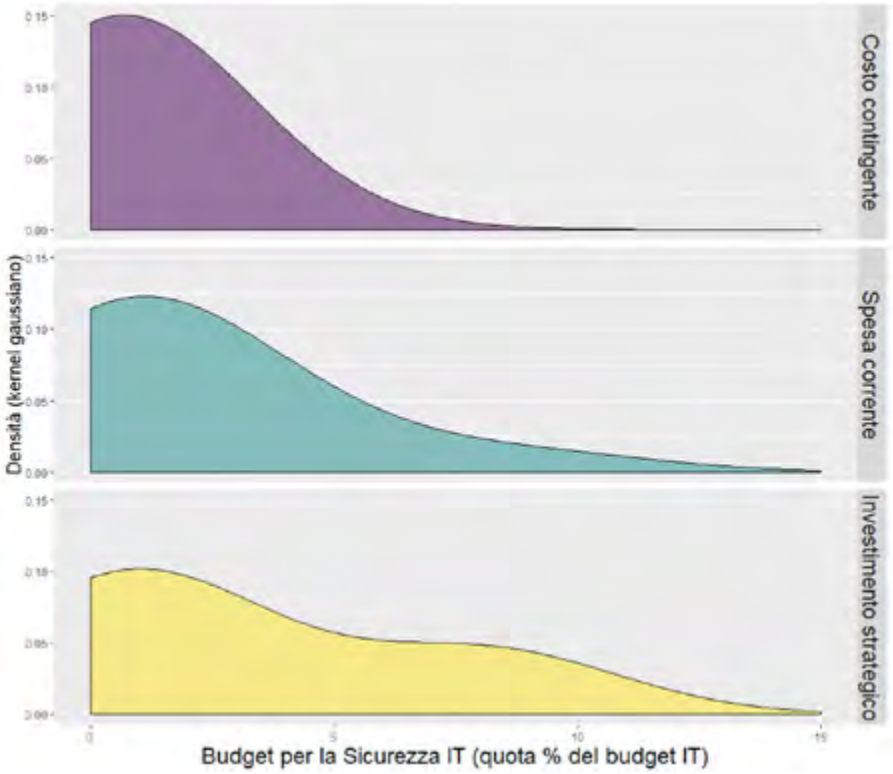


Figura 2 - *Stima della distribuzione del budget in base alla percezione del ruolo della Sicurezza IT.*
Fonte: IDC Italia, 2019 (rispondenti n=300, imprese con oltre 50 addetti; estrapolazione all'universo)

Nelle edizioni precedenti del rapporto si è più volte evidenziata la stretta correlazione tra Sicurezza IT e Trasformazione Digitale, soprattutto a livello di priorità strategiche nell'agenda delle imprese italiane. Esaminando più in profondità tale relazione e cercando di coglierne l'impatto a livello economico, l'associazione tra le dimensioni dimostra una intensità meno apprezzabile del previsto, quantomeno rispetto alle dimensioni quantitative dei budget.

Osservando il dato che emerge da ***fig. 3***, la distribuzione dei budget destinati alla Sicurezza è sostanzialmente omologa fra le imprese che stanno portando avanti progetti avanzati di trasformazione digitale e quelle che invece stanno ancora muovendosi in modo preliminare, e, soprattutto, le differenze nel comportamento delle estremità delle distribuzioni è piuttosto limitato. L'unica differenza sostanziale si osserva nello spostamento della mediana (linea

in grassetto nei box): nelle imprese che si stanno trasformando il dato si attesta attorno al 2%, mentre nelle imprese che sono ancora all'inizio del percorso si posiziona sotto l'1%.

Come già osservato in altre indagini, la Trasformazione Digitale è un fattore di sviluppo molto importante, ma da sola non ha probabilmente la forza sufficiente per andare a incidere sulla dimensione effettiva del budget, soprattutto quando il budget della Sicurezza è allocato sulla quota destinata alla manutenzione dell'IT, anziché su quella destinata all'innovazione dei sistemi.

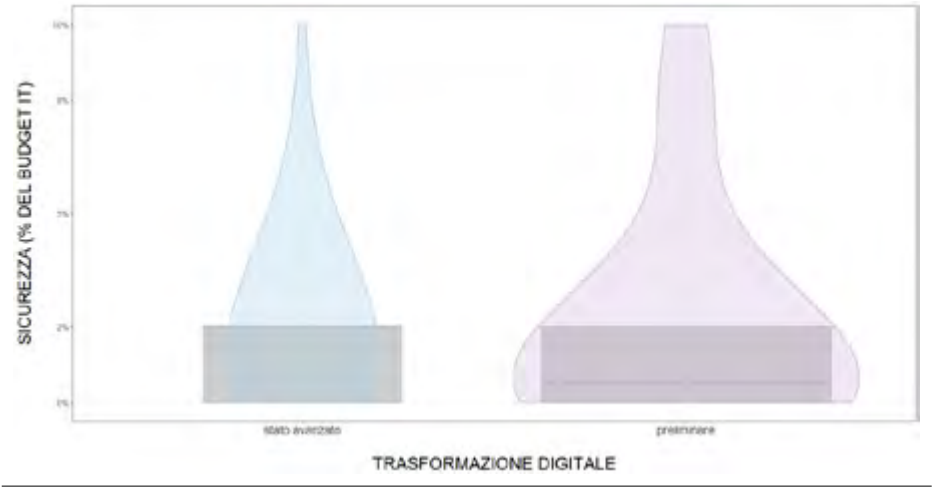


Figura 3 - *L'impatto della Trasformazione Digitale sul budget per la Sicurezza IT. Fonte: IDC Italia, 2019 (rispondenti n=300, imprese con oltre 50 addetti; estrapolazione all'universo)*

Infatti, per comprendere quali sono le potenzialità inespresse delle imprese italiane, in termini di investimento nelle tecnologie per la sicurezza, occorre guardare al rapporto tra budget destinato all'innovazione e budget destinato alla manutenzione dei sistemi. Da quanto emerge dalle ultime indagini nel perimetro delle organizzazioni di media e grande dimensione, le imprese italiane prevedono di allocare circa il 60% del loro budget IT ad attività di manutenzione, mentre il restante 40% ad iniziative legate all'innovazione dei sistemi. Si è già osservato in precedenza come la percezione della Sicurezza IT sia piuttosto differenziata nel segmento delle Medie e Grandi Imprese: in molti casi le tecnologie per la sicurezza sono considerate un investimento strategico, in altrettanti casi sono considerate come costi correnti, se non del tutto contingenti. Queste considerazioni concorrono necessariamente nella determinazione del budget destinato alla Sicurezza IT, insieme alle valutazioni relative alla manutenzione/ innovazione dei sistemi.

Come si osserva in ***fig. 4***, dove sono rappresentate per curve di livello le densità congiunte delle previsioni relative al budget rate per la Sicurezza IT e quelle relative alle dimensioni dicotomiche di innovazione vs. manutenzione, è possibile osservare quali siano le potenzialità di crescita della sicurezza quando sussiste una associazione positiva del tema della sicurezza con quello dell'innovazione aziendale. Laddove le tecnologie diventano il fattore abilitante di nuovi modelli digitali, le risorse destinate alla Sicurezza IT si espandono in misura ragguardevole: passando dal riquadro di sinistra, dove la sicurezza è soltanto una spesa contingente, fino a quello di destra, dove ricopre un ruolo strategico, si osserva una progressiva espansione delle curve di livello, che rappresentano la numerosità relativa delle imprese, in alto a destra di ciascun quadrante, ad indicare l'aumento del numero di organizzazioni che investono in misura significativa sui temi della sicurezza e dell'innovazione, in misura che appare consistentemente congiunta e correlata. Quando si legge che la Sicurezza IT è l'abilitatore dell'innovazione aziendale, il fenomeno che concretamente si osserva sul mercato è quello rappresentato nella ***fig. 4***. Viceversa, quando la Sicurezza IT non riveste un ruolo strategico, la grande concentrazione delle imprese si sposta in basso a sinistra di ciascun quadrante, in una direzione che è ampiamente correlata ai budget di manutenzione.

Figura 4 - *Il rapporto tra budget destinato all'Innovazione e alla Sicurezza IT. Fonte: IDC Italia, 2019 (rispondenti n=300, imprese con oltre 50 addetti; estrapolazione all'universo)*

In conclusione, nell'orizzonte temporale del 2019 il mercato della Sicurezza IT persevera nella sua tendenza endemica a procedere con intensità marcatamente divergenti tra segmenti di aziende: una prima parte del mercato riesce a integrare le tecnologie della sicurezza in una roadmap organica di sviluppo aziendale, in un programma di trasformazione in fase di implementazione avanzata, e dunque investe riconoscendo un ruolo strategico ad alcune soluzioni tecnologiche; una seconda parte del mercato non è ancora riuscita a comprendere come contestualizzare il tassello della sicurezza nel puzzle molto spesso ca-

otico delle trasformazioni e delle priorità aziendali. Questa divergenza di visione, che può apparire molto astratta, si traduce molto più concretamente in una differenza nell'intensità di investimento che può arrivare fino a sette volte.

La Sicurezza IT tra priorità tecnologiche e di mercato

Nella sezione seguente si affronta l'impatto della Sicurezza IT rispetto alla pianificazione strategica delle imprese, con riferimento sia alle priorità tecnologiche, riconducibili alla progettualità del dipartimento IT, che alle priorità di business e di mercato, riconducibili alla progettualità dell'impresa nel suo complesso. L'intento di questa sezione è quello di evidenziare come la Sicurezza IT svolga un ruolo sinergico rispetto alle altre priorità aziendali, contribuendo a realizzare obiettivi più complessi di trasformazione aziendale, e come le priorità strategiche delle imprese che investono in Sicurezza IT siano differenti, talora in misura significativa, dalle priorità normali delle imprese.

Il 23% delle imprese italiane indica la Sicurezza tra le principali priorità IT delle imprese, insieme ad altri obiettivi tipici della funzione, come l'automazione (40%), il controllo dei costi IT (34%) e la qualità del servizio erogato (27%). Come osservato nelle scorse edizioni del rapporto, la Sicurezza svolge molto spesso la funzione di infrastruttura abilitante e dunque risulta ampiamente correlata con le altre priorità IT: in modo particolare, i dati di quest'anno evidenziano una forte correlazione tra Sicurezza IT e altre priorità come la gestione di ambienti ibridi, il supporto all'innovazione aziendale, la continuità e la qualità del servizio. Questi dati proseguono con continuità la serie storica di evidenze che provano il ruolo della Sicurezza nell'abilitazione dei processi digitalizzazione delle imprese, quantomeno nell'ambito della funzione IT, che forse, tutto sommato, sta diventando uno spazio angusto per la gestione di un tema così ampio come la Trasformazione Digitale.

Quale legame con le priorità di business? Oltre all'inevitabile influenza che le tecnologie per la sicurezza assumono rispetto alle priorità IT, la sinergia tra Sicurezza IT e le priorità di mercato delle imprese italiane sta diventando sempre più stringente e apprezzabile in modo sensibile.

Come evidenziato nella *Fig.* 5, dove si rappresenta il coefficiente tau di Kendall, un numero sempre maggiore di imprese evidenzia una notevole sinergia tra Sicurezza IT e alcuni specifici obiettivi di business, come la collaborazione nella filiera dei partner e degli stakeholder, la conformità alle nuove normative e regolamentazioni, l'innovazione di prodotto e servizio, il miglioramento della marginalità aziendale. In un mondo dove le tecnologie digitali non sono soltanto mezzi di comunicazione, ma sono l'infrastruttura per muoversi nel mercato, la Sicurezza IT non serve soltanto per tutelare le informazioni aziendali, diventa essenziale per competere nell'economia reale.

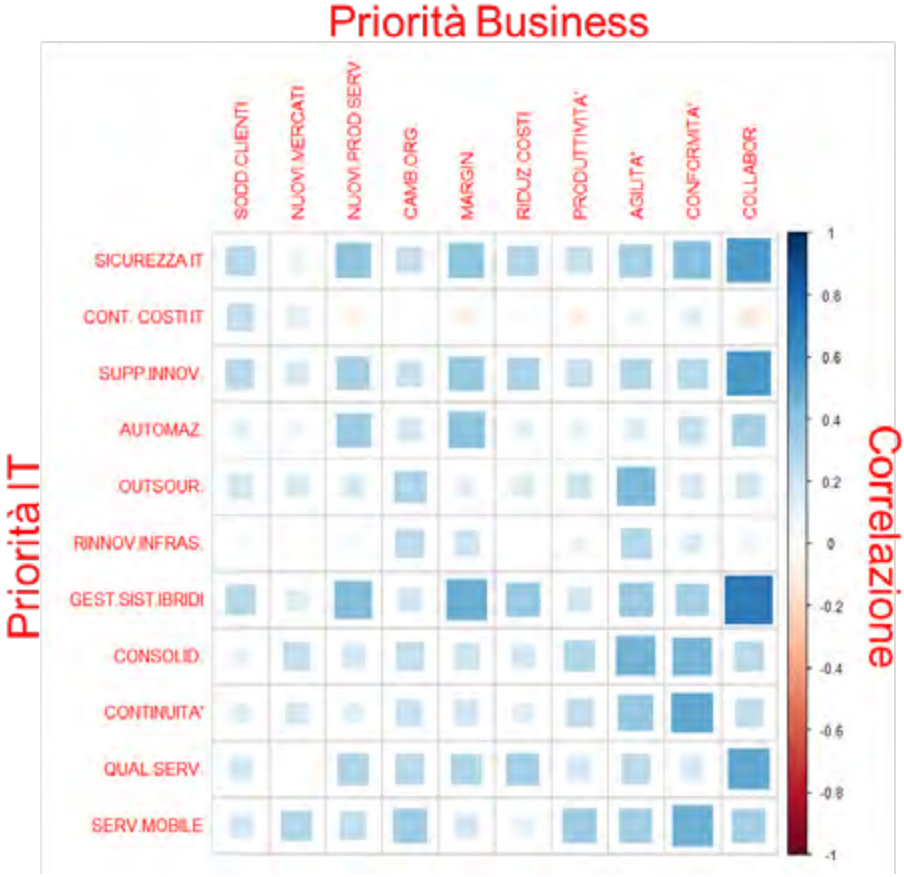


Figura 5 - *La Sicurezza IT tra priorità IT e priorità di business/mercato.*
Fonte: IDC Italia, 2019 (rispondenti n=300, imprese con oltre 50 addetti); estrapolazione all'universo)

Le imprese che investono oltre il 5% del proprio budget ICT nelle tecnologie per la sicurezza esprimono una particolare sensibilità rispetto ad alcune priorità di mercato rispetto alla media delle imprese: circa il 38% delle imprese si rivolge verso temi specifici quali la produttività e l'innovazione di prodotto/ servizio a dispetto di una media del 27%. Anche i temi del cambiamento organizzativo, dell'agilità e del time-to-market, dell'ingresso in nuovi mercati, risaltano in qualche misura in modo più importante tra le imprese che stanno investendo con maggiore intensità nella Sicurezza IT, a ulteriore evidenza del valore sempre più ampio e generale che stanno assumendo alcune tecnologie per garantire la resilienza delle imprese. Da questo punto di vista, la Sicurezza IT assume una potenzialità che oltrepassa la Trasformazione Digitale diventando un dispositivo di garanzia in qualsiasi momento di transizione tecnologica e organizzativa delle imprese.
Questa rilevanza del comparto per le logiche di business si riflette nelle previsioni di investimento delle imprese italiane. Confrontando con le altre aree ICT (***Fig. 6***), emerge con chiarezza l'importanza della Sicurezza IT sotto il profilo degli investimenti pianificati: circa il 30% delle imprese nel perimetro dell'indagine ha pianificato investimenti nell'area della Sicurezza IT nei prossimi 12 mesi, inferiore soltanto alle previsioni sulle applicazioni core-business, che si collocano al 33%, ponendosi ampiamente al di sopra delle altre principali aree di investimento tecnologico. Discorso invece nettamente diverso per i processi di valutazione preliminari, dove soltanto il 4% delle imprese si muove nel territorio grigio dello scouting tecnologico e degli studi di fattibilità, ampiamente al di sotto della media del 17% delle altre aree: al "decisionismo" sotto il profilo della pianificazione si accompagna forse la tendenza a valutare con rapidità le soluzioni su cui investire, forse la tendenza ad attestarsi su scelte tecnologiche consolidate, oppure ancora una oggettiva difficoltà ad approfondire e valutare le tecnologie per la sicurezza.

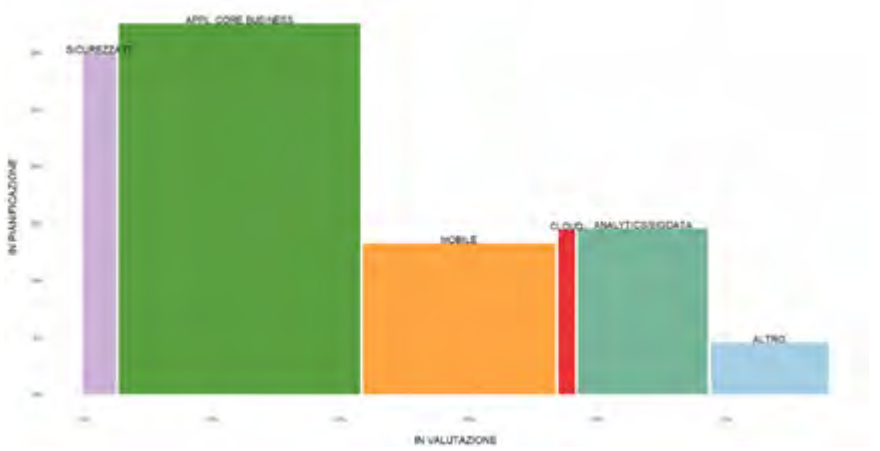


Figura 6 - *La Sicurezza IT tra attività di scouting e investimento. Fonte: IDC Italia, 2019 (rispondenti n=300, imprese con oltre 50 addetti); estrapolazione all'universo)*

Sono molteplici le sfide che le imprese italiane si trovano a sostenere, non solo a livello tecnologico, ma organizzativo e culturale, quando si confrontano con la Sicurezza IT.
È possibile evidenziare una chiara associazione tra il ruolo attribuito alle tecnologie nei capitoli di spesa (contingente-corrente-strategico) e le difficoltà che vengono rappresentate dalle imprese italiane. Senza pretendere di esprimere una specifica direzione in termini di causalità, in termini puramente descrittivi le differenze tra i gruppi risaltano nella Fig. 7, schematizzando in modo piuttosto chiaro tre distinte sensibilità del mercato con cui gli operatori si confrontano quotidianamente.

Una difficoltà tipicamente evidenziata è quella relativa alla disponibilità di adeguate risorse finanziarie da allocare a budget per gli investimenti, segnalata dal 22% delle imprese, che però diventa il fattore bloccante per eccellenza tra le imprese che considerano la Sicurezza una spesa contingente (quasi il 50% delle imprese nel gruppo). Invece, le imprese che affrontano le tecnologie come un investimento strategico mettono in evidenza la difficoltà di assicurare il supporto e la sponsorship del top management aziendale (oltre il 30% dei casi rispetto a un dato medio attorno al 20%). La complessità degli attacchi è un tema neutrale rispetto alle diverse opinioni che le imprese esprimono in merito al ruolo della Sicurezza IT come capitolo di spesa: rimane un tema avvertito dal 20% delle imprese, con una rilevanza marginale, di qualche punto superiore alla media, nel gruppo delle imprese che collocano la Sicurezza tra le spese correnti.

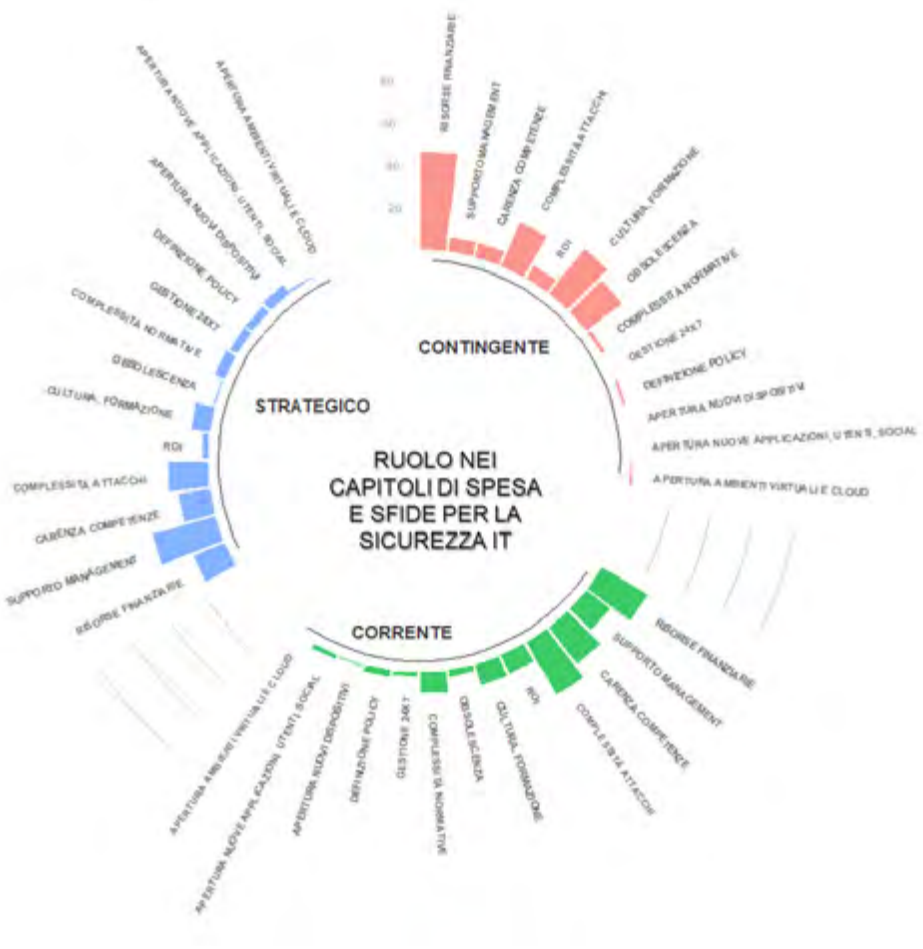


Figura 7 - *La Sicurezza tra le aree di investimento nelle soluzioni ICT. Fonte: IDC Italia, 2019 (rispondenti n=300, imprese con oltre 50 addetti); estrapolazione pesata all'universo)*

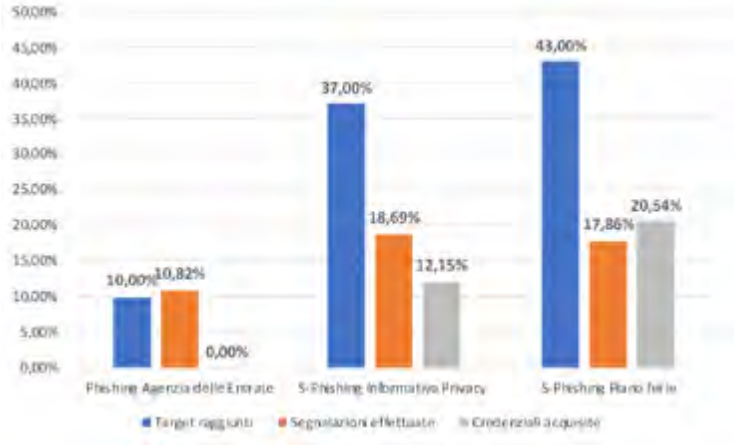
Programmi di security awareness: una necessità non più rimandabile

[A cura di Garibaldi Conte]

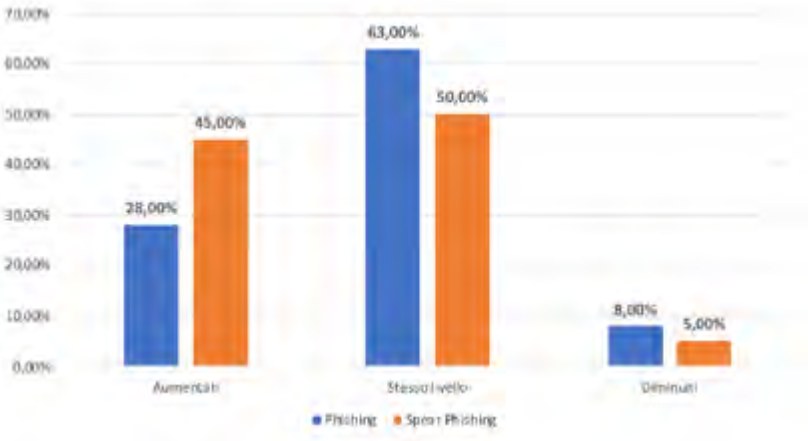
Lo scenario

Tutti gli analisti ed esperti di sicurezza concordano che la maggior parte degli incidenti di sicurezza è legata ad errori umani (si stima che siano circa l'80%-90% degli incidenti) confermando come il fattore umano sia, anche per la sicurezza informatica, l'anello debole del sistema.
Solo in Italia si è stimato che circa il 53% degli attacchi sono dovuti a cause endogene (utilizzo di password deboli e non alfanumeriche, accesso di device aziendali a connessioni pubbliche, navigazione in siti non sicuri e il trasporto di dati sensibili con chiavi USB non cifrate,…) e a queste si sommano gli attacchi di phishing e spear phishing che provocano impatti significativi sull'azienda sia in termini di frodi e dati rubati che come incremento dei costi operativi per il ripristino dagli incidenti occorsi.
Non stupisce quindi che gli attacchi di phishing aumentino sempre più. Dal Rapporto Clusit 2018 si evidenzia un 34% di aumento nel 2017 e un 22% solo nel primo semestre 2018. Si stima infatti che circa il 50% degli utenti Internet riceva almeno una mail di phishing al giorno e di questi, circa il 25% di questi ci cade compromettendo la sicurezza del proprio terminale o dei sistemi aziendali ai quali accede.

Parlando dell'Italia, lo scorso anno oltre 16 milioni di utenti della rete, più di un terzo della popolazione adulta (37%), sono stati colpiti da attacchi informatici. I danni si attestano a quasi 3,5 miliardi di euro e a più di 2 giorni lavorativi in media per utente occupati a rimediare ai problemi generati.
La principale ragione del successo di tali attacchi è legata alla poca consapevolezza degli utenti (si stima che circa il 97% degli utenti di Internet non sappia riconoscere una mail di phishing), ma va anche osservato che gli attacchi di phishing diventano sempre più sofisticati in quanto utilizzano tecniche di social engineering sempre più evolute.
A titolo esemplificativo, i dati relativi ad una campagna di phishing e spear phishing effettuata da un'azienda per misurare il livello di consapevolezza dei propri dipendenti, mostrano come effettuando dei phishing mirati (Spear Phishing), ma soprattutto modificando l'oggetto del phishing, il numero di vittime e di credenziali rubate aumenti in maniera significativa.



Tale dato è confermato da una ricerca svolta negli Stati Uniti nel 2018 da Osterman Research[1] su circa 134 aziende che hanno evidenziato come gli attacchi di Phishing e Spear Phishing sono aumentati nell'ultimo anno per quasi la metà degli intervistati.



Questi dati evidenziamo alcuni fattori rilevanti:

- il primo è che, nonostante gli investimenti che le aziende fanno in misure di anti-phishing e anti-spearphishing per i loro sistemi di posta elettronica, i nuovi attacchi sono sempre maggiori e più sofisticati e sono in grado di aggirare le difese messe in campo vanificando, di fatto, gli investimenti fatti;
- i programmi di security awareness per i dipendenti sono ancora carenti, se non assenti, e

[1] https://www.ostermanresearch.com

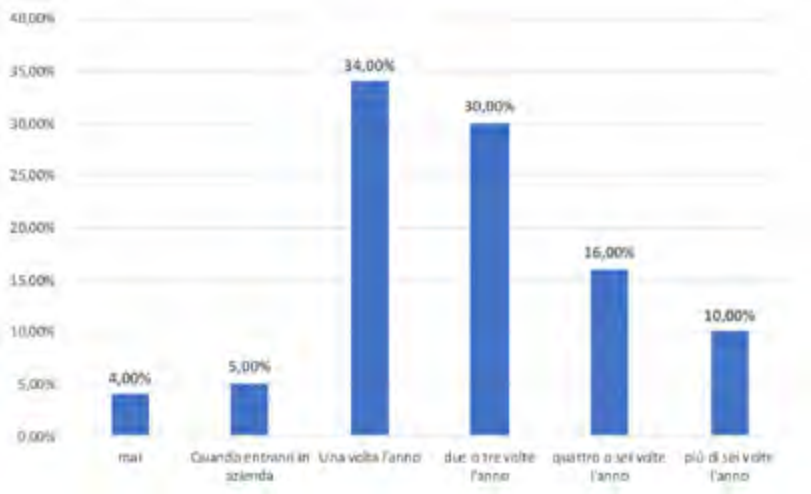
tutta la sicurezza delle infrastrutture delle aziende è basata sulle soluzioni tecnologiche messe in campo;
- la "vita social" delle persone è notevolmente aumentata e vi è l'abitudine, da parte di queste, di condividere su siti facilmente aggredibili dai cyber criminali, informazioni aziendali quali, ad esempio, gli indirizzi di posta elettronica.

Va infine notato che gli attacchi di phishing sono il preambolo di attacchi molto più ampi ed impattanti e non sempre si è in grado di comprendere l'effetto che esso avrà fintanto che questo non si verifica. Il classico esempio è in ambito pagamenti elettronici dove il furto delle credenziali di accesso al proprio sistema di home banking o della carta di credito può avvenire molto tempo prima che venga effettuata la frode.

I programmi di Security Awareness

Dai dati mostrati, si evidenzia chiaramente come la programmazione ed esecuzione di programmi di awareness è diventata una necessità per tutte le aziende non più rimandabile.
L'importanza e l'urgenza di tali programmi e la necessità di sensibilizzare le persone sulla sicurezza informatica è una tematica molto chiara agli operatori del settore e alle istituzioni che promuovono sempre più iniziative di sensibilizzazione in tale ambito (si pensi al mese europeo della sicurezza informatica), ma lo stesso non si può dire per le aziende dove l'awareness sulla sicurezza informatica è ancora ad uno stato embrionale.
Qualche segnale positivo comunque non manca. Nell'ultimo anno, gli investimenti in Security Awareness sono aumentati del 56% soprattutto a causa dell'entrata in vigore di normative europee quali il GDPR e la NIS, ma va anche osservato che la Security Awareness rappresenta ancora una quota marginale degli investimenti in ambito sicurezza informatica.
Paradossalmente, manca la "cultura" della security awareness che molto spesso viene intesa come "formazione" e non come un vero percorso culturale che sia in grado di modificare profondamente i comportamenti delle persone quando navigano in Internet o utilizzano i sistemi aziendali.
Gli attuali Programmi di Security Awareness, quando sono presenti, si basano prevalentemente su modalità di formazione classica (sessioni formative in aula, corsi on line, newsletters, etc) che vengono percepite dai loro fruitori come degli "obblighi aziendali" non attirando così la loro attenzione e interesse per attivare il percorso di cambiamento richiesto.
Questi interventi sono assolutamente necessari per poter aumentare il bagaglio di conoscenza sulla sicurezza informatica nei propri dipendenti, ma non sono sufficienti se non si aumenta la loro efficacia in termini sia di erogazione che di contenuti. Uno degli errori più comuni che si commette in tale ambito è quello di avere una erogazione di tali sessioni formative piatta senza considerare le peculiarità della popolazione cui sono dirette quali l'estrazione culturale, l'età e, soprattutto, il loro ruolo in azienda.
Molte aziende stanno iniziando ad utilizzare tecniche di simulazione di Phishing e Spear Phishing per misurare il livello di awareness dei propri dipendenti, ma molto spesso a queste attività non seguono dei programmi di awareness mirati.

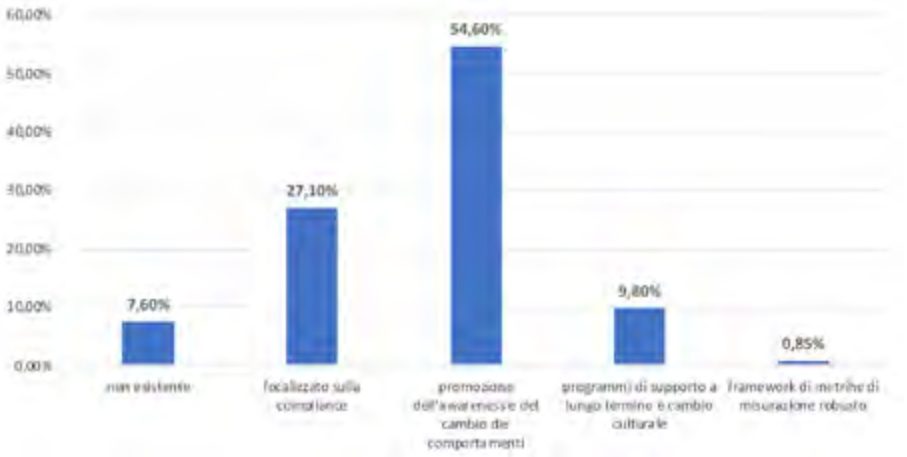
Altro aspetto rilevante in tale ambito è la frequenza di erogazione di tali attività.
Dalla ricerca di Osterman Research citata precedentemente emerge che circa il 64% delle aziende esegue iniziative di security awareness una/due/tre volte l'anno.



Tale frequenza è completamente inadeguata se si considera che rendere una persona "consapevole" sulle tematiche di sicurezza informatica modificando in maniera adeguata i suoi comportamenti è un percorso lungo che richiede circa un anno di interventi formativi.

Altro aspetto rilevante è l'obiettivo con cui vengono elaborati gli attuali programmi di Security Awareness.
Da un ricerca a livello mondiale effettuata nel 2017 dal SANS Institute[2] per misurare il livello di maturità dei programmi di Security Awareness delle aziende, emerge che, anche se circa il 54% delle aziende sta promuovendo programmi di security awareness mirati alla modifica dei comportamenti delle persone, esiste ancora una quota di circa il 35% di aziende che o non ha adottato programmi di security awareness oppure si limita al minimo richiesto dalle normative applicabili al proprio settore.

[2] https://www.sans.org



Dalla ricerca emergono altri aspetti rilevanti:

- gli attuali programmi di security awareness, anche se considerati sufficientemente efficaci, non sono accompagnati da programmi a lungo termine e non hanno definito un framework di indicatori che sia in grado di misurare e monitorare l'efficacia dei programmi stessi;
- le persone impiegate nei programmi di security awareness sono insufficienti sia per il tempo impiegato (generalmente lavorano part-time sul programma) che per numero (si stima circa 1,5 FTE[3]). La stima è che debbono almeno raddoppiare nei prossimi anni.
- Il supporto del management ai programmi di security awareness non è sempre adeguato ed è direttamente proporzionale alla maturità del programma sviluppato. Gli intervistati hanno infatti dichiarato un supporto del management insufficiente intorno al 60-50% per i primi due livelli di maturità che decresce in maniera significativa (25%, 17% e 0%) per i tre successivi livelli.

La Security Awareness domani: scenari evolutivi e best practice

I dati illustrati nei paragrafi precedenti mostrano una situazione sulla security awareness alquanto variegata. Se da una parte si nota una maggiore sensibilizzazione delle aziende sull'importanza della tematica, dovuta soprattutto all'incremento esponenziale degli attacchi che subiscono, dall'altra si evidenzia una certa incertezza su come muoversi in tale ambito, dovuta sia ad una "carenza culturale" sulla tematica che ad una non immediata visibilità da parte del management dei benefici che un programma di security awareness induce in azienda.

[3] Full Time Equivalent

Un driver evolutivo molto importante in tale ambito è sicuramente legato alle Istituzioni le quali, attraverso le iniziative di promozione della security awareness, e soprattutto l'emissione di normative che la rendono obbligatoria, inducono le aziende ad affrontare la tematica e a sviluppare programmi di security awareness aziendale.

A titolo esemplificativo, l'entrata in vigore del GDPR ha prodotto un forte aumento degli investimenti sulla sicurezza, ma ha anche aumentato la sensibilizzazione delle aziende su alcune tematiche critiche (vedi i Data Breach) dove la Normativa ha introdotto obblighi stringenti e multe molto salate. Il management delle aziende sta iniziando a comprendere che per evitare i data breach non basta acquisire solo soluzioni di sicurezza tecniche (tra l'altro necessarie), ma deve anche agire sui propri dipendenti e, paradossalmente, la paura di una multa da parte dell'Autorità potrebbe giustificare l'investimento nella security awareness.

Altro aspetto rilevante è la ri-focalizzazione dei programmi di security awareness su tutti i principali componenti: contenuti, modalità di erogazione, durata e framework di misurazione.
Le aziende devono interiorizzare il concetto che un programma di security awareness è un percorso che deve essere intrapreso da tutti gli stakeholders dell'azienda (Management, dipendenti, terze parti, clienti) con forme adeguate al segmento di persone cui è diretto. Per tale ragione, i programmi di security awareness devono uscire dalla semplice "formazione" e devono adottare forme di erogazione più efficaci e personalizzate alle peculiarità demografiche, culturali e lavorative dei diversi segmenti che compongono la popolazione aziendale.
I benefici attesi non saranno immediati, ma, attraverso una misurazione puntuale degli effetti prodotti, sarà possibile effettuare una continua taratura del programma aumentando e mantenendo nel continuo la sua efficacia.

Il management aziendale deve dare un supporto adeguato e deve comprendere che la security awareness non è una tematica confinata all'ambito tecnico, ma è una trasformazione culturale che impatta su tutta l'azienda. Per tale ragione, uno dei principali obiettivi di un programma di awareness è proprio la sensibilizzazione del Management aziendale, che deve fornire le necessarie risorse al programma. Un ottimo strumento di sensibilizzazione del Management può essere la rappresentazione e condivisione dei benefici che il programma induce (vedi il Return of Security Investment) convincendo quindi il Management sull'efficacia ed utilità del programma di security awareness messo in campo.

La sicurezza delle imprese è fatta di persone competenti e consapevoli

Un manifesto per la competenza digitale e la consapevolezza in materia di sicurezza online con focus sulla Generazione Z

[A cura di Ettore Guarnaccia]

L'onda della trasformazione digitale sta investendo e trasformando profondamente le imprese. Esse richiamano o sviluppano al loro interno nuove professionalità basate su competenze tecnologiche (sviluppo e semantica web, comunicazione digitale, robotica, cyber security, ethical hacking, intelligenza artificiale, realtà aumentata) e soft skill (pensiero computazionale, creatività, autonomia, capacità comunicativa, problem solving, lavoro in team, capacità di pianificare e organizzare, conseguimento di obiettivi e resistenza allo stress). L'esigenza di abilità digitali è in continua crescita non solo nei ruoli informatici, ma in tutte le aree aziendali: business management, marketing e vendite in testa. Il fenomeno è particolarmente evidente per l'industria 4.0, rivoluzione diretta alla produzione automatizzata e interconnessa, basata su robotica avanzata, realtà aumentata, simulazione virtuale, cloud computing, big data analytics e IoT.

La cyber security, in particolare, sta assumendo un ruolo di rilievo agli occhi del business e del top management, grazie al recente proliferare di notizie di cronaca su data breach, infezioni da malware e danni alla reputazione aziendale di tante aziende. Il processo di trasformazione digitale, infatti, è diretto a realizzare prodotti e servizi digitali innovativi, accattivanti, semplici da usare, ma anche resilienti, scalabili, sicuri, in grado di garantire un'adeguata protezione dei dati e la conformità con leggi e regolamentazioni.

La sfida che ne deriva è soddisfare la domanda che questi fenomeni stanno generando: secondo l'Unione Europea, entro il 2020 si registrerà un deficit di 825mila risorse con competenze digitali, avremo 500mila posti ICT vacanti e ben 9 lavori su 10 richiederanno abilità digitali. Eppure solo un lavoratore su tre oggi dispone di preparazione adeguata e due aziende su tre lamentano scarsa competenza interna. Non è più solo un problema di reperire specialisti ICT, bensì di rispondere alla più vasta domanda di abilità digitali, oltre che per sviluppare o gestire sistemi, per servirsene con efficacia e sicurezza per comunicare, vendere, produrre e amministrare.

Ma un problema merita la nostra attenzione: la nuova generazione di futuri cittadini e lavoratori non dispone delle competenze digitali richieste. Secondo il rapporto AICA pubblicato dalla ECDL[1], solo il 15% della popolazione studentesca è esperta di tecnologie e il 45% dimostra conoscenze piuttosto rudimentali, solo il 7% dei giovani tra i 15 e i 29 anni dimostra capacità digitali di livello adeguato, mentre secondo una ricerca ICILS (3) il 25% degli studenti europei ha un basso livello di competenza digitale.

[1] Il falso mito del "nativo digitale": perché i ragazzi hanno bisogno di sviluppare le proprie competenze digitali – AICA, Associazione Italiana per l'Informatica e il Calcolo Automatico - http://ecdl.org/media/position_paper_italian.pdf

Il rapporto "Orizzonte Europa 2014" della Commissione Europea[2] evidenzia che il livello di competenza digitale di bambini e adolescenti europei resta insufficiente, in particolare per quanto riguarda l'**alfabetizzazione informatica critica e partecipativa**: gli studenti non sanno leggere i contenuti, relazionarsi con essi o adottare una propria reazione critica o creativa.

Se la situazione generale è preoccupante, nelle classifiche dell'UE in materia di digitalizzazione e competenza digitale l'Italia è ancora in coda[3]. La ricerca "Il futuro è oggi: sei pronto?" svolta da University2Business nel biennio 2015-2017[4] rileva che le competenze digitali sono considerate importanti dai due terzi degli studenti universitari italiani, ma la maggioranza di essi (53%) è ferma a una conoscenza di base, da semplice utilizzatore di Internet e dei social media (60% delle femmine e 45% dei maschi). Anche gli esiti delle prove di lettura in digitale pubblicate dal MIUR[5] evidenziano che solo un quarto degli studenti italiani consulta il web in modo orientato e critico, con oltre un terzo appena o per nulla in grado di gestire le proprie competenze, mentre emerge chiaramente la necessità di integrare le tecnologie digitali nella didattica e sperimentare nuove metodologie nella pratica pedagogica quotidiana. E nessuno pare accennare agli aspetti di sicurezza tecnologici, di processo e relativi al comportamento umano.

I grandi e rapidi cambiamenti di una società ipertecnologica e iperconnessa creano molte opportunità nel mondo del lavoro e dei mercati globali, ma è indispensabile essere in grado di comprenderle e sfruttarle, ecco perché è importante che le nuove generazioni di cittadini e lavoratori siano dotate degli strumenti cognitivi per cavalcare l'onda della trasformazione digitale mondiale. Il World Economic Forum ha stilato una lista delle abilità[6] necessarie ai giovani studenti di oggi e di domani, suddividendole in otto aree differenti, ma interconnesse:

- **Identità digitale**: capacità di gestire identità, reputazione, presenza online e possibili impatti.
- **Uso del digitale**: capacità di usare i dispositivi digitali con un salutare bilanciamento fra vita reale e virtuale.
- **Incolumità digitale**: capacità di riconoscere, evitare, limitare e gestire i rischi online e l'accesso a contenuti turbativi.

---

2 "Horizon Report Europe - 2014 Schools Edition" – EU Science Hub – The European Commission's science and knowledge service - https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/horizon-report-europe-2014-schools-edition

3 The Digital Economy and Society Index (DESI) 2018 - https://ec.europa.eu/digital-single-market/desi

4 Ricerca "Il futuro è oggi: sei pronto?" di University2Business svolta su un campione di studenti universitari (circa 2.600 nel 2015 e 4.000 nel 2017) e di responsabili delle risorse umane (168 nel 2015 e 250 nel 2017) in merito alle competenze digitali e imprenditoriali degli studenti universitari italiani. (http://www.ilfuturoeoggi.it/la_ricerca.php)

5 "Studenti, computer e apprendimento: dati e riflessioni – Uno sguardo agli esiti delle prove in Lettura in Digitale dell'indagine OCSE PISA 2012 e alla situazione in Italia" – Ministero dell'Istruzione, dell'Università e della Ricerca. (http://www.istruzione.it/alle-gati/2016/MIUR_2015-Studenti-computer-e-apprendimento.pdf)

6 8 digital skills we must teach our children – World Economic Forum https://www.weforum.org/agenda/2016/06/8-digital-skills-we-must-teach-our-children/

- **Sicurezza digitale**: capacità di rilevare minacce informatiche (es. attacchi, truffe e malware), comprendere e adottare best practice e strumenti di protezione.
- **Intelligenza emotiva digitale**: capacità di essere empatici e costruire proficue relazioni online.
- **Comunicazione digitale**: capacità di comunicare e collaborare con gli altri utilizzando le tecnologie e i media digitali.
- **Letteratura digitale**: pensiero computazionale e capacità di cercare, trovare, valutare, utilizzare, condividere e generare contenuti.
- **Diritti digitali**: capacità di comprendere e difendere i diritti personali e legali, inclusi privacy, proprietà intellettuale e libertà di espressione.

Un necessario quanto apprezzabile sforzo tassonomico degli obiettivi, cui le nuove generazioni, tuttavia, non paiono rispondere in modo adeguato. Ci riferiamo alla Generazione Z, quella dei nativi digitali che inizia dagli ultimi anni del precedente millennio, nati e cresciuti in una società ipertecnologica e iperconnessa, che iniziano ad affacciarsi al mondo del lavoro: non hanno mai visto un mondo senza Internet, smartphone e social media, sono immersi in una continua innovazione tecnologica e costituiscono una vera rivoluzione in fatto di comportamenti e apprendimento. Considerati erroneamente dalla società grandi esperti di tecnologie, in realtà dimostrano una grave carenza in termini di competenza tecnologica e di abilità digitali.
Non hanno vissuto la nascita e i vari stadi di sviluppo di Internet e delle tecnologie digitali nel tempo, non hanno modo di aprire e smontare i dispositivi come si poteva in passato, pagando così il presso delle tecnologie integrate e portabili *always on*: l'esperienza del prima e del dopo, del fai da te. La disinvoltura di utilizzo che hanno acquisito nel rapporto continuativo con la tecnologia è qualcosa di notevolmente diverso dalla reale competenza, che presuppone una comprensione ben più profonda.
Un'insegnante[7] ha avuto l'idea di mettere alla prova le competenze informatiche dei nativi digitali prendendo in esame il quadro delle competenze digitali di Europass[8]: ha scoperto che un numero molto ristretto di giovani può rispondere alla descrizione dell'utente autonomo o, più spesso, dell'utente base. Molto scarse le competenze di strutturazione e editing di testi, così come le abilità digitali tradizionali e fondamentali. I testi prodotti sono spesso affetti da errori di formattazione, spazi duplicati, allineamenti maldestri, utilizzo incerto dei font, incapacità di creare una semplice casella di testo, inserire un grafico o costruire una tabella. Non conoscono gli strumenti di presentazione o i fogli di calcolo, non conoscono le potenzialità dei motori di ricerca né l'uso corretto della posta elettronica o le regole basilari

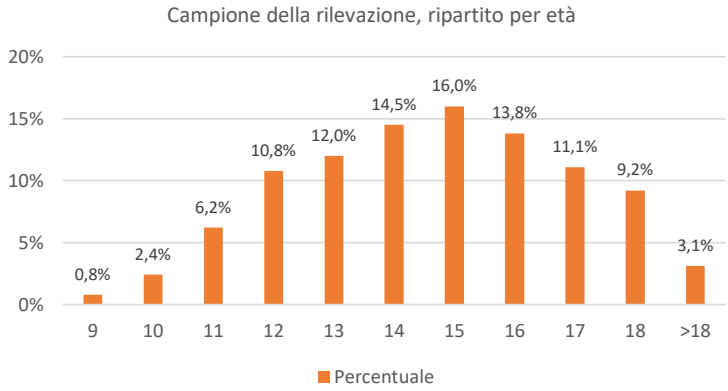
[7] Articolo "Nativi e analfabeti digitali: il paradosso della Generazione Goole" di Anna Rita Longo – Scientificast (2017) https://www.scientificast.it/2017/11/02/nativi-analfabeti-digitali-paradosso-della-generazione-google/

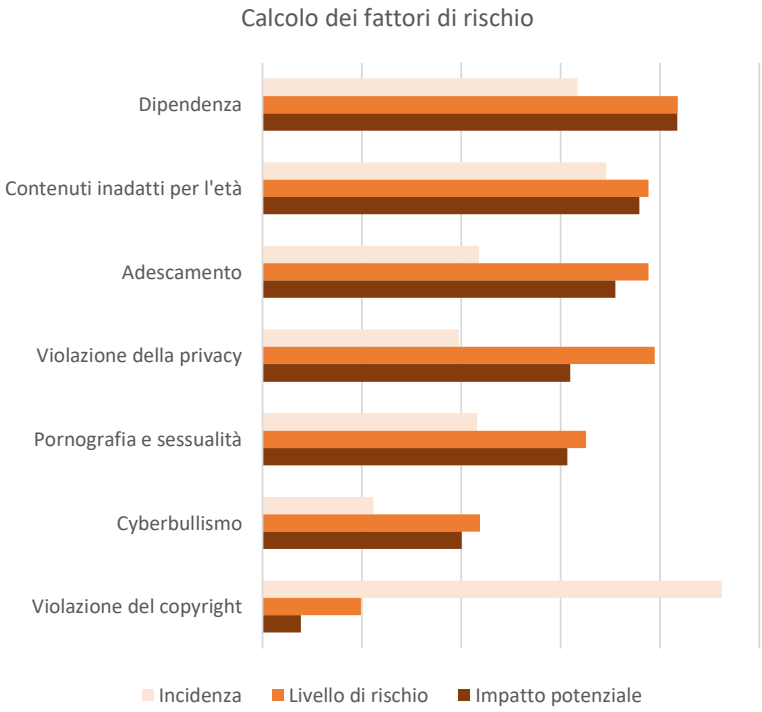
[8] Europass è costituito da cinque documenti destinati ad aiutare i cittadini europei a identificare chiaramente e facilmente le proprie competenze e qualifiche in Europa. Fra que-sti è incluso il quadro delle competenze digitali: https://europass.cedefop.europa.eu/it/resour-ces/digital-competences

di comunicazione formale/informale e l'utilizzo dei campi standard. La disinvoltura e l'agilità con cui mulinellano i pollici sui display di smartphone e tablet non trova analoga corrispondenza quando sono alle prese con una tastiera, sia essa fisica o virtuale, dimostrandosi visibilmente impacciati e usando spesso solo i due indici per scrivere.
La lacuna più grave riguarda la sicurezza, comprovata dall'incauta e disinvolta pubblicazione di dati sensibili e informazioni personali sul web, dall'ignoranza dei protocolli di sicurezza e dei sistemi di protezione, dall'uso di password spesso banali e riutilizzate su più account, uniti all'ingenuità di fondo nell'uso dei servizi digitali che li espone al rischio di subire violazioni informatiche, truffe di vario genere, molestie, tentativi di adescamento e danni irreparabili sul piano dell'immagine personale e dell'autostima. Il concetto di "nativo digitale" genera negli adulti, specialmente genitori e insegnanti e quindi, perché no, nei *recruiter senior*, un'errata percezione delle competenze. Questo, almeno nel prossimo futuro, non deve continuare a tradursi nella rinuncia o nell'omissione di insegnamenti e programmi scolastici indirizzati allo sviluppo delle competenze digitali, soprattutto in materia di valutazione di minacce e rischi, nonché di prevenzione e sicurezza in generale. In estrema sintesi, gli appartenenti alla Generazione Z, eccezionali utenti ma senza una reale competenza tecnologica, sono potenzialmente un mix estremamente pericoloso.
Per sé stessi e per il mondo delle imprese.

Competenza, rischi e minacce: il profilo della Generazione Z in un'indagine sulla consapevolezza digitale

Da professionista della cyber security, genitore e formatore volontario nelle scuole, ho allestito un questionario di 100 domande su aspetti qualitativi, comportamentali ed emozionali che non ho trovato nelle tante ricerche reperite sul tema, e l'ho somministrato online e presso 15 istituti scolastici a un campione di oltre duemila bambini e ragazzi di età compresa fra 9 e oltre 18 anni (dalla quarta elementare alla quinta superiore).





L'ho fatto perché nutrivo molti dubbi sul livello di consapevolezza della nuova generazione e sugli effetti che questo avrebbe potuto avere sulla loro vita. Ne ho fatto un libro, autoprodotto, che tratta oltre 40 argomenti fra tendenze, minacce e rischi, ed è arricchito dalla rappresentazione dei dati raccolti (oltre 500 grafici per età, classe e sesso), da oltre 200 studi e ricerche di terze parti e dall'esperienza di professionisti psicologi, tecnologi ed esperti di comunicazione.

L'indagine conferma la scarsa competenza digitale della nuova generazione: meno di un rispondente su dieci è in grado di descrivere correttamente cos'è Internet, mentre la maggior parte confonde concetti di base che dovrebbero essere ormai assodati da tempo. La predisposizione dei giovani a **concedere l'amicizia a perfetti sconosciuti** (oltre uno su due) o a persone conosciute esclusivamente online (quasi due su tre) è molto diffusa. Un rispondente su tre concede l'amicizia a perfetti sconosciuti senza alcun problema, sulla base del solo aspetto fisico o dell'interesse suscitato dal richiedente, mentre un terzo la concede se il richiedente ha amicizie in comune o appare come un coetaneo (vedi falsi profili e furti d'identità). La maggioranza dei giovani **pubblica informazioni e contenuti visivi riguar-**

danti la propria sfera privata, senza preoccuparsi delle possibili conseguenze in termini di immagine personale o possibile utilizzo di questi dati da parte di malintenzionati. Anche **la capacità di bilanciare in maniera salutare la vita virtuale con quella reale è un serio problema**: uno su due ammette di andare a letto tardi e di dormire troppo poco pur di continuare a usare i dispositivi digitali, uno su quattro rinuncia a studiare, uno su quattro fatica a concentrarsi su un particolare compito, uno su cinque dichiara di dormire male e di sentirsi stanco, mentre in alcuni casi si arriva a rovinare relazioni, ad alimentarsi in maniera scorretta o a rinunciare all'igiene personale. Uno su tre ammette di continuare a chattare a notte inoltrata (fenomeno del vamping), uno su quattro già a 9 anni.
Insufficiente qualità del sonno e della vita, difficoltà di concentrazione e complicazione delle relazioni sono chiari indicatori della dipendenza diffusa che affligge la nuova generazione (e con gradi differenti anche le precedenti), anche a causa della natura particolarmente attrattiva e assuefacente delle moderne tecnologie digitali: basti pensare al like di Facebook, alle notifiche, alle stories e a tutti gli altri stratagemmi che sfruttano i meccanismi neurologici della gratificazione e della ricompensa variabile. **Questa dipendenza diffusa comporta un aumento della sedentarietà e dei difetti visivi**. Sono in pochi coloro che passano almeno 2-3 ore all'aria aperta e alla luce naturale come raccomandato da diversi studi internazionali, mentre uno su tre in media è affetto da difetti visivi, in particolare la miopia, con una preoccupante incidenza di uno su due già a 17 anni e un trend in forte aumento. Il discorso riguarda anche i videogiochi, con un rispondente su cinque che gioca quotidianamente dalle 2 ore in su, addirittura uno su due che viene lasciato dai genitori a giocare senza supervisione fino al raggiungimento della propria soglia di tolleranza, e uno su cinque **cade in preda alla rabbia** se è costretto a interrompere il gioco o gli viene impedito di giocare. **Sintomi di astinenza dal gioco digitale** sono osservabili su un soggetto su tre nella fascia 9-14 anni, soprattutto alle età più basse, mentre si nota anche una **diffusa incapacità a inventare forme di gioco alternative non digitali** (uno su tre prova noia senza smartphone o videogiochi).

Inoltre sono in **pochi coloro che dimostrano la capacità di riconoscere le principali minacce online**: l'uso di social ad accesso anonimo è molto diffuso sebbene sia alla base di storie drammatiche di suicidio adolescenziale, l'uso di **videochat esplicitamente a sfondo sessuale** (uno su cinque a 10-14 anni) può comportare seri turbamenti della sfera sessuale, l'**emulazione di fenomeni e ideologie pericolosi** (online challenge, selfie e video estremi, videogiochi violenti, anoressia, bulimia, autolesionismo e tendenza al suicidio) può portare a danni permanenti o alla morte, i tentativi di **adescamento online** sono frequenti (uno su quattro riceve proposte da sconosciuti, uno su dieci con una certa frequenza, uno su sei è stato vittima di tentativi di coercizione da parte di malintenzionati), mentre la pericolosissima pratica del **sexting** (in media uno su sei, uno su quattro a 16 anni) può condurre a ricatti, estorsioni, seri danni all'immagine personale e, nei casi più gravi, al suicidio. **Purtroppo il processo di accrescimento delle loro abilità digitali non è supportato né dall'ambiente famigliare né dal sistema educativo scolastico.**

Molti genitori sono tagliati fuori dal mondo digitale dei loro figli e non hanno la capacità di riconoscerne i fattori di rischio, di conseguenza non possono trasmettere loro con efficacia i migliori strumenti cognitivi necessari a prevenire e gestire situazioni pericolose e incidenti di percorso. L'uso di strumenti di controllo parentale riguarda un'esigua minoranza degli intervistati ed è limitato alle fasce d'età più basse (fino ai 12 anni), anzi la maggior parte dei figli (due su tre già a 9 anni, la quasi totalità dai 13 anni in su) afferma di avere completa autonomia di utilizzo dei dispositivi digitali senza alcuna supervisione dei genitori. I genitori di oltre un rispondente su due non sanno cosa fanno i figli online, mentre sono spesso loro stessi a pubblicare contenuti sui propri figli (sharenting), tanto che due terzi dei nuovi nati finiscono online nel giro di un'ora dalla nascita e un minore su quattro afferma che i suoi genitori hanno pubblicato immagini che lo ritraggono in costume da bagno o intimo (con il rischio che vengano riutilizzate in circuiti di pedofilia). Nella maggior parte dei casi sono i genitori a spingere i figli ad aprire account social prima dei 13 anni, età minima richiesta dalla maggior parte delle piattaforme.

Al tempo stesso, il sistema educativo scolastico si rivela incapace di sviluppare la competenza digitale corredata dalla necessaria consapevolezza. Uno studente delle elementari su due non ha mai partecipato a incontri educativi o di sensibilizzazione (quasi sempre sporadici e tenuti su base volontaria), uno su quattro alle medie e uno su sei alle superiori. Il sistema educativo non ha ancora recepito né i cambiamenti generazionali né quelli tecnologici, restando ancorato a criteri e metodi non più attuali, di fatto inadatti a garantire un apprendimento efficace e stimolante per le nuove generazioni. Quasi due docenti su tre sono ultracinquantenni a fronte di una media europea di uno su tre e l'innalzamento dell'età pensionistica aggrava ulteriormente il problema. Il mercato del lavoro è fatto di innovazione, digitalizzazione, social, immediatezza, comunicazione, creatività, tutti aspetti che la scuola non comprende nella propria offerta formativa. L'impegno di molti istituti scolastici nell'organizzare incontri educativi sulle opportunità e i rischi online è indice di un generale aumento della percezione sull'importanza delle competenze digitali: **se oggi il cyberbullismo è uno dei fattori di rischio con più bassa incidenza fra i minorenni è grazie al fatto che si è investito molto sul dibattito mediatico e sull'educazione nelle scuole** (nove minori su dieci hanno partecipato a incontri sul bullismo e otto su dieci sul cyberbullismo a scuola) negli ultimi anni. Insomma, dove si è investito, i risultati si sono chiaramente visti. **Purtroppo si parla ancora troppo poco di fattori di rischio ben più pericolosi e diffusi come la dipendenza, la pedofilia, l'adescamento e il sexting.**
Il trasferimento di competenze, educazione e sensibilizzazione in materia non può ridursi alla buona volontà di quei pochi dirigenti e insegnanti che ne hanno compreso l'importanza e scelgono di impegnarsi in prima persona per garantirlo ai loro alunni, spesso superando ostacoli burocratici e la resistenza interna del sistema. È urgente definire un programma strutturato di iniziative educative che parta dal MIUR e coinvolga **attivamente gli esperti in materia**. C'è ancora molto da fare, siamo in ritardo di almeno un decennio e c'è il rischio

che questa generazione sia condannata a esaurire il proprio percorso scolastico senza le competenze digitali necessarie a proteggersi dai rischi online e a rispondere adeguatamente alla domanda delle aziende quando accederanno al mondo del lavoro.
La Generazione Z è abituata all'estrema sintesi delle comunicazioni (vedi WhatsApp e Instagram), al fatto che c'è sempre un filtro per mostrare il proprio lato migliore, ma denota la forte diminuzione del livello di attenzione e la ricerca delle gratificazioni immediate. L'*hic et nunc* che sperimentano con il digitale fin dalla nascita, la tendenza a dormire poco e male, l'incapacità di curare la propria reputazione digitale impediranno a molti di soddisfare le aspettative delle aziende che ricercano competenza, abilità digitali e soft skill per supportare i loro processi di trasformazione digitale, garantendo la salvaguardia del business, la protezione dei dati e la sostenibilità per il consumatore. È indispensabile agire subito con una strategia ben precisa a livello nazionale, trovando il coraggio di cambiare e innovare non solo nell'ambito aziendale, ma soprattutto in quello famigliare e scolastico (magari con il supporto delle aziende stesse), per creare una classe di cittadini e lavoratori competenti, consapevoli e in possesso dei migliori principi in materia di etica, rispetto, regole di convivenza, responsabilità e sicurezza, per disegnare e realizzare la società del futuro.

È **urgente sviluppare un piano strutturato di introduzione di una nuova disciplina nel sistema educativo scolastico: l'Educazione Digitale!**
Facciamo in modo che essa fornisca le basi culturali minime per usare in maniera proficua, responsabile, rispettosa e sicura le moderne tecnologie digitali. Nel frattempo abbiamo forgiato una generazione eccezionalmente capace di interagire con la tecnologia, ma pericolosamente all'oscuro della sua vera natura, dei meccanismi e dei risvolti potenzialmente dannosi, mentre l'evoluzione tecnologica ha generato dispositivi sempre più *smart* che hanno reso gli utenti pericolosamente *dummy*
Di questo e molto altro parlo nel mio libro "**Generazione Z – Fotografia statistica e fenomenologica di una generazione ipertecnologica e iperconnessa**" pubblicato a ottobre 2018 e disponibile su Amazon. Il mio più sentito ringraziamento a Gigi Tagliapietra, presidente onorario del Clusit, e a Federica Boniolo, presidente di #UnitiinRete, per le preziose prefazioni, a Gregorio Ceccone, Garibaldi Conte, Guido D'Acuti, Davide Dal Maso, Andrea Micheletti e Claudio Simoni per aver arricchito il testo con la lettura dei risultati dell'indagine alla luce della loro preparazione ed esperienza sul campo, a Achab S.r.l., socio Clusit dal 2018, per aver creduto nel progetto e finanziato la produzione e la distribuzione della prima tiratura cartacea con cui è stato possibile diffondere consapevolezza nel pubblico, e infine alle associazioni Rete Progetti, #UnitiinRete e Clusit per l'impegno a fare rete insieme per promuovere la cultura in materia di sicurezza online.

Il panorama delle startup italiane nel settore cybersecurity e legal-tech

Stato dell'arte e valutazioni sul trend evolutivo

[A cura di Giuseppe Vaciago]

1. Introduzione

A distanza di quasi un anno dall'entrata in vigore del GDPR e in previsione dell'emanazione del Cybersecurity Act[1], appare quantomeno superfluo fare un bilancio di come le varie società di consulenza informatica o aziendale, gli studi legali, i dottori commercialisti e, curiosamente, alcune società specializzate nella sicurezza e salute sul luogo del lavoro, hanno affrontato questa nuova sfida.

È, invece, necessario comprendere come, a livello nazionale, soprattutto le PMI intendano affrontare, sulla base del principio di *accountability*, il nuovo paradigma di gestione del dato introdotto dal GDPR. Sotto questo profilo, è evidente che servono nuove soluzioni tecnologiche in grado di consentire un approccio rivolto, *by design e by default*, alla privacy, alla cybersecurity e più in generale alla *data governance*.

Per questa ragione, ho ritenuto opportuno analizzare, in modo non esaustivo, se e come il mercato italiano delle startup abbia recepito adeguatamente la nuova e indubitabile opportunità di business sorta dopo l'entrata in vigore del GDPR. La prima impressione è che si sia persa una buona occasione per creare soluzioni integrate in grado di far dialogare in modo armonico ed efficiente il settore IT con la funzione "legal", "compliance" e "internal audit" delle aziende più strutturate. Poche società, infatti, hanno colto tale collegamento sia a livello di comunicazione che di soluzioni software.

Un'altra sfida che, a livello nazionale, si sta rischiando di perdere è quella del settore legal-tech. Negli ultimi anni a livello mondiale il mercato delle legal-tech è cresciuto esponenzialmente. Il totale degli investimenti è stato tra il 2012 e il 2017 di 2,15 miliardi di dollari La sproporzione tra Stati Uniti e resto del mondo è netta: negli Stati Uniti sono stati investiti 2 miliardi di dollari, in Europa 93 milioni di dollari, mentre in Canada 30 milioni. Interessante notare, invece, che nel solo stato di Israele l'investimento è stato pari a 12 milioni[2].

---

[1] Regolamento del Parlamento Europeo e del Consiglio relativo all'ENISA, l'agenzia dell'Unione europea per la cibersicurezza, che abroga il regolamento (UE) n. 526/2013, e relativo alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione. Disponibile al seguente Url: https://eur-lex.europa.eu/resource.html?uri=cellar:0ae19c15-ae6f-11e7-837e-01aa75ed71a1.0018.02/DOC_1&format=PDF.

[2] Deepanshu Gupta, Feed Report Legal Tech, Tracxn Technologies Research, October 2017.

A livello italiano, il settore del legal-tech è ancora praticamente inesistente: ad oggi vi sono solo 13 società iscritte nel registro delle startup innovative della Camera di Commercio, a differenza del Regno Unito dove sono già 59. È, in ogni caso, evidente che il mercato europeo non ha ancora recepito le potenzialità di questi servizi a differenza di quello americano, dove il sistema giuridico (common law) e le maggiori potenzialità economiche del settore legale hanno permesso una crescita più repentina.

Per arrivare ad una prima conclusione, solo una corretta sintesi tra il settore legal-tech e il mondo delle cybersecurity può essere in grado di essere di fornire soluzioni conformi a livello normativo e in linea con gli standard di sicurezza che saranno richiesti dopo l'entrata in vigore del Cybersecurity Act.

2. Cybersecurity startup: il panorama nazionale a confronto con quello internazionale

Dall'analisi svolta a livello nazionale, appare sicuramente interessante notare come, a livello geografico, vi sia una buona concentrazione di cybersecurity startup in Emilia-Romagna e in Lombardia, mentre ve ne siano poche in centro e sud Italia[3].

Inoltre, come anticipato in premessa, poche hanno colto, anche solo a livello di marketing, l'importanza di evidenziare la compliance GDPR come punto di forza del loro prodotto. Alcune di queste realtà hanno correttamente puntato al settore bancario e assicurativo, mentre la maggioranza di esse ha deciso di mantenere un approccio più generalista.

Poche società hanno realizzato soluzioni rivolte al mondo delle applicazioni *mobile* o dell'*IoT*. Tale settore rappresenta un ambito dove nei prossimi anni sarà necessario puntare con maggiore attenzione. Grande attenzione è stata data, come era giusto che fosse, alle minacce che provengono dalla navigazione web, mentre colpisce che non siano ancora molte le società che propongano soluzioni innovative di cifratura, soprattutto se si considera l'attenzione posta dal GDPR a questo tema. Sappiamo bene però quanto sia complesso, soprattutto per una PMI, gestire a livello interno qualsiasi sistema di cifratura.

L'espansione del mercato della cybersecurity è indiscutibile: il mercato globale passerà dai 105 miliardi di dollari di investimento nel 2015 ai 181 miliardi di dollari nel 2021. Se si considera che l'investimento globale nel 2004 era di 4 miliardi di dollari, questa vertiginosa crescita esponenziale del mercato deve necessariamente indurre anche gli investitori italiani a credere seriamente in questo settore[4]. Tuttavia, le molte operazioni fatte sul mercato

[3] Il report di dettaglio delle società analizzate è disponibile al seguente URL: https://bit.ly/2XbHesr.

[4] Fonte: Zion Market Research. La ricerca è disponibile al seguente URL: https://globenewswire.com/news-release/2018/11/09/1649006/0/en/Global-Size-of-Cyber-Security-Market-to-Surge-to-USD-181-77-Billion-in-2021-Zion-Market-Research.html.

nazionale hanno principalmente riguardato investimenti su società di consulenza e non di prodotto a dimostrazione che uno dei limiti principali a livello nazionale rimane quello del coraggio nel "mettere mano al portafoglio" quando il livello di rischio aumenta.

A livello internazionale, il polo di maggiore interesse oltre a quello statunitense è sicuramente quello israeliano. Il primo elemento distintivo rispetto al mercato italiano è, ovviamente, dato dal diverso approccio dei *venture capitalist* fin dai primi *round* di investimento. È evidente che un'idea può vedere la luce solo con investimenti adeguati e alcuni Paesi hanno compreso da tempo quanto sia necessario avere un approccio lungimirante accettando il rischio di perdere capitali ingenti. In secondo luogo, è sicuramente interessante notare come molte delle startup nate in un contesto diverso da quello Europeo, pur non avendo alcun obbligo al riguardo, abbiano promosso soluzioni GDPR compliant: dalla gestione del data breach, a sistemi innovativi di IAM (*Identity access management*, dalla cifratura e da sistemi DLP (*Data Loss Prevention*) fino ad arrivare a società che promuovono *tool* di valutazione del rischio cyber nel contesto aziendale al fine di garantire l'effettuazione di *security assessment* in conformità con il GDPR.

Al netto di queste considerazioni preliminari, i trend principali evidenziati da un'analisi fatta durante lo Startupbootcamp FinTech & CyberSecurity[5] svoltosi recentemente in Amsterdam sono di triplice natura.

In primo luogo, le cybersecurity startup si stanno sempre più indirizzando verso il *machine learning* e, più in generale all'universo AI, attraverso l'introduzione di tecniche di tipo euristico in grado di predire attacchi futuri. In secondo luogo, come naturale conseguenza del *machine learning*, le soluzioni più innovative di cybersecurity si stanno spostando verso il paradigma predittivo e non più verso la tradizionale modalità reattiva. L'idea non è quella della gestione dell'*incident response*, ma di evitare che lo stesso avvenga attraverso sistemi di prevenzione basati anche sulla creazione di sistemi innovativi ed efficaci di *awareness* aziendale. In terzo e ultimo luogo, partendo dal presupposto che il cybercrime non ha confini territoriali, le cybersecurity startup stanno cercando, fin da subito, di proporsi come uno standard globale e non di limitare il loro raggio di azione al mercato nazionale di riferimento.

I settori principalmente interessati sono quello aerospaziale, governativo, finanziario, telecomunicazioni e sanitario. Soprattutto su quest'ultimo settore, la necessità di proporre soluzioni efficaci in termini di sicurezza informatica si fa sempre più pressante considerato l'elevato rischio sia in termini di sicurezza che di privacy nel caso in cui una struttura sanitaria dovesse subire un cyber-attacco.

[5] Per maggiori dettagli si veda il seguente URL: https://www.startupbootcamp.org/accelerator/fintech-cybersecurity-amsterdam/.

Da ultimo vale la pena di evidenziare un ulteriore possibile ostacolo per la crescita delle startup evidenziato da Lenard R. Koschwitz, Senior Director di Allied For Startups (network di advocacy Europeo a favore del mondo delle Startup), il quale ha provocatoriamente affermato che il GDPR non è di aiuto alle startup. Questo, per quanto possa sembrare assurdo, vale in modo particolare per il settore della cybersecurity. I condivisibili principi della *privacy by design* e *by default* sono di difficile applicazione in un futuro sempre più orientato a soluzioni fondate sul *machine learning* e sull'intelligenza artificiale. Il concetto di decisioni automatiche e di profilazione nel mondo della cybersecurity sono di basilare importanza per poter garantire l'efficienza di un sistema, ma una interpretazione troppo letterale del GDPR potrebbe interrompere sul nascere progetti potenzialmente innovativi e in linea con l'art. 32 dello stesso Regolamento Europeo. Ciò non significa che si debba promuovere la disapplicazione del GDPR per le startup, ma sicuramente si devono aiutare tali realtà con delle indicazioni chiari ed efficaci come peraltro previsto dal nuovo articolo 154 bis del D.lgs. 196/2003 (novellato dal D.lgs. 101/2018) che prevede l'arrivo di specifiche linee guida per adeguarsi al GDPR per micro, piccole e medie imprese.

3. Legaltech startup: il panorama nazionale a confronto con quello internazionale

Le società presenti nel mercato legal-tech offrono diversi servizi sia alle imprese che agli studi legali. L'Università di Stanford in California, con il progetto CodeX[6] ha provato a dividerle in nove categorie: 1. *Marketplace* 2. *Document Automation* 3. *Practice Management* 4. *Legal Research* 5. *Legal Education* 6. *Online Dispute Resolution* 7. *E-Discovery* 8. *Analytics* 9. *Compliance*.

Allo stato, a livello nazionale, la gran parte di queste società si occupa di fornire servizi di *document automation* e e-discovery, ma stanno sicuramente crescendo anche quelle che offrono servizi di *compliance*, *analytics* e *legal research*.
È francamente complesso fare un bilancio di un settore che, in Italia, ha appena iniziato ad affacciarsi sul mercato. Sicuramente alcune soluzioni di *document automation* stanno iniziando a diventare degli standard sul mercato nazionale, ma è ancora presto per un'analisi più compiuta. Certamente, come già detto in precedenza, è importante che il mondo legal-tech inizi a dialogare di più con quello cybersecurity al fine di proporre soluzioni GDPR compliant efficaci ed economicamente sostenibili.
Tuttavia, in linea generale, si possono evidenziare tre principali criticità e tre grandi opportunità che questo settore potrebbe avere una volta che avrà preso piede in Italia esattamente come è già avvenuto negli Stati Uniti.

Le criticità sono: (i) la trasparenza dell'algoritmo con cui il software analizza tematiche di natura legale e di *compliance* e il rischio che lo stesso possa incorrere in falsi positivi; (ii) il

[6] CodeX, Stanford Center for Legal Informatics, available at https://law.stanford.edu/codex-the-stanford-center-for-legal-informatics/.

"paradosso di Mida" in forza del quale "Machines take the law literally... Humans don't"[7]. All'interno di un panorama così ampio e complesso di informazioni, è, infatti, possibile che alcuni contenuti legali che necessitano la valutazione di un essere umano possano venire fraintesi da una macchina; (iii) il *digital divide*, in quanto nel contesto europeo e specificamente in quello italiano, il livello di conoscenza dei servizi legal-tech è molto basso e potrebbe generare grande confusione al fruitore del servizio.

Le opportunità sono: (i) l'accesso all'informazione data dalla capacità computazionale raggiunta nella gestione dei *Big Data* e nei sistemi di *machine learning* che permette di fornire al mondo legale una serie di informazioni che solo alcuni anni fa era impensabile avere a disposizione; (ii) la maggiore efficienza nel servizio legale, in quanto i servizi legal-tech, se testati in modo corretto e prudente, possono sicuramente garantire maggiore trasparenza e rapidità nel processo decisionale; (iii) il risparmio di spesa che costituisce una diretta conseguenza della maggiore efficienza del sistema legale.

A livello internazionale, considerati i numeri evidenziati nel primo paragrafo, il panorama è fisiologicamente diverso: sono davvero numerose le soluzioni integrate di *document automation* e di intelligenza artificiale applicate al diritto.

Tuttavia, la prima e più nota società legal-tech statunitense è stata creata nel 2008 ed oggi ha un fatturato di 10 milioni di dollari e 200 dipendenti. Youtube è nata tre anni prima e ha attualmente una previsione di fatturato per il 2018 di 15 miliardi di dollari e supera i 3.000 dipendenti. È, ovviamente, un paragone scorretto e provocatorio, ma ci mostra come il settore Legal Tech non sia ancora un ambito particolarmente remunerativo. Considerato che i primi 10 studi legali americani generano un fatturato globale di 23,28 miliardi di dollari, è indubitabile che ci sia ancora molto da fare[8]. Ciò che forse non si è compreso è che la soluzione tecnologica non deve mai prevalere sul contenuto legale. Se è vero che la norma può essere rappresentata facilmente in un sistema binario, è altresì vero che una soluzione legale necessita di un dato esperienziale non sempre facile da trovare nei dipendenti di una legal-tech. Se però l'avvocato medio statunitense è di 125.000 dollari annui, non è sicuramente facile che tale figura professionale possa trovare spazio in una startup[9].

Inoltre, come già ampiamento osservato, è di fondamentale importanza che il settore del legal tech si accosti a soluzioni integrate di *compliance* e cybersecurity rivolgendosi quindi sempre di più al mercato B2B.

---

7 Sharad Goel, Fairness, Accountability, and Transparency of Algorithms, in CodeX Future Law Conference, April, 2018.

8 Per un approfondimento si veda il seguente URL: https://www.investopedia.com/articles/personal-finance/010715/worlds-top-10-law-firms.asp

9 Per un approfondimento si veda il seguente URL: https://money.usnews.com/careers/best-jobs/lawyer/salary.

4. Conclusioni

In conclusione, la professione legale è sicuramente ad un bivio importante e delicato. I servizi legal-tech e, soprattutto, l'utilizzo dell'intelligenza artificiale non vanno sopravvalutati, ma non devono nemmeno essere ostracizzati. Il percorso da compiere deve necessariamente essere graduale perché la realtà italiana e il contesto europeo scontano un ritardo piuttosto significativo rispetto alle sperimentazioni già effettuate negli Stati Uniti. Pertanto, il primo passaggio fondamentale per avvicinarsi alla professione legale del futuro è quello di trasformare, ove possibile, il servizio legale in un processo organizzato. Una volta proceduralizzato tale servizio sarà possibile comprendere quale parte del processo potrà essere automatizzato e quale dovrà essere di assoluto dominio del professionista.

Per quanto riguarda le startup nate nel mondo della cybersecurity sono molto interessanti le osservazioni fatte da I3P (incubatore del Politecnico di Torino). I3P ha osservato, in 20 anni di esperienza sul campo, che in Italia sopravvive quasi il 90% delle startup. Quasi nessuna, però, diventa grande: una su dieci ha un fatturato superiore ai 500mila euro; ma la media si avvicina a 170mila. Questo dato è in netta controtendenza non solo con le realtà statunitensi, ma anche con quelle europee e denota due caratteristiche proprie del nostro Paese: l'estremo individualismo e l'eccesso di prudenza nella capacità di investimento.
Tuttavia, il mondo delle startup deve avere coraggio se vuole innovare e deve necessariamente accettare il rischio di fallire nel suo progetto. Il fatto di minimizzare il rischio ha come conseguenza positiva la sopravvivenza della stessa realtà che progressivamente finisce per virare dal mondo dell'impresa al magmatico universo della consulenza.

Viviamo, però, in un momento storico, sia dal punto di vista di evoluzione tecnologica che di compliance normativa, dove la rapidità dei cambiamenti impone un cambio di paradigma: dobbiamo realizzare prodotti e soluzioni in grado di aiutare la protezione del dato evitando di pensare che sia sufficiente una buona consulenza che avrà come risultato, nel migliore dei casi, l'indicazione della necessità di adottare quelle soluzioni tecnologiche che il nostro Paese non è in grado di produrre e che, sempre di più, sta importando dall'estero.

L'auspicio è quindi che ci sia la volontà da parte dello Stato, delle grandi imprese nazionali, delle PMI e soprattutto degli startupper di intraprendere questo fondamentale e importante cambio di passo.

La logica del profitto alla base dell'aumento del cryptojacking

[A cura di Liviu Arsene, Bitdefender]

Se tradizionalmente il mining implicava l'uso di GPU (Graphics Processing Unit) e di altre costose attrezzature progettate per sfruttare la loro potenza aggregata di calcolo per generare unità di cripto-valute, verso la fine del 2017 è diventato disponibile un metodo per usare le CPU (Central Processing Unit) basato su JavaScript.

Questa tecnica offriva alcuni importanti vantaggi. Il primo era che il mining non dipendeva più dalle GPU e questo comportava una notevole riduzione dei costi legati all'acquisto di schede grafiche. In secondo luogo le CPU sono decisamente più promettenti dalla prospettiva dei criminali informatici, essendo presenti su tutti i computer, indipendentemente dalla loro potenza, e a differenza di schede grafiche sufficientemente potenti. Di conseguenza, se in passato il mining di cripto-valute richiedeva un significativo investimento in hardware, da ora era sufficiente sfruttare la potenza delle CPU.

Il processo che sfrutta illegalmente le risorse informatiche di una vittima per generare criptovaluta di solito viene chiamato cryptojacking. In sostanza, gli aggressori sottraggono potenza di calcolo installando un'applicazione di mining di criptovaluta sul sistema della vittima, che sia un PC o uno smartphone. La generazione di valuta virtuale, nota anche come criptovaluta, è molto dispendiosa in termini di potenza di elaborazione, motivo per cui gli aggressori devono infettare un vasto numero di vittime e utilizzarne la potenza di calcolo per generare nuove unità monetarie virtuali.

Forse uno dei vantaggi più importanti era che il mining di cripto-valute poteva essere effettuato tramite browser, senza dover installare alcunché nel sistema della vittima. Più tempo un utente avesse passato su un sito web compromesso, più potenza di calcolo avrebbe "ceduto" al mining.
L'uso dei miner di criptovalute come strumento di generazione di introiti per i criminali informatici ha raggiunto il suo massimo picco nella prima metà del 2018, dopo che gli aggressori hanno iniziato a sfruttare uno script web apparentemente innocuo, CoinHive, e a iniettarlo in siti web dal traffico elevato allo scopo di rubare potenza di calcolo agli ignari visitatori. Dalla seconda metà del 2018 il mining di cripto-valute sembra aver preso di mira organizzazioni e infrastrutture cloud di grandi dimensioni, quando i criminali hanno capito di poter agire indisturbati per molto tempo e ottenere al contempo molti più profitti di quanto avrebbero mai potuto dallo sfruttamento di CPU di livello consumer.

Tutto ruota intorno ai soldi

La prassi di scovare vulnerabilità XSS si è consolidata rapidamente, di pari passo alla crescente facilità nell'implementazione di script di mining in seguito a una compromissione. All'inizio del 2018 ci sono stati numerosi rapporti di cryptojacking diretto verso utenti medi, poiché gli aggressori colpivano soprattutto siti web vulnerabili.
Ma nella seconda metà del 2018 i criminali hanno compreso che nonostante violare siti web per sfruttare i miner di cripto-valuta fosse ancora lucrativo, il ritorno di investimento si stava assottigliando, perché per interrompere il mining era sufficiente che gli utenti chiudessero il sito web. Questo limite è stato presto superato spostando gli attacchi verso grandi infrastrutture e ambienti cloud, che offrivano una superiore potenza di calcolo e una maggiore produttività.
Ben presto le organizzazioni sono state prese di mira dagli aggressori, intenzionati a implementare i miner di criptovalute nelle loro infrastrutture. Test, Kubernetes e Jenkins sono solo alcuni dei bersagli di questi attacchi. Sfruttando la potenza del cloud e del provisioning automatizzato, i criminali sono riusciti ad attivare i miner e a ottenere ricavi molto più rapidamente e in modo molto più efficiente di quanto avrebbero fatto sui siti web con maggiore traffico.
L'ulteriore vantaggio di attaccare ambienti cloud è che è possibile regolare il processo di mining in modo da ridurre il consumo di potenza di calcolo, per non insospettire i responsabili IT. Questo tipo di approccio ha di fatto permesso agli aggressori di sfruttare a loro favore le prestazioni e il maggiore tempo di attività del cloud.
In definitiva, il cryptojacking ruota tutto intorno al denaro e più tempo un miner riesce a restare nascosto all'interno di un'infrastruttura, più valuta genera. Perfino sistemi che fanno parte di infrastrutture critiche sono stati colpiti da questo tipo di minaccia. Si è scoperto che una società di fornitura idrica aveva ospitato dei miner nei propri sistemi per mesi.
Non sappiamo ancora quanto stiano fruttando ai criminali gli attacchi diretti a infrastrutture cloud, ma il cryptojacking può danneggiare anche fisicamente un'infrastruttura. Ad esempio, alcune applicazioni Android piene zeppe di malware di mining possono provocare

un notevole consumo della batteria, finendo per danneggiarla. Queste conseguenze fisiche possono estendersi a tipi di hardware diversi dagli smartphone.

L'evoluzione del cryptojacking

Confrontando la trasformazione del cryptojacking rispetto a quella dei ransomware o dei malware fileless, possiamo affermare che si è trattata di una delle evoluzioni più drastiche nel corso del 2018. Se inizialmente i criminali sfruttavano le vulnerabilità XSS dei siti web o plugin vulnerabili per implementare gli script di mining di cripto-valuta, alla fine dell'anno hanno cominciato a usare malware fileless per iniettare i loro payload in infrastrutture di grandi dimensioni e appartenenti a organizzazioni.
Come abbiamo osservato nel nostro precedente rapporto di metà anno sulle minacce informatiche, i primi due mesi del 2018 hanno visto una crescente affermazione dei malware di mining, stabilizzatasi nei mesi successivi. La sempre maggiore complessità del mining di unità di cripto-valute ha spinto i criminali a cercare maggiore potenza di calcolo. E poiché solo le organizzazioni erano in possesso delle infrastrutture necessarie allo scopo, era solo questione di tempo prima che venissero prese di mira.
Gli aggressori hanno usato strumenti di solito associati a minacce persistenti avanzate, spesso accompagnati da tecniche malware fileless per l'attivazione di miner, allo scopo di implementare segretamente i propri cryptojacker e agire indisturbati il più a lungo possibile.
Confrontare l'evoluzione dei rapporti sui malware rispetto al ransomware e ai malware fileless ci permette di avere un quadro più chiaro della situazione e di scoprire che i criminali hanno spostato la loro attenzione dagli utenti comuni alle aziende.
In termini di rapporti, i miner di criptovalute hanno seguito un'interessante curva discendente. Prendere di mira le infrastrutture può rivelarsi estremamente più lucrativo per quanto riguarda il mining, ma il numero di vittime interessate è significativamente minore rispetto a quelle di un sito web ad alto traffico infettato con uno script di cryptojacking.
Questo significa che l'interesse generale a implementare miner di valuta è ancora molto alto tra i criminali informatici, così come a sfruttare i ransomware.

Il modo in cui gli attacchi ransomware e fileless si sono evoluti in Italia appare in linea con le tendenze globali, per entrambe le famiglie di malware. Gli attacchi ransomware sono diminuiti tra luglio e agosto. A novembre, il ransomware aveva raggiunto la minore percentuale rilevata nella seconda metà del 2018.
Anche i malware fileless sono diminuiti in Italia tra luglio e agosto, ma hanno avuto un picco a ottobre. Sappiamo che gli aggressori lanciano le loro campagne malware ciclicamente, concentrandole soprattutto nella stagione invernale rispetto a quella estiva. Ciò può significare che è il periodo in cui si aspettano un maggiore impatto e un ritorno dell'investimento più elevato.
L'utilizzo di miner di valuta è diminuito da luglio a ottobre 2018, una tendenza in linea con le statistiche a livello globale. Questo significa che a partire da luglio i miner si sono costantemente ridotti di mese in mese fino a novembre.

Anche l'evoluzione dei miner di valuta osservata in Italia nella seconda metà del 2018 sembra confermare le tendenze globali. Ad esempio, i ransomware sono costantemente diminuiti ogni mese, hanno avuto un picco a settembre, ma sono di nuovo calati a novembre.

Il cryptojacking è qui per restare

L'uso di malware per aumentare i profitti in cripto-valute degli aggressori continuerà durante il 2019. Questa minaccia è in cima alla lista delle tecniche di attacco più utilizzate a livello globale, soprattutto perché è meno complicata da sfruttare rispetto al ransomware e perché è difficile che le vittime si accorgano che il loro computer è usato per generare soldi per gli aggressori.

Abbiamo già visto tentativi di cryptojacking drive-by attraverso pubblicità malevole che nascondono miner di cripto-valute basati su browser ed è probabile che ne osserveremo altri nel 2019. Tuttavia, poiché il mining di ogni nuova unità richiede sempre più potenza di calcolo, i criminali prenderanno anche di mira le organizzazioni dotate di infrastrutture cloud, nella speranza di ampliare la portata delle loro operazioni. È molto più redditizio sfruttare i vantaggi del provisioning automatico, piuttosto che cercare di ingannare gli utenti domestici convincendoli a visitare siti web compromessi. Uno di questi vantaggi è ad esempio che le infrastrutture cloud rimangono attive per molto più tempo, mentre gli utenti possono semplicemente chiudere il sito web e arrestare così il processo di mining.
Gli utenti finali sono incoraggiati a usare una soluzione di sicurezza in grado di bloccare efficacemente sia siti web che ospitano script di mining di valuta sia applicazioni manomesse che iniettano software di mining. Le organizzazioni devono implementare soluzioni di sicurezza endpoint capaci di rilevare e bloccare sia i software che i siti web compromessi, e che siano dotate anche di un software in grado di garantire le prestazioni di riferimento delle loro infrastrutture. In questo modo i team di sicurezza e IT possono monitorare e individuare qualsiasi comportamento sospetto relativamente al consumo di potenza di calcolo su cloud, solitamente associato a un'infezione di cryptojacking nascosta.
Vale anche la pena notare che sebbene la maggior parte delle organizzazioni trattino le infezioni tramite malware per cripto-valute come benigne, di solito questi attacchi sono associati a potenziali violazioni di dati di più vasta portata. Ad esempio, se qualcosa è riuscito a penetrare nella vostra infrastruttura cloud senza che ve ne siate accorti, gli aggressori potrebbero aver sfruttato quella stessa vulnerabilità o quello stesso accesso per fare molti più danni rispetto al semplice mining di cripto-valute. Una volta rilevata un'infezione di cryptojacking, è importante procedere a un'indagine completa e dettagliata per individuare il punto in origine dell'attacco, valutare i potenziali danni e impedire che altri tipi di minacce colpiscano l'infrastruttura sfruttando la stessa vulnerabilità.
Esistono soluzioni integrate di sicurezza e monitoraggio degli endpoint in grado di offrire alle organizzazioni la visibilità necessaria a proteggere i workload sia fisici che virtuali e di eseguire un'investigazione analitica in seguito a un allarme causato da una potenziale violazione dei dati.

Infrastrutture critiche vulnerabili. Sempre più alto il rischio di attacchi agli impianti idrici ed energetici

Proteggere acqua ed energia dovrebbe rimanere la massima priorità nella continua integrazione dell'Industrial Internet of Things nelle utility.

[A cura di Gastone Nencini]

Nella maggior parte dei Paesi in tutto il mondo, il settore energetico rappresenta la principale infrastruttura critica. Non è difficile immaginarlo, considerando che nelle più grandi economie industriali quasi tutti gli aspetti economici dipendono direttamente da un approvvigionamento energetico costante. E l'acqua è un'estensione naturale del settore energetico, una vera e propria necessità di vita.

Con impianti attivi in ogni parte del mondo e considerando anche l'importanza dell'acqua come componente chiave degli impianti geotermici, è fondamentale studiare i rischi informatici che queste industrie devono affrontare, in un'epoca in cui i cyber attacchi dominano quotidianamente i titoli dei giornali.

La nostra ricerca, intitolata "*Exposed and Vulnerable Critical Infrastructure*", ha proprio l'obiettivo di dimostrare quanto sia facile scoprire e sfruttare le vulnerabilità dei sistemi HMI (human machine interface systems) utilizzati nei settori idrico ed energetico, servendosi di tecniche di intelligence open-source basiche. I sistemi HMI sono una componente fondamentale dei sistemi IT industriali, che permettono agli operatori umani di interagire con gli ambienti di controllo, supervisione e acquisizione dati (supervisory control and data acquisition - SCADA).

Secondo i nostri dati, le vulnerabilità SCADA sono aumentate del 200% nel 2018 e i nostri ricercatori hanno rilevato una notevole quantità di sistemi non adeguatamente protetti in rete, che rischiano di esporre le risorse critiche, e di conseguenza l'intera popolazione, al rischio di attacchi informatici. Per la nostra ricerca abbiamo quindi raccolto una vasta gamma di schermate HMI per provare quanto i sistemi delle infrastrutture critiche mondiali (dai pozzi petroliferi agli impianti idroelettrici agli impianti di depurazione idrica) siano esposti su Internet e facilmente rilevabili utilizzando fonti di dati aperte a tutti, teorizzando i reali attacchi informatici da cui la società dovrebbe proteggere le proprie strutture.

Fingersi hacker alla ricerca di vulnerabilità (non molto) nascoste

Per identificare questi sistemi esposti, abbiamo combinato due metodi: innanzitutto, ci siamo serviti di tecniche consolidate di Internet scanning: a oggi esistono numerosi servizi che eseguono regolarmente la scansione di Internet consentendo ai ricercatori di effettuare ricerche dettagliate all'interno dei risultati. Il più usato è di gran lunga Shodan: questo motore di ricerca analizza la maggior parte delle porte esposte sui dispositivi connessi a Internet, ricavando una quantità significativa di metadati altamente informativi. Questo include i servizi in esecuzione sul dispositivo, le loro versioni, il sistema operativo e la posizione geogra-

fica del dispositivo (basandosi sul suo indirizzo IP). Nel nostro caso, servendoci di Shodan, abbiamo limitato la ricerca ai dispositivi ICS delle industrie idriche ed energetiche.
Come secondo metodo ci siamo serviti del cosiddetto approccio di "GeoStalking". Identificando per prima cosa la posizione fisica di un impianto, abbiamo poi rintracciato la posizione di tale struttura su Internet, creando una mappatura degli indirizzi IP corrispondenti. Se un aggressore, ad esempio, individuasse la posizione fisica di una turbina eolica, potrebbe facilmente servirsi della geolocalizzazione IP per ottenere un elenco di tutte le reti IP nelle immediate vicinanze del bersaglio. Tuttavia, la geolocalizzazione IP è raramente precisa, quindi l'hacker dovrebbe servirsi di una scansione delle porte o di Shodan per determinare quali indirizzi IP corrispondano ai dispositivi ICS di un parco eolico. Valutando la vulnerabilità di questi IP, potrebbe trovare agevolmente la via di accesso per ottenere il controllo della struttura o interromperne l'attività.

Geolocalizzazione di stazioni energetiche su Google Maps (Map data ©2018 Google)

Sistemi esposti in aumento: teorizzare minacce reali

La gran parte dei sistemi che sono stati identificati come esposti appartengono a piccole utility di società idriche ed energetiche e nessuna è gestito da grandi corporazioni. È importante ricordare, tuttavia, che le aziende più piccole influenzano la sicurezza anche delle società maggiori, poiché spesso sono parte della supply chain che fornisce loro risorse. Un attacco informatico contro le imprese medio-piccole influenzerà indirettamente anche le grandi aziende.
Prendiamo per esempio un pozzo di gas indipendente che rifornisce una grande centrale elettrica locale. Un fallimento del sistema a causa di un cyber attacco mirato causerà un calo della fornitura di gas, che potrebbe portare a una riduzione della produzione energetica generale e influenzare sia l'impianto più grande sia gli utenti che si affidano ai suoi servizi.

In breve, la supply chain è solida quanto il suo anello più debole.
Inoltre, a causa di questo collegamento tra aziende di diverse dimensioni, le attività delle piccole imprese esposte su Internet possono essere sfruttate dagli aggressori come test per attacchi su più larga scala. In caso che vengano scoperti, infatti, l'impatto sarebbe molto minore rispetto a quello che subirebbero nelle reti più grandi che rappresentano il loro vero target.
I nostri laboratori hanno individuato vulnerabilità nei sistemi di interfaccia uomo-macchina nel settore idrico in tutto il mondo; HMI esposte nelle industrie petrolifere americane e negli impianti energetici e di biogas europei, che comprendono sistemi per l'energia solare, eolica e idro-elettrica.

In Italia sono stati rilevati sistemi HMI esposti in impianti di biogas, per esempio, attraverso i quali è possibile accedere al menu di reset e allarmi, ma anche in centrali per la produzione energetica attraverso pale eoliche, con la possibilità di controllare i comandi di start, stop, reset e i parametri di sistema delle turbine. Numerose anche le telecamere scoperte in diversi impianti idrici.

Web camera esposta che mostra un'infrastruttura idrica

The controls for this wind turbine are located in Italy. According to additional screenshots found on the turbine manufacturer's website (name deleted for privacy), all aspects of the turbine, i.e., start, stop, reset, and system parameters, can be controlled using this software.

Esempio di schermata di controllo di una turbina in Italia

Sebbene il numero di HMI esposti rintracciati dai nostri esperimenti sia relativamente basso, desta comunque delle preoccupazioni perché questi sistemi non dovrebbero essere visibili online tout court.

Molti sistemi HMI vulnerabili sono sistemi legacy che non erano stati pensati per essere connessi alle reti e oggi vengono adattati a nuovi utilizzi. Questi HMI sono accessibili tramite server VNC (virtual network computing - strumento di condivisione del desktop da remoto) installati sul dispositivo dell'aggressore, a volte senza che l'interfaccia richieda un'autenticazione dell'utente. Anche nel caso dei sistemi attivi, utilizzati regolarmente, gli operatori non sono stati in grado di individuare e disabilitare l'utente non autenticato dal server VCN nonostante le visite ripetute. Dal momento che alcuni di questi sistemi di interfaccia uomo-macchina consentono di accedere a funzionalità critiche in grado di lanciare allarmi e interrompere o modificare la produzione, un hacker che se ne servisse potrebbe causare danni potenzialmente distruttivi al sistema.

L'abuso di HMI esposti, tuttavia, è solo uno degli attacchi informatici quotidiani affrontati dai dispositivi ICS connessi a Internet. Altri rischi noti includono gli attacchi DDoS, le vulnerability exploitation e il movimento laterale.

Un attacco DDoS (Distributed Denial of Service) è una forma di denial of service che comporta un'interruzione della rete tramite un attacco lanciato da più posizioni differenti. I motori di ricerca IoT come Shodan.io e Censys.io hanno reso possibile cercare e scoprire facilmente i dispositivi ICS esposti, per cui, utilizzando le botnet, i criminali informatici

possono inondare questi sistemi con un traffico di rete superfluo, sovraccaricandoli fino allo spegnimento. L'arresto di un dispositivo ICS determinato da un attacco DDoS potrebbe causare l'interruzione di alcuni processi critici oppure tali processi potrebbero continuare a essere eseguiti senza controllo, arrivando a causare danni materiali anche gravi.
L'attacco vulnerability exploitation rappresenta invece lo sfruttamento deliberato di punti deboli noti in un programma software al fine di compromettere il sistema, con obiettivi quasi sempre malevoli. I dispositivi ICS presentano molte vulnerabilità nascoste che un utente malintenzionato può sfruttare per poter compromettere il sistema. Al momento attuale, il sito *Industrial Control Systems Cyber Emergency Response Team (ICSCERT)* elenca 923 avvisi e 124 allarmi. Le vulnerabilità ICS sono difficili da correggere per vari motivi, tra cui il fatto che i dispositivi siano localizzati fisicamente in aree geografiche remote e gestiscano processi critici che non consentono interruzioni.
Per finire, i movimenti laterali in un attacco informatico implicano in genere attività correlate al furto di credenziali, la ricognizione e infiltrazione in altri computer per colpire dispositivi o sistemi più critici. Innanzitutto, gli aggressori compromettono una macchina all'interno della rete di un'organizzazione, in questo caso un controller ICS esposto, e utilizzandola come testa di ponte, tentano di ottenere accesso e diffusione ad altri computer collegati in rete, inclusa la rete aziendale principale. La furtività è un fattore importante nel movimento laterale, poiché questo attacco richiede di rimanere inosservato a lungo per poter penetrare il più profondamente possibile nella rete target.

La rete sotterranea del cybercrimine

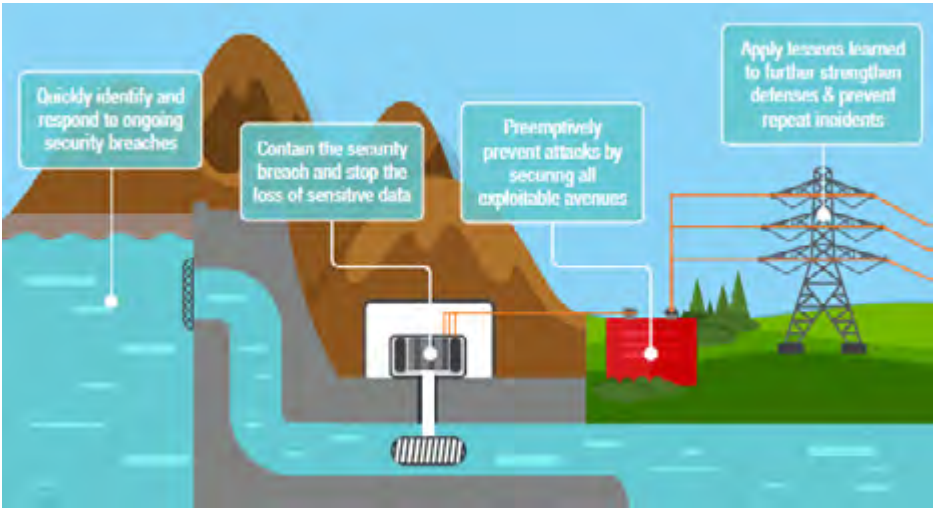
Uno dei compiti più impegnativi nelle indagini sulla criminalità informatica è l'attribuzione delle responsabilità, ma sebbene sia molto difficile individuare esattamente chi sia il colpevole, è molto più facile classificare le tipologie più comuni di aggressori e le motivazioni che li guidano.
A causa di uno scarso ritorno sull'investimento e dato che gli attacchi ICS non hanno la stessa scalabilità finanziaria degli attacchi più diffusi, i settori idrico ed energetico sembrano essere presi di mira principalmente da due gruppi di hacker. Da un lato, ci sono gruppi sofisticati e ricchi di risorse, più interessati ad azioni di spionaggio che non a un guadagno finanziario. Dall'altro, abbiamo attaccanti opportunisti o curiosi che vengono a scoprire tali apparecchiature ICS/SCADA utilizzando, come nei nostri test, servizi come Shodan, Censys e simili.
Tuttavia, sebbene queste siano le principali tipologie di aggressore in questo settore specifico, esistono anche altri colpevoli potenzialmente interessati, tra cui altri Stati, cyberterroristi, concorrenti e "hacktivisti".

La consapevolezza è sempre la miglior difesa

In conclusione, possiamo dire che il settore idrico e il settore energetico sono fondamentali non solo per l'economia di ogni nazione ma, cosa ancora più rilevante, per la vita degli esseri umani. Data l'importanza estrema di queste industrie, è quindi necessario mettere in atto

con urgenza un piano per proteggere al meglio le infrastrutture critiche dagli attacchi informatici, valutando la propria esposizione alle minacce, i rischi risultanti e implementando di conseguenza le corrette misure di sicurezza.
I notiziari riportano ormai quotidianamente notizie di attacchi di questo genere: da Black Energy a Triton, da Stuxnet a Shamoon, il messaggio chiave che possiamo trarne è che la protezione delle infrastrutture dovrebbe diventare la massima priorità per le aziende incaricate di gestirle.
Il principio difensivo chiave consiste nell'accettare compromessi e prendere le necessarie contromisure per proteggere i sistemi di controllo industriali e la supply chain dei settori idrico ed energetico sia contro attacchi esterni sia da attacchi provenienti da appaltatori, system integrator e fonti interne. Sono quattro i principali aspetti da considerare:

- **La protezione degli ICS**, tramite best practice quali la segmentazione della rete, l'offerta di accesso remoto sicuro, la gestione delle patch e dei sistemi di rilevamento di intrusioni e malware efficienti, anche tramite audit periodiche.
- **La messa in sicurezza degli ambienti di collaborative network**, tramite l'immediato coinvolgimento del team IT nelle fasi di pianificazione e sviluppo, così da effettuare una corretta valutazione del rischio e garantire gli standard di conformità e la concessione selettiva degli accessi, alle diverse tipologie di dati, ai vari partner.
- **La gestione delle minacce alla supply chain**, migliorando i programmi di gestione del rischio, valutando le vulnerabilità dei sistemi HMI prima di connetterli alla rete e garantendo il maggior isolamento possibile tra i sistemi HMI e la rete aziendale, così da preservare le esigenze operative eliminando il rischio di una loro esposizione e sfruttamento da parte di attori malintenzionati.
- **La protezione dalle minacce interne**, tenendo monitorate le attività della rete e i movimenti dei dati che possano identificare comportamenti sospetti; impostando controlli di accesso per garantire che i dipendenti accedano solo alle informazioni di cui hanno bisogno e revocando immediatamente i privilegi agli ex dipendenti; ma soprattutto mantenendo i propri dipendenti contenti, cosicché sviluppino una maggiore lealtà verso l'azienda.



In linea generale, la valutazione del rischio da parte dei team IT è fondamentale per proteggere i sistemi industriali dagli attacchi informatici. Il processo di miglioramento richiederà del tempo, data la complessità dei sistemi delle infrastrutture critiche e il gran numero di attori coinvolti nel settore, ma creare consapevolezza sulle aree vulnerabili che richiedono attenzione immediata aiuta ad accelerare il processo ed è stato l'obiettivo principale della nostra ricerca.

Attacchi e difese nel Cloud Computing nel 2018

[A cura di Andrea Piazza, Microsoft]

Il 2018 è stato l'anno in cui l'adozione del Cloud è divenuta la prassi per un gran numero di organizzazioni sia nel settore pubblico che privato, divenendo in diversi casi la soluzione preferenziale per l'esecuzione di nuovi progetti. Lo confermano vari studi, come quello dell'Osservatorio Cloud Transformation della School of Management del Politecnico di Milano[1]. Se negli anni passati l'adozione si è focalizzata inizialmente all'adozione di servizi SaaS e alla realizzazione di datacenter ibridi (On Premise + IaaS), l'anno passato ha mostrato una crescita rilevante di servizi PaaS (in particolare Artificial Intelligence), di architetture Multi-Cloud e di Serverless computing, e di servizi Cloud di gestione della sicurezza.
Al contempo la maggiore adozione dei servizi Cloud ha messo a disposizione di una platea più ampia di utenti dei servizi di sicurezza maggiormente potenziati. Grazie a strumenti come Machine Learning e Intelligenza Artificiale applicati a una mole sempre maggiore di dati, la sicurezza è divenuta uno dei settori che ha maggiormente beneficiato dell'adozione del Cloud e ne rappresenta uno dei principali fattori di adozione, poiché questi strumenti permettono di sopperire almeno parzialmente alla cronica mancanza di specialisti di sicurezza attraverso l'automazione delle attività di remediation più semplici e standardizzate[2].

Nei precedenti articoli pubblicati nei report CLUSIT per gli anni 2016 e 2017 mi sono soffermato sulle principali tipologie di minacce a cui sono esposti i servizi cloud, le principali misure di rilevazione a disposizione, e le misure di protezione proattive che possono essere adottate per limitare le possibilità di successo degli attacchi più frequenti. In questo focus-on fornirò porterò alcuni esempi di attacchi avvenuti nel 2018, fornirò un aggiornamento in merito alla frequenza e tipologia di minacce riscontrate nel corso dell'anno nei servizi cloud Azure ed Office 365 relativi a clienti italiani, e dagli strumenti antimalware Microsoft. L'obiettivo è di fornire dei dati oggettivi sugli attacchi ed evidenziare i trend anno su anno relativi alle tipologie di attacco più frequenti.

Esempi di attacchi nel Cloud nel 2018

Le tipologie di attacco si sono ovviamente evolute rispetto agli anni precedenti. Riporto a titolo di esempio tre casi reali relativamente recenti che hanno impattato una diversa tipologia di servizio Cloud.

- IaaS - Utilizzo di servizi cloud compromessi a scopi di criptomining: il furto di potere computazionale si sta spesso rilevando molto più conveniente dal punto di vista economico per gli attaccanti che non il furto di dati. Attraverso il furto di credenziali usate per

[1] https://www.zerounoweb.it/cloud-computing/osservatorio-cloud-transformation-2018-politecnico-di-milano-tutti-i-dati-in-anteprima/

[2] https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/automated-investigations-windows-defender-advanced-threat-protection

l'accesso a servizi Cloud, l'attaccante entra in possesso delle risorse computazionali IaaS dell'organizzazione e le sfrutta per usarne la potenza computazionale, evadendo le misure di rilevamento attraverso tattiche come il ridotto utilizzo di CPU o il mascheramento degli indirizzi IP del server di mining tramite l'uso di Content Delivery Networks.[3]
- PaaS - Esfiltrazione di dati inavvertitamente esposti su Storage PaaS: i casi di questo tipo sono tra i più numerosi, e si verificano solitamente a seguito di un'errata configurazione dello storage che viene esposto pubblicamente e senza richiesta di autenticazione.[4]
- SaaS - Open Authentication (OAuth) phishing: inducendo l'utente ad installare un'applicazione e richiedendo il consenso per l'applicazione ad accedere a specifici dati attraverso una richiesta di permessi OAuth, l'attaccante ottiene un accesso continuo ai dati dell'utente senza bisogno di conoscerne la password e anche a fronte di un successivo cambio di password. Il tutto avviene senza che l'utente possa insospettirsi come in un tradizionale attacco di phishing: l'utente viene rediretto a un sito legittimo su una connessione HTTPS per concedere l'accesso all'applicazione. [5]

Statistiche sugli attacchi

Nei report precedenti avevo condiviso attraverso il punto di osservazione di Microsoft le statistiche relative a tre scenari
- alert generati sui clienti italiani che utilizzano servizi in Azure (IaaS e PaaS)
- le minacce rilevate da Office 365 Advanced Threat Protection per i clienti italiani (SaaS)
- le minacce rilevate dai sistemi antimalware Microsoft su sistemi basati in Italia (Hybrid)

Quest'analisi viene ulteriormente ampliata in questo report 2018, con l'obiettivo di fornire un raffronto anno su anno, soffermandosi su:
- alert generati sui clienti italiani che utilizzano servizi in Azure nel trimestre novembre 2018 -gennaio 2019
- minacce rilevate da Office 365 Advanced Threat Protection per i clienti italiani nel semestre agosto 2018 - gennaio 2019
- minacce rilevate dai sistemi antimalware Microsoft su sistemi basati in Italia nel periodo maggio 2018 - gennaio 2019

Attacchi rilevati su Azure nel 2018

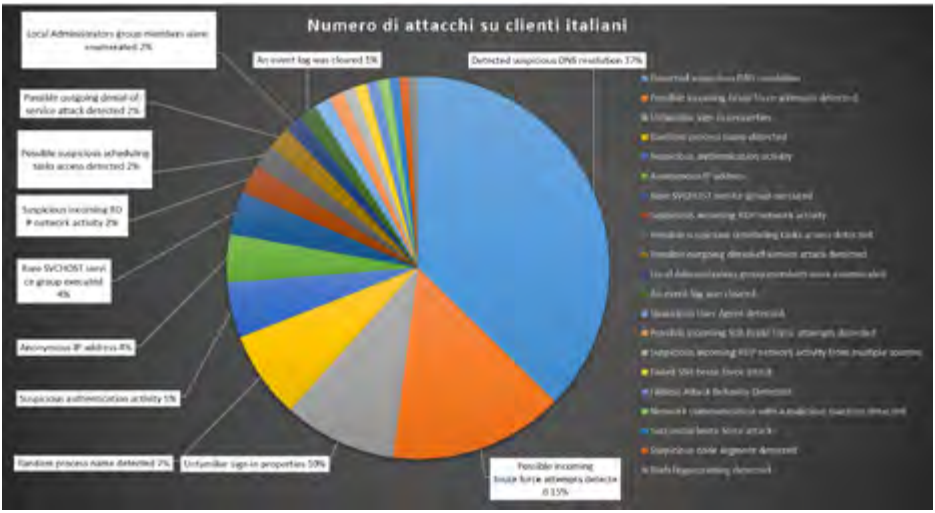
I dati qui descritti si riferiscono all'ultimo quarto del 2018. Si tratta di un campione di circa 43000 alert (+400% rispetto al periodo analogo del 2017), con una media di circa 467 alert al giorno. È importante sottolineare come gli alert si riferiscano sia ad attacchi verso i sistemi in Azure sia in uscita da essi.

---

[3] https://gizmodo.com/teslas-cloud-hacked-used-to-mine-cryptocurrency-1823155247

[4] https://cyware.com/news/insurance-startup-agentrun-accidentally-leaks-customers-personal-and-health-information-in-cloud-configuration-error-b9e885ff

[5] https://www.darkreading.com/endpoint/why-oauth-phishing-poses-a-new-threat-to-users/a/d-id/1328803



L'analisi di questi dati dal punto di vista della prevalenza ci mostra come:

- Più di un terzo degli alert generati a fronte di attacchi su Azure faccia riferimento a **comunicazioni DNS malevole**. Si tratta in particolare di rilevazioni di client che tentano di comunicare con domini malevoli e canali di command&control. Il DNS viene spesso usato inoltre come canale per esfiltrare dati da sistemi compromessi, attraverso ad esempio il tunneling del traffico TCP attraverso l'infrastruttura DNS, oppure tramite server DNS custom in grado di interpretare messaggi DNS opportunamente codificati.
- Circa il 15% degli attacchi rientra nella categoria **Brute Force** sui tradizionali protocolli di amministrazione (RDP ed SSH) e su SQL. Un ventesimo di questi tentativi ha successo.
- Un altro 15% è rappresentato da alert generati da Identity Protection, ovvero dovuti ad **attacchi alle credenziali** di Azure Active Directory. Tra questi rientrano tentativi di sign-in da indirizzi IP anonimi, da locazioni inconsuete, o da indirizzi IP noti per essere malevoli o compromessi[6].
- Un ulteriore 15% è raggruppabile nella categoria dell'**esecuzione di processi sospetti**. Tra questi rientrano alert legati all'esecuzione di processi aventi un nome casuale (e quindi tipicamente associabile ad attività malevola), di servizi o di task schedulati sospetti[7].
- I rilevamenti lato network riguardano innanzitutto **DDoS** lanciati a partire da sistemi ospitati in Azure e **Port Sweeping** (cioè la scansione di vari sistemi alla ricerca di una specifica porta in ascolto) rappresentano un sottoinsieme limitato degli attacchi complessivi, complessivamente intorno al 2%. A ciò si aggiungono **comunicazioni con sistemi**

[6] https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-risk-events

[7] https://docs.microsoft.com/en-us/azure/security-center/security-center-alerts-type

malevoli.

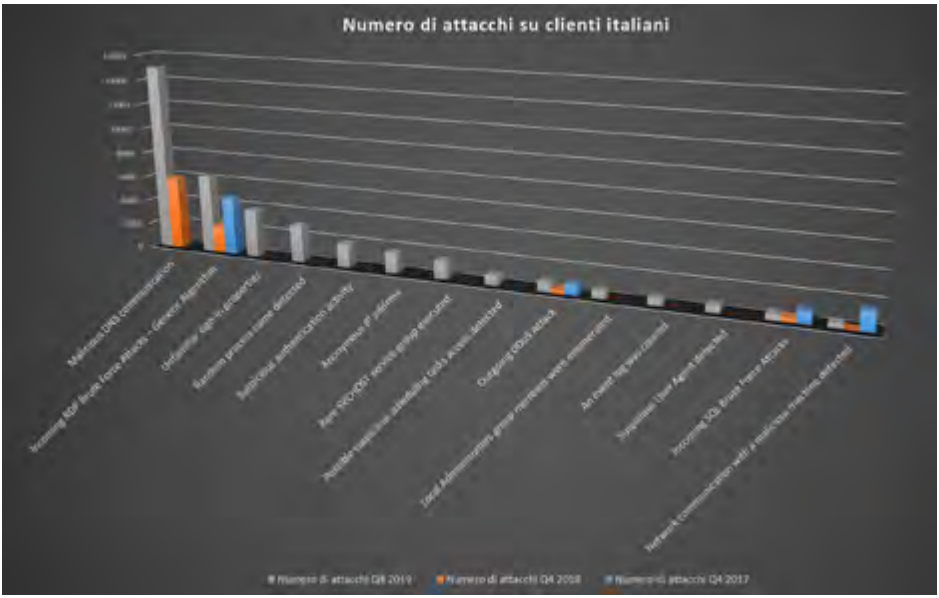
- Un'ultima categoria di alert è rappresentata da attività di **fingerprinting/reconnaissance**, come l'enumerazione dei membri del gruppo Administrators, vulnerability scanning sugli App Service (applicazioni web), e la cancellazione dei log di sistema.

La tabella seguente fornisce il dettaglio del numero di alert generati per tipologia in ciascuno dei tre anni di riferimento.

Alert Display Name	Numero di attacchi Q4 2017	Numero di attacchi Q4 2018	Numero di attacchi Q4 2019
Malicious DNS communication	0	5886	14957
Incoming RDP Brute Force Attacks – Generic Algorithm	4662	2251	6264
Unfamiliar sign-in properties	0	0	3840
Random process name detected	0	0	2959
Suspicious authentication activity	0	0	1889
Anonymous IP address	0	0	1629
Rare SVCHOST service group executed	0	0	1469
Possible suspicious scheduling tasks access detected	0	0	809
Outgoing DDoS Attack	814	340	794
Local Administrators group members were enumerated	0	0	617
An event log was cleared	0	0	589
Suspicious User Agent detected	0	0	542
Incoming SQL Brute Force Attacks	928	356	498
Network communication with a malicious machine detected	1479	54	384
Malicious AppServices	0	15	78
Outgoing SSH brute force network activity to multiple destinations	105	11	54
Incoming SSH brute force network activity	55	5	42
Outgoing SSH brute force network activity	21	5	20
Outgoing RDP brute force network activity	34	7	15
Possible compromised machine detected	16	194	2

Outgoing port scanning activity detected	341	110	1
Outgoing port scanning activity detected	83	1	1
Spam	650	92	0
Other	459	0	5543

Il grafico seguente mostra come in termini assoluti tutti gli alert siano in crescita, fatta eccezione per quelli legati al Brute Force di SQL e per gli attacchi via network (port scanning, comunicazioni con sistemi malevoli via rete).



Riepilogo come di consueto le misure principali per proteggersi dagli attacchi sopra citati:

- Utilizzo dei cosiddetti **DNS Firewall**, ovvero particolari server DNS che ispezionano le query DNS per individuare segnali di attività malware, generare alert e/o bloccare il traffico. È infine consigliabile l'abilitazione di **Azure Security Center** e della componente **DNS Analytics** di Azure Log Analytics[8] per un monitoraggio continuo del traffico DNS.
- Per la protezione dagli attacchi brute-force, l'utilizzo della **Multifactor Authentication** e di credenziali forti rappresenta sempre la prima linea di difesa. Evitare inoltre l'esposizione di protocolli e servizi non necessari riduce le possibilità di essere attaccati. Queste misure di protezione devono poi essere affiancate dalle misure di rilevamento degli attacchi.

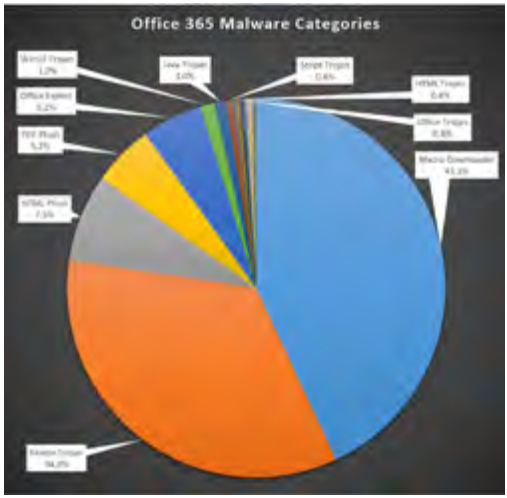
[8] https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-dns

- Per prevenire l'esecuzione di processi non desiderati, sono a disposizione soluzioni di application whitelisting come Adaptive application controls[9] che permettono di apprendere quali sono le applicazioni normalmente utilizzate su un sistema e di creare automaticamente delle regole di whitelisting che bloccano tutti gli altri software, andando a colmare eventuali lacune nella protezione antimalware.
- Per quanto riguarda la protezione dagli attacchi DDOS, oltre alle funzionalità di base incluse in Azure, sono disponibili sul mercato diverse opzioni sia Microsoft che di terze parti che consentono di aggiungere funzionalità avanzate di protezione[10].
- Nel corso del 2018 è stato pubblicato dal Center for Internet Security (CIS) in partnership con Microsoft il security benchmark[11] che raccoglie diverse best practice di sicurezza per Azure.

Attacchi rilevati su Office 365

I dati seguenti coprono in questo caso un arco temporale di 6 mesi, compreso tra agosto 2018 e gennaio 2019, e mostrano quali siano, ad alto livello, le principali categorie di minacce rilevate da Office 365 ATP sui clienti italiani. Ricordo che Office 365 ATP è lo strumento deputato alla protezione della posta elettronica dalle minacce più avanzate, attraverso l'utilizzo di tecnologie di detonation degli allegati e di analisi dei link che consentono di ridurre i tempi di rilevamento delle nuove varianti e di ridurre al minimo l'esposizione al rischio del paziente zero.

Categoria	Numero
Macro Downloader	49740
Macro Trojan	39588
HTML Phish	8640
PDF Phish	6025
Office Exploit	5999
Win32 Trojan	1396
Java Trojan	1176
Script Trojan	519
HTML Trojan	445
Office Trojan	354
Script Downloader	326
Win32 Downloader	211



[9] https://docs.microsoft.com/en-us/azure/security-center/security-center-adaptive-application

[10] https://azure.microsoft.com/en-us/services/ddos-protection/

[11] https://azure.microsoft.com/en-us/resources/cis-microsoft-azure-foundations-security-benchmark/

Categoria	Numero
Office Downloader	194
HTML Downloader	167
PDF Trojan	133
Script Malware	124
XPS Phish	97
PDF Downloader	73
Office Phish	72
Win32 Exploit	54
PDF Spam	49
LNK Downloader	47

Categoria	Numero
HTML Malware	14
LNK Trojan	12
Office Malware	11
Win32 InfoStealer	10
PDF Malware	6
Win32 Phish	4
Win32 Malware	3
Macro Malware	3
Win32 Backdoor	2
HTML Spam	2

La stragrande maggioranza dei malware intercettati da Office 365 ATP è rappresentata da Macro (oltre il 77%) di tipo Trojan e Downloader (software deputati a scaricare ulteriori componenti malevole dopo l'infezione iniziale).
Una percentuale inferiore ma ancora molto significativa (5-7%) è rappresentata da 3 categorie:

- PDF Phishing
- HTML Phishing
- Exploit tramite file Office

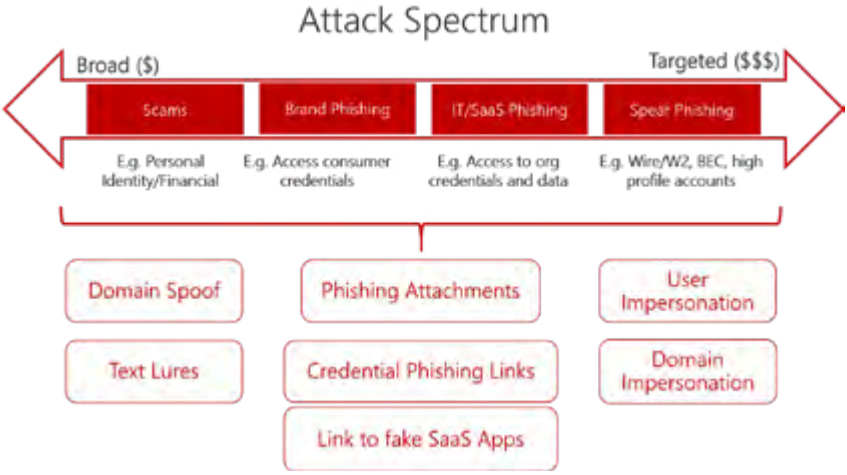
Infine, troviamo minacce di tipo trojan di diverse tipologie (eseguibili Windows, Java Script, HTML ed Office).
La gestione della configurazione di sicurezza della Macro in Office risulta quindi una delle azioni più importanti da implementare. Raccomando quindi l'utilizzo della baseline di sicurezza per Office 365[12] che copre nel dettaglio le configurazioni consigliate, e l'abilitazione della funzionalità di Attack Surface Reduction[13] per ridurre la superficie d'attacco sulle postazioni di lavoro.
La tabella seguente mostra il raffronto anno su anno delle categorie di minacce.

[12] https://blogs.technet.microsoft.com/secguide/2018/02/13/security-baseline-for-office-2016-and-office-365-proplus-apps-final/

[13] https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-exploit-guard/enable-attack-surface-reduction#enable-and-audit-attack-surface-reduction-rules

Categoria	2017	2018
Downloader	18,35%	43,95%
Trojan	61,03%	37,77%
Phish	7,70%	12,85%
Exploit	0,98%	5,24%
Malware	0,00%	0,14%
Spam	0,00%	0,04%
Infostealer	10,42%	0,01%

Rispetto ai dati dell'anno precedente, la prevalenza percentuale dei Downloader è più che raddoppiata (dal 18 al 44%) mentre i Trojan presentano una tendenza opposta.
Aumenta decisamente l'incidenza degli Exploit e del Phishing.
Le tecniche di phishing continuano ad evolversi: la figura seguente[14] mostra alcune tra le principali tecniche usati nell'ambito del phishing per attacchi che spaziano da quelli su larga scala sino a quelli mirati.



Se da un lato rimane sempre di fondamentale importanza un'adeguata formazione di sicurezza dell'utente finale per limitare il successo di questo attacchi, è altresì vero che gli strumenti di protezione della posta richiedono continui e rapidi aggiornamenti per rimanere al passo degli attaccanti. In quest'ottica il vantaggio dei servizi Cloud è evidente, grazie al beneficio offerto da aggiornamenti continui che vengono immediatamente messi a disposizione dell'intero ecosistema che si avvale del servizio.

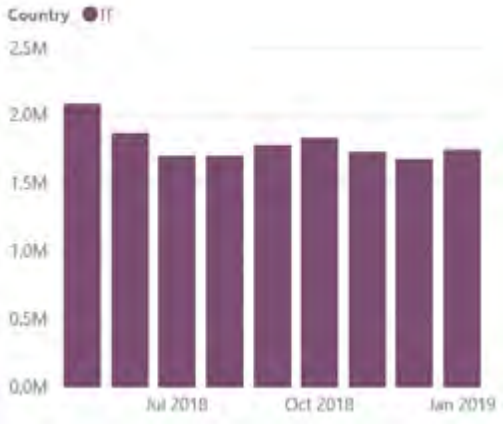
[14] https://cloudblogs.microsoft.com/microsoftsecure/2018/10/17/how-office-365-learned-to-reel-in-phish/

Ricordo infine che a gennaio 2019 è stato pubblicato dal Center for Internet Security (CIS) in partnership con Microsoft il security benchmark per Office 365[15] che permette di definire una baseline di sicurezza iniziale per il servizio.

Attacchi rilevati da Antimalware

In quest'ultimo paragrafo ci soffermiamo sui dati relativi alle rilevazioni compiute attraverso gli strumenti antimalware Microsoft. Sono inclusi dati provenienti da strumenti come Windows Defender, System Center Endpoint Protection, Microsoft Safety Scanner e Microsoft Security Essentials, ed altri strumenti che utilizzano come minimo comune denominatore il Microsoft Malware Protection Engine. L'engine Microsoft è utilizzato anche come uno dei possibili meccanismi di protezione dei sistemi virtuali in Azure.
Nel caso dei sistemi antimalware, l'utilizzo del cloud è diventato prevalente come meccanismo per migliorare la protezione. Diversi vendor, inclusa Microsoft, usano funzionalità di verifica dei file sospetti nel cloud con l'obiettivo di ridurre i tempi di risposta alla rilevazione di nuovi malware da ore a secondi e di proteggere anche il cosiddetto "paziente zero". Attraverso meccanismi euristici, machine learning, e analisi automatizzate del file, viene determinato se il file sospetto è malevolo o innocuo, e in taluni casi viene richiesto l'invio del file completo per eseguire un'analisi più approfondita. Gli esiti delle analisi nel cloud vengono poi tipicamente messi a disposizione di tutti gli utenti del sistema antimalware in modo che di questi risultati possano beneficiare tutti gli utilizzatori dell'antimalware nel momento in cui dovessero venire a contatto dello stesso file.

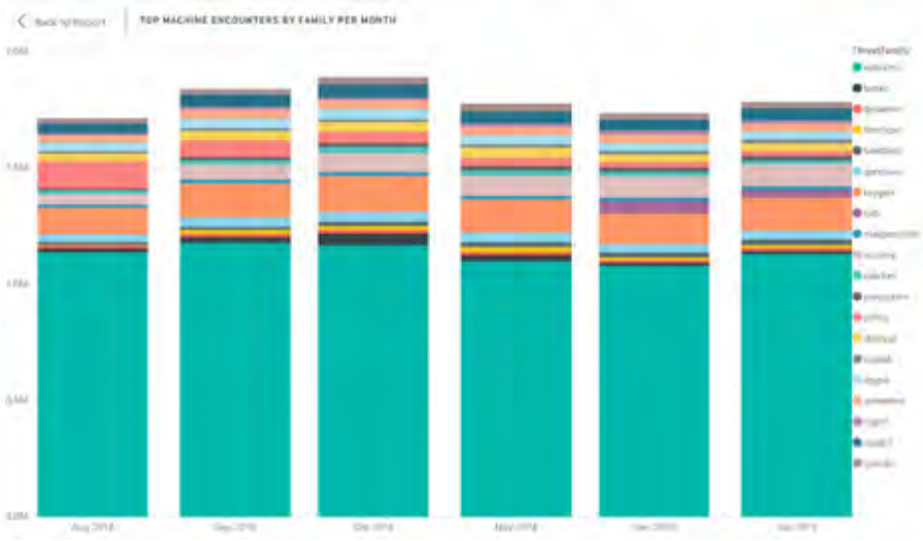
La figura seguente mostra i dati relativi ai cosiddetti "Malware Encounter" ovvero il numero di sistemi che hanno riportato la rilevazione di almeno un malware.



[15] https://cloudblogs.microsoft.com/microsoftsecure/2019/01/10/best-practices-for-securely-using-microsoft-365-the-cis-microsoft-365-foundations-benchmark-now-available/

Complessivamente la tendenza è in decrescita, dato che è ancora più evidente se confrontato con l'anno precedente dove i malware encounter nel periodo settembre 2017 - gennaio 2018 si attestavano stabilmente al di sopra dei 2.5Mln con punte di 3Mln.

Le due figure seguenti rappresentano rispettivamente:
- il numero di Machine Encounter per tipologia di minaccia rilevati in Italia nel corso degli ultimi 6 mesi.
- Il numero di File Encounter per tipologia di minaccia rilevati in Italia nel corso degli ultimi 6 mesi



Le famiglie di malware più diffuse rientrano nelle categorie:
- **Hack tools**:, le famiglie di tool utilizzate per "craccare" copie non registrate di software Microsoft e di terze parti, come AutoKMS, Wpakill, Gendows e Patcher risultano essere tra i più diffusi in assoluto. Spesso l'utilizzo di questi strumenti è associato all'installazione di malware o software non desiderato[16]. Analogamente, la famiglia dei Keygen è riscontrata su un largo numero di sistemi. Più del 50% dei sistemi su cui è presente la famiglia Keygen presenta anche altre forme di malware[17].
- **Trojan**: tra le varie minacce prevalenti in questo ambito, segnalo BroCoiner, un cryptominer di Monero basato su codice Javascript.
- **Potentially Unwanted Applications**: rientrano in questa famiglia quei software che

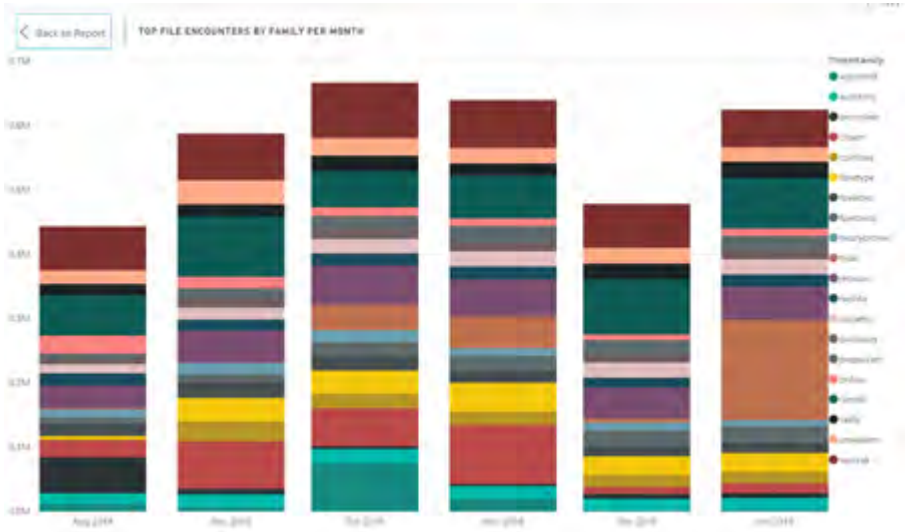
[16] SIR v13 https://www.microsoft.com/en-us/download/details.aspx?id=34955

[17] https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=HackTool:Win32/Keygen&threatId=-2147373502

installano insieme a funzionalità desiderate delle componenti indesiderate senza richiedere il consenso dell'utente. Ne è un esempio la famiglia Prepscram, che va ad installare dei Browser Modifier, oppure VPN Proxy Unblockers come Hola.

- **Browser Modifiers**: anche quest'anno il più diffuso è stato Win32/Xeelyak, un browser modifier che apporta dei cambiamenti al browser (Google Chrome e Internet Explorer) senza consenso:
  - Modifica della homepage
  - Modifica del motore di ricerca
  - Aggiunta di estensioni browser e toolbar
  - Disabilitazione di feature di sicurezza del browser

Tipicamente questa minaccia viene installata attraverso altri software non desiderati come BrowserModifier:Win32/Sasquor e BrowserModifier:Win32/Suptab.
Per la definizione di questi software non desiderati, che alterano senza consenso la configurazione del PC, Microsoft utilizza un insieme di criteri oggettivi e documentati[18].



Chiudo con una nota di colore, relativa alla famiglia dei Worm: a distanza di 10 anni dal suo rilascio, Conficker è ancora la famiglia numero uno di Worm presenti in Italia, con una popolazione stabile di macchine infette dell'ordine di circa 10000 sistemi, pari a circa il 10% di tutti i sistemi al mondo infetti. Solo la Cina ha un numero (di poco) superiore.

[18] https://www.microsoft.com/en-us/wdsi/antimalware-support/malware-and-unwanted-software-evaluation-criteria

Conclusioni

Il numero di attacchi verso servizi Cloud nel 2018 è aumentato di pari passo con l'adozione dei servizi stessi, e si è evoluto introducendo nuove tipologie di minacce in tutte le fasi della catena di attacco e in modo trasversale ai servizi SaaS, PaaS e IaaS.

Allo stesso tempo è diminuita il numero di sistemi affetti da malware rilevati in Italia nel corso dell'anno.

A fronte di questa evoluzione il mercato ha risposto mettendo a disposizione strumenti avanzati di protezione, rilevamento e risposta automatica agli incidenti che aiuta i professionisti della sicurezza a mantenere il controllo sui servizi cloud e a rimuovere dal carico di lavoro delle figure più specializzate la gestione degli incidenti meno complessi.

Rimane a mio parere fondamentale adottare le best practice di sicurezza[19] [20] del mondo cloud che hanno ormai raggiunto un buon livello di maturità con un punto di vista che privilegi sempre di più un approccio cloud-first anche nella gestione della sicurezza.

[19] https://docs.microsoft.com/en-us/office365/securitycompliance/security-best-practices

[20] https://docs.microsoft.com/en-us/azure/security/security-best-practices-and-patterns

GLOSSARIO

Account hijacking	Compromissione di un account ottenuta ad esempio mediante ***phishing***.
Account take-over	Acquisizione illecita di un account al fine di impersonificare la vittima (ad esempio di effettuare transazioni finanziarie sui suoi conti).
ACDC (Advanced Cyber Defence Center)	Progetto europeo la cui finalità è offrire soluzioni e creare conoscenza per aiutare le organizzazioni in tutta Europa a combattere le botnet. (www.acdc-project.eu/).
Adware	Tipo di ***malware*** che visualizza pubblicità solitamente senza il consenso dell'utente. Può includere funzionalità ***spyware***.
AISP (Account Information Service Provider)	Prestatori di servizi di informazione sui conti di pagamento che forniscono ai clienti che detengono uno o più conti di pagamento online presso uno o più Istituti di Credito, servizi informativi relativi a saldi o movimenti dei conti aperti.
Altcoins (Alternative coins)	Criptovalute di seconda generazione. Spesso implementano funzioni o caratteristiche aggiuntive a quelle originariamente ipotizzate dai creatori di Bitcoin. Tra esse vi sono un maggior livello di anonimato o la non tracciabilità delle transazioni (Monero, Zcash, DeepOnion), la possibilità di generare e gestire ***smart contract*** o creare token di sviluppatori terzi ospitati sulla medesima ***blockchain*** (Ethereum, NEO, Stratis), l'aumento della velocità dei trasferimenti e della scalabilità del sistema (Ripple, Stellar Lumens), nonchè la predisposizione per l'utilizzo tramite dispositivi dell'Internet of Things (IOTA).
Analytics-As-A-Service	Servizi on demand per l'analisi di dati utilizzabili anche nell'ambito della sicurezza, ad esempio, per passare al setaccio i dati della rete aziendale e individuare eventi anomali ed eventuali attacchi.

Apt (Advanced Persistent Treath)	Schemi di attacco articolati, mirati a specifiche entità o organizzazioni contraddistinti da: • un accurato studio del bersaglio preventivo che spesso continua anche durante l'attacco • l'impiego di tool e ***malware*** sofisticati • la lunga durata o la persistenza nel tempo cercando di rimanere inosservati per continuare a perpetrare quanto più possibile il proprio effetto.
Arbitrary File Read	***Vulnerabilità*** che consente ad un attaccante di accedere a file tramite richieste Web remote.
Attacchi Pivot back	Tipo di attacco nel quale viene compromessa una risorsa nel public cloud per ottenere informazioni che possono poi essere usate per attaccare l'ambiente on premise.
Backdoor	Soluzione tecnica che consente l'accesso ad un sistema superando i normali meccanismi di protezione.
BEC fraud (Business e-mail compromise)	Tipi di attacco phishing mirati verso figure aziendali al fine di convincere le vittime a trasferire somme di denaro o rilevare dati personali. (Vedi anche CEO fraud)
BIA (Business Impact Analysis)	Tecnica di valutazione delle conseguenze sul business di un'organizzazione (economiche, reputazionali, legali…) di interruzioni derivanti da vari scenari avversi (indisponibilità del sistema informativo o parte di esso, indisponibilità del personale, indisponibilità dei locali…).
Blocj	Tecnica utilizzata nell'ambito dell'***e-voting***. Con la firma elettronica cieca (blind signature) la preferenza espressa dall'elettore viene cifrata. Successivamente viene apposta la firma elettronica da un ufficiale elettorale, che autentica il voto e infine si ha il deposito nell'urna.

Blockchain	Tecnologia che consente la registrazione di transazioni, in uno scenario trustless, fra gli attori della stessa blockchain mediante l'utilizzo di un registro digitale immodificabile presente su vari nodi della rete, costituito da blocchi (block) fra loro concatenati (chain).
Booter-stresser	Strumenti a pagamento che consentono di scatenare attacchi *DDOS*.
Botnet	Insieme di dispositivi (compromessi da ***malware***) connessi alla rete utilizzati per effettuare, a loro insaputa, un attacco ad esempio di tipo *DDOS*.
Buffer overflow	Evento che ha luogo quando viene superato il limite di archiviazione predefinito di un'area di memorizzazione temporanea.
Business continuity	Soluzioni di natura tecnica ed organizzativa predisposte per garantire la continuità dell'erogazione di un servizio (eventualmente con uno SLA ridotto).
Captatore informatico	Software che viene immesso in dispositivi elettronici portatili al fine di intercettare comunicazioni o conversazioni tra presenti, il cui uso è specificatamente regolamentato dal Codice Penale, nel corso di indagini su alcuni specifici crimini.
Carding	Scambio e compravendita di informazioni riguardanti carte di credito, debito o account bancari, che vengono poi utilizzate per eseguire truffe di carattere finanziario acquistando beni o trasferendo fondi ai danni dei legittimi proprietari.
CEO Fraud	Tipi di attacco phishing mirati verso figure aziendali ad altissimo profilo, generalmente amministratori delegati, presidenti dell'azienda, direttori finanziari, etc.

CERT (Computer Emergency Response Team)	Struttura destinata a rispondere agli incidenti informatici e alla rilevazione e contrasto alle minacce. Fra i principali obiettivi di un CERT (vedi CERT Nazionale): fornire informazioni tempestive su potenziali minacce informatiche che possano recare danno a imprese e cittadini; incrementare la consapevolezza e la cultura della sicurezza; cooperare con istituzioni analoghe, nazionali ed internazionali, e con altri attori pubblici e privati coinvolti nella sicurezza informatica promuovendo la loro interazione; facilitare la risposta ad incidenti informatici su larga scala; fornire supporto nel processo di soluzione di crisi cibernetica.
Cifratura "at rest" o "a riposo"	Cifratura dei dati nello storage.
Cifratura omomorfa	Tecnica utilizzata nell'ambito dell'*e-voting*. Con questo sistema di cifratura è possibile sommare due numeri cifrati o compiere altre operazioni algebriche senza decifrarli.
CISP (Card-based Payment Instrument Issuing Service Provider)	Prestatori di servizi di pagamento emittenti strumenti di pagamento basati su carta, che potranno emettere carte di debito a valere su conti di pagamento detenuti dai clienti presso Istituti di Credito diversi.
Cloud weaponization	Tipo di attacco nel quale l'attaccante ottiene un primo punto d'ingresso nell'infrastruttura cloud attraverso la compromissione e il controllo di alcune machine virtuali. L'attaccante utilizza poi questi sistemi per attaccare, compromettere e controllare migliaia di altre macchine, incluse altre appartenenti allo stesso service provider cloud dell'attacco iniziale, e altre appartenenti ad altri service provider pubblici.
Cognitive Security	Applicazione all'ambito della sicurezza delle soluzioni di Cognitive Computing.

C&C (Command & Control)	I centri di comando e controllo (C&C) sono quegli host utilizzati per l'invio dei comandi alle macchine infette (bot) dal ***malware*** utilizzato per la costruzione della ***botnet***. Tali host fungono da ponte nelle comunicazioni tra gli host infetti e chi gestisce la botnet, al fine di rendere più difficile la localizzazione di questi ultimi.
Credential Stuffing	Attacco nel quale vengono utilizzate coppie di user id/password raccolte in precedenza in modo fraudolento.
Cryptovaluta	Token digitale che costituisce uno strumento di pagamento. È possibile includere nei messaggi di pagamento ulteriori informazioni cosichè i token possono rappresentare digitalmente anche altri asset materiali o immateriali.
CVSS versione 3 (Common Vulnerability Scoring System)	Sistema di valutazione delle vulnerabilità che fornisce un modo per acquisire le principali caratteristiche di una vulnerabilità e per produrre un punteggio numerico che rifletta la sua gravità, nonché una rappresentazione testuale di tale punteggio. Il punteggio numerico può quindi essere tradotto in una rappresentazione qualitativa (come bassa, media, alta e critica) per aiutare le organizzazioni a valutare e prioritizzare in modo adeguato i loro processi di gestione delle vulnerabilità. (https://www.first.org/cvss/specification-document)
Constituency	Nell'ambito di un *CERT* indica a chi è rivolto il servizio (ad esempio Pubblica Amministrazione Centrale, Regioni e Città metropolitane).
Cryptojacking	Processo che sfrutta illegalmente le risorse informatiche di una vittima per generare criptovaluta. In sostanza gli aggressori sottraggono potenza di calcolo installando un'applicazione di mining di criptovaluta sul sistema della vittima, che sia un PC o uno smartphone. La generazione di valuta virtuale, nota anche come criptovaluta, è molto dispendiosa in termini di potenza di elaborazione, motivo per cui gli aggressori devono infettare un vasto numero di vittime e utilizzarne la potenza di calcolo per generare nuove unità monetarie virtuali.

CSIRT (Computer Security Incident Response Team)	Struttura sostanzialmente simile ad un *CERT*.
Cyber intelligence	Attività volte a raccogliere e rielaborare informazioni al fine prevedere possibili minacce (non esclusivamente di natura informatica) agli asset oggetto di tutela.
Cybersquatting	Attività volta ad appropriarsi di nomi di dominio di terzi, in particolare di marchi commerciali di rilievo, al fine di trarne profitto.
Cyber crime	Attività criminali effettuate mediante l'uso di strumenti informatici.
Cyber espionage	Attività di spionaggio effettuata mediante l'uso di tecniche informatiche illecite.
Cyber Kill Chain	La cyber kill chain è un modello definito dagli analisti di Lockheed Martin come supporto decisionale rispetto alla rilevazione e risposta alle minacce. Esso include le seguenti fasi: reconnaissance, weaponization, delivery, exploitation, installation and persistence, command and control (C2), actions.
Cyber resilience	Capacità di un'organizzazione di resistere preventivamente o ad un attacco e di ripristinare la normale operatività successivamente allo stesso.

Cyber security	Gruppo di attività e competenze multidisciplinari, complesse e sofisticate, molte delle quali non informatiche, che sono oggettivamente di difficile integrazione con le prassi esistenti di gestione dell'ICT e di allocazione dei budget relativi, poiché la loro implementazione richiede di superare paradigmi tecnologici e silos organizzativi costruiti negli anni a partire da esigenze di compliance e da metodi e strumenti propri della sicurezza informatica "tradizionale". lo scopo complessivo di questo insieme di discipline è il proteggere tutti quegli asset materiali ed immateriali che possono essere aggrediti tramite il "cyberspazio" ovvero che dipendono da esso, garantendo allo stesso tempo la governance, l'assurance e la business continuity di tutta l'infrastruttura digitale a supporto.
Cyber Diplomacy	"Incoraggiamo tutti gli Stati a impegnarsi in comportamenti rispettosi delle leggi e delle norme e che concorrano al rafforzamento della fiducia nel rispettivo uso delle TIC. Approcci collaborativi contribuirebbero anche a lottare contro l'uso del cyberspazio ad opera di attori non-Stato, a scopo terroristico e criminale". *(Dichiarazione del G7 sul comportamento responsabile degli stati nel cyberspazio) www.esteri.it/mae/resource/doc/2017/04/declaration_on_cyberspace_ita.doc*
Cyber-reasoning systems	Sistemi sviluppati per individuare automaticamente le vulnerabilità delle reti più complesse implementando algoritmi cognitivi.
Cyber-weapon	***Malware*** (o anche hardware) progettato o utilizzato per causare danni attraverso il dominio cyber. *(NATO Cooperative Cyber Defence Centre of Excellence).*
Cryptolocker	***Malware*** che ha come finalità criptare i file presenti nel dispositivo infetto al fine di richiedere un riscatto alla vittima per renderli nuovamente intellegibili.
CVV2 (Card Verification Value 2)	Codice di sicurezza utilizzato sulle carte di pagamento.

Dark web	Parte oscura del World Wide Web, sottoinsieme del deep web, accessibile mediante l'uso di apposite applicazioni software.
DPIA (Data Protection Impact Assessment)	Valutazione d'impatto sulla protezione dei dati. Una valutazione d'impatto sulla protezione dei dati è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli. (Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679)
Data breach	La violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati. *(Art. 4.12 GDPR)* Alcuni possibili esempi: l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati; il furto o la perdita di dispositivi informatici contenenti dati personali; la deliberata alterazione di dati personali; l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.; la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità; la divulgazione non autorizzata dei dati personali. *(Garante per la protezione dei dati personali)*
Deep Web	L'insieme dei contenuti presenti sul web e non indicizzati dai comuni motori di ricerca (Google, Bing…).
Defacement	Manipolazione del contenuto di una pagina web (tipicamente la home page) a scopi dimostrativi.

DES (Data Encryption Standard)	Algoritmo per la cifratura dei dati a chiave simmetrica.
DNS (Domain Name System)	Indica sia l'insieme gerarchico di dispositivi, sia il ***protocollo***, utilizzati per associare un indirizzo IP ad un nome di dominio tramite un database distribuito.
DNS Open Resolver	Sistemi vulnerabili utilizzati come strumento per perpetrare attacchi informatici di tipo *DDOS* amplificati.
Sinkhole	Tecnica per reindirizzare il traffico di rete verso uno specifico server al fine, ad esempio, di analizzarlo.
DNSSEC (Domain Name System Security Extensions)	Insieme di specifiche per garantire alcuni aspetti di sicurezza delle informazioni fornite dai *DNS*.
Dos (Denial of Service)	Attacchi volti a rendere inaccessibili alcuni tipi di servizi. Possono essere divisi in due tipologie: • applicativi, tesi a generare un numero di richieste maggiore o uguale al numero di richieste massimo a cui un server può rispondere (ad esempio numero di richieste web HTTP/HTTPS concorrenti); • volumetrici, tesi a generare un volume di traffico maggiore o uguale alla banda disponibile in modo da saturarne le risorse. Se vengono utilizzati più dispositivi per l'attacco coordinati da un centro di *C&C* si parla di *DDOS* (Destribuited Denial of Service).
DDoS (Distributed Denial of Service)	Attacchi *DOS* distribuiti, cioè basati sull'uso di una rete di apparati, costituenti in una botnet dai quali parte l'attacco verso l'obiettivo.
DDoS-for-hire	Letteralmente servizio DDoS da noleggiare.
DGA (Domain generation algorithms)	Algoritmo utilizzato da alcuni ***malware*** per la generazione di migliaia di nomi di dominio alcuni dei quali sono utilizzati dai loro server *C&C*.

DNS cache poisoning	Tipo di attacco nel quale l'attaccante inserisce corrispondenze Indirizzo-IP alterate all'interno della cache del meccanismo di risoluzione degli indirizzi IP. Come risultato la cache userà l'indirizzo IP alterato in tutte le successive transazioni. L'indirizzo che comparirà nella barra URL di un browser sarà quello corretto e desiderato, ma il corrispondente indirizzo IP utilizzato sarà quello alterato e tutto il traffico di rete sarà quindi reindirizzato verso il sito replica controllato dai cyber criminali e nel quale si simulano log in per tracciare tutti i fattori di autenticazione inseriti.
Downloader	Software deputati a scaricare ulteriori componenti malevoli dopo l'infezione iniziale.
Drive-by exploit kit	Il fenomeno dei drive-by ***exploit kit*** è particolarmente insidioso e si realizza inducendo l'utente a navigare su pagine web che nascondono attacchi, appunto gli ***exploit kit***, per versioni vulnerabili di Java o dei plug-in del browser. Questi attacchi sono in grado di sfruttare macchine utente vulnerabili, impiantandovi malware, con la semplice navigazione sulle pagine malevole anche in assenza di interazione dell'utente con la pagina.
DRdos (Destribuited Reflection Denial of Service)	Sfruttando lo ***spoofing*** dell'indirizzo IP di una vittima, un utente malintenzionato può inviare piccole richieste ad un host vulnerabile inducendolo ad indirizzare le risposte alla vittima dell'attacco. Questa tipologia di DDOS permette al malintenzionato di amplificare la potenza del suo attacco anche di 600 volte, come dimostrato nel caso del protocollo NTP.
Dual use	I prodotti a duplice uso sono beni e tecnologie che possono avere un impiego sia civile che militare, includendo prodotti che possono in qualche modo servire nella fabbricazione di armi nucleari o di altri congegni esplosivi nucleari. (da Regolamento (CE) n. 428/2009 - regime comunitario di controllo delle esportazioni, del trasferimento, dell'intermediazione e del transito di prodotti a duplice uso).
Eavesdropping	Nell'ambito VOIP è un attacco del tutto simile al classico man-in-the-middle. L'attaccante si inserisce in una comunicazione tra due utenti con lo scopo di spiare, registrare e rubare informazioni.

EDR (Endpoint Detection and Response)	Dispositivi la cui finalità è quella di mantenere un costante monitoraggio di eventi sospetti al fine di garantire una reazione preventiva e continua alle minacce.
eIDAS	REGOLAMENTO (UE) N. 910/2014 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE finalizzato a garantire il buon funzionamento del mercato interno perseguendo al contempo un adeguato livello di sicurezza dei mezzi di identificazione elettronica e dei servizi fiduciari.
E-voting	Con l'espressione "sistema di e-voting" ci si riferisce al momento in cui una tecnologia elettronica è impiegata in una o più fasi di un processo elettorale, scrutinio compreso, senza che sia necessariamente sfruttata la rete Internet.
Exploit	Codice con cui è possibile sfruttare una ***vulnerabilità*** di un sistema. Nel database Common Vulnerabilities and Exposures (cve.mitre.org) sono presenti sia le vulnerabilità note, sia i relativi exploit.
Exploit kit	Applicazioni utilizzabili anche da attaccanti non esperti, che consentono di sfruttare in forma automatizzata le ***vulnerabilità*** di un dispositivo (di norma browser e applicazioni richiamate da un browser).
Fast flux	Tecnica che permette di nascondere i *DNS* usati per la risoluzione dei domini malevoli dietro ad una rete di macchine compromesse in continua mutazione e perciò difficili da mappare e spegnere.
Fix	Codice realizzato per risolvere errori o ***vulnerabilità*** nei software.

GDPR	REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).
GRE (Generic Routing Encapsulation)	Protocollo di tunneling che incapsula vari protocolli di livello rete all'interno collegamenti virtuali point-to-point.
Info Stealer	Software orientati a rubare informazioni all'utente compromesso.
Hacktivism	Azioni, compresi attacchi informatici, effettuate per finalità politiche o sociali.
Hit & Run (o Pulse wave)	Attacchi di breve durata, ma frequenti nell'arco di poche ore.
Honeypot	Letteralmente barattolo del miele. Indica un asset esca isolato verso cui indirizzare e raccogliere informazioni su eventuali attacchi, al fine di tutelare il reale sistema informativo.
HTTP POST DoS Attack	Attacco che sfrutta un difetto di progettazione di molti server web. L'attaccante inizia una connessione http del tutto lecita verso un server web andando ad abusare del campo 'Content-Lenght'. Visto che la maggior parte dei server web accetta dimensioni del payload del messaggio anche di 2Gb, l'attaccante comincia ad inviare il corpo del messaggio ad una ridottissima velocità (anche 1byte ogni 110 secondi). Ciò comporta che il server web resta in ascolto per molto tempo, lasciando aperti i canali http (del tutto leciti) andando quindi a saturare tutte le sue risorse visto che le connessioni restano aperte.
Kill Switch	Termine generico per indicare un dispositivo che serve a bloccare in modo forzato un'attività.

ICMP (Internet Control Message Protocol)	Protocolli che consentono ai dispositivi di una rete di comunicare informazioni di controllo e messaggi.
IDS (Intrusion detection system)	Dispositivo in grado di identificare modelli riconducibili a possibili attacchi alla rete o ai sistemi.
IMEI (International Mobile Equipment Identity)	Codice univoco che identifica un terminale mobile
IMSI (International Mobile Subscriber Identity)	Codice univoco internazionale che combina SIM, nazione ed operatore telefonico.
Information warfare	Insieme di tecniche di raccolta, elaborazione, gestione, diffusione delle informazioni, per ottenere un vantaggio in campo militare, politico, economico…
Incident handling	Gestione di un incidente di sicurezza informatica. ENISA classifica le fasi di tale gestione in Incident report, Registration, Triage, Incident resolution, Incident closure, Post-analysis.
Infostealer	*Malware* finalizzato a sottrarre informazioni, quali ad esempio credenziali, dal dispositivo infetto.
Interception and Modification	Nell'ambito VOIP intercettazione di comunicazioni lecite tra utenti ed alterazione delle stesse con lo scopo di arrecare disservizi come l'abbassamento della qualità delle conversazioni e/o l'interruzione completa e continua del servizio.

Intrusion software	Spyware (definizione della Commissione Europea nell'ambito della regolamentazione dell'esportazione di prodotti dual use). Un "intrusion software", ad esempio, può essere utilizzato da una società di security per testare la sicurezza di un sistema informatico e al contempo essere usato da uno Stato non democratico per controllare e intercettare le conversazioni dei propri cittadini.
IoC (Indicatori di compromissione)	Qualsiasi informazione che possa essere utilizzata per cercare o identificare sistemi potenzialmente compromessi (indirizzo IP/ nome dominio, URL, file hash, indirizzo email, X-Mailer…) (Common Framework for Artifact Analysis Activities – ENISA)
IPMI (Intelligent Platform Management Interface)	Specifica di una interfaccia di basso livello utilizzata da diversi costruttori che consente ad un amministratore di sistema di gestire server a livello hardware. Attraverso la BMC (Baseboard Management Controller) consente, tra le altre cose, l'accesso al BIOS, ai dischi ed ai dispositivi hardware in generale e, di fatto, il controllo del server. IPMI contiene una serie di vulnerabilità ampiamente descritte e conosciute e, in definitiva, non dovrebbe essere aperto all'esterno.
IPS (Intrusion prevention system)	Dispositivo in grado non solo di identificare possibili attacchi, ma anche di prevenirli.
Istant phishing	Tecnica di attacco nella quale nell'istante in cui l'utente inserisce le credenziali, o più in generale le informazioni all'interno del sito clone, il cyber criminale apre una sessione verso il vero sito della banca e utilizza, quasi in real time, queste informazioni per effettuare azioni dispositive.
Keylogger	*Malware* (o dispositivi hardware) in grado di registrare quello che la vittima digita sulla tastiera (o altrimenti inserisce), comunicando tali informazioni all'attaccante.
Malvertising	Tecniche che utilizzano l'ambito della pubblicità on line come veicolo di diffusione di ***malware***.

Malware	Definizione generica di applicazioni finalizzate a arrecare in qualche modo danno alla vittima (ad esempio raccogliendo o intercettando informazioni, creando malfunzionamenti nei dispositivi sui quali sono presenti, criptando i file al fine di richiedere un riscatto per renderli nuovamente intellegibili…).
Man in the browser	Tecnica che consente di intercettare le informazioni trasmesse dalla vittima, quali le credenziali di accesso al sito di una banca, al fine di poterle riutilizzare.
Memcached	Software spesso usato sui server web per effettuare caching di dati e per diminuire il traffico sul database o sul backend. Il server memcached è pensato per non essere esposto direttamente su Internet, per questo nella sua configurazione di default non richiede autenticazione e risponde sia via TCP che via UDP.
MFU (Malicious File Upload)	Attacco ad un web server basato sul caricamento remoto di ***malware*** o più semplicemente di file di grandi dimensioni.
Mining	Creazione di nuova criptovaluta attraverso la potenza di calcolo degli elaboratori di una ***blockchain***.
MitC (Man in the Cloud) *Definizione coniata dall'azienda Imperva*	Tipo di attacco nel quale la potenziale vittima è indotta a installare del software malevolo attraverso meccanismi classici come l'invio di una mail contenente un link a un sito malevolo. Successivamente il malware viene scaricato, installato, e ricerca una cartella per la memorizzazione di dati nel cloud sul sistema dell'utente. Successivamente, il malware sostituisce il token di sincronizzazione dell'utente con quello dell'attaccante.
Mix-nets schemi	Tecnica utilizzata nell'ambito dell'*e-voting*. Gli schemi di voto mix-nets sono sistemi basati su insiemi di server con cui è possibile crittare e permutare i voti espressi, in modo da rendere pressoché impossibile ricostruire la coppia voto-elettore.
Mules	Soggetti che consentono di "convertire" attività illegali in denaro (cash out) ad esempio attraverso attività di riciclaggio.

NIS (Network and Information Security)	DIRETTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.
NTP (Network Time Protocol)	*Protocollo* che consente la sincronizzazione degli orologi dei dispositivi connessi ad una rete.
OSINT (Open Source INTelligence)	Attività di intelligence tramite la consultazione di fonti aperte di pubblico accesso.
OTP (One Time Password)	Dispositivo di sicurezza basato sull'uso di password utilizzabili per una sola volta, di norma entro uno spazio temporale limitato.
OT (Operation Technology)	Componenti hardware e software dedicati al monitoraggio ed alla gestione di asset fisici in ambito industriale, trasporti…
Payload	Letteralmente carico utile. Nell'ambito della sicurezza informatica è la parte di un ***malware*** che arreca danni.
Password hard-coded	Password inserite direttamente nel codice del software.
Pharming	Tecnica che consente di indirizzare la vittima verso un sito bersaglio simile all'originale (ad esempio un sito bancario) al fine di intercettare ad esempio le credenziali di accesso.
PHI (Protected Health Information)	Informazioni personali relative alla salute fisica o mentale di una persona fisica, comprese le relative valutazioni, cure… ed i relativi pagamenti, indipendentemente dalla forma o dal media utilizzato per la loro rappresentazione.
Phishing	Tecnica che induce la vittima, mediante una falsa comunicazione in posta elettronica, a collegarsi verso un sito bersaglio simile all'originale (ad esempio il sito di una banca) al fine di intercettare informazioni trasmesse, quali le credenziali di accesso.

Phone hacking	Attività di hacking che ha come oggetto i sistemi telefonici; ad esempio mediante l'accesso illegittimo a caselle vocali.
Ping flood:	Attacco basato sul continuo ping dell'indirizzo della macchina vittima. Se migliaia e migliaia di computer, che fanno parte di una botnet, effettuano questa azione continuamente, la vittima esaurirà presto le sue risorse.
Ping of Death	Attacco basato sull'inoltro di un pacchetto di ping non standard, forgiato in modo tale da mandare in crash lo stack di networking della macchina vittima.
PISP (Payment Initiation Service Provider)	Prestatori di servizi di disposizione di ordini che trasmettono un ordine di pagamento emesso da un cliente che detiene un conto online presso un Istituto di Credito a favore di un conto di un beneficiario o operatore commerciale (e-merchant).
Protocollo di comunicazione	Insieme di regole che disciplinano le modalità con cui i dispositivi connessi ad una rete si scambiano informazioni.
PSD2 Direttiva sui servizi di pagamento nel mercato interno	DIRETTIVA (UE) 2015/2366 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE che stabilisce le regole in base alle quali gli Stati membri distinguono le varie categorie di prestatori di servizi di pagamento.
Pulse Wave (o Hit & Run)	*Hit & Run (o Pulse wave)*
QTSP (Qualified Trust Service Provider)	Un ***prestatore di servizi fiduciari*** che presta uno o più servizi fiduciari qualificati e cui l'organismo di vigilanza assegna la qualifica di prestatore di servizi fiduciari qualificato.
Ransomware	*Malware* che induce limitazioni nell'uso di un dispositivo (ad esempio criptando i dati (crypto-ransomware), o impedendo l'accesso al dispositivo (locker-ransomware).

RDP (Remote Desktop Protocol)	Protocollo per la comunicazione remota fra computer (in particolare per le comunicazioni tra Terminal Server e il client Terminal Server).
Resource ransom	Tecnica di attacco che nel mondo cloud consiste nel tentare di bloccare l'accesso a risorse nel cloud compromettendo l'account cloud pubblico della vittima e tentando di cifrare o limitare in altro modo l'accesso al maggior numero possibile di risorse cloud.
Rootkit	*Malware* che consente sia il controllo occulto di un dispositivo, sia di nascondere la presenza propria e di altri malware.
Sandboxing	Ambiente protetto nel quale è possibile testare applicazioni senza compromettere l'intero sistema informatico.
Scrubbing center	Letteralmente centro di pulizia. In uno Scrubbing center il traffico di rete viene analizzato e "ripulito" delle componenti dannose.
Service Abuse	Tecniche di attacco in ambito VOIP in cui si utilizza l'infrastruttura della rete VOIP della vittima per generare traffico verso numerazioni particolari a tariffazione speciale.
Side-channel attacks	Tecnica di attacco nella quale l'attaccante tenta di posizionare una macchina virtuale sullo stesso server fisico della potenziale vittima.
SIEM (Security information & event management)	Sistema per la raccolta e normalizzazione dei log e per la correlazione degli eventi finalizzato al monitoraggio della sicurezza.
Smart contracts	Programmi per computer in esecuzione sul registro generale; sono diventati una caratteristica fondamentale delle ***blockchain*** di seconda generazione come Ethereum o NEO. Questo tipo di programmi sono attualmente utilizzati per facilitare, verificare o applicare regole tra le parti in occasione delle ICO o nella fruizione dei servizi offerti dagli operatori del settore, consentendo l'elaborazione diretta e le interazioni con altri contratti intelligenti.

SOC (Security Operations Center)	Centro la gestione delle funzionalità di sicurezza e per il monitoraggio degli eventi che potrebbero essere una fonte di minaccia.
Social engineering	Tecniche di attacco basate sulla raccolta di informazioni mediante studio/interazione con una persona.
Social Threats	Versione VOIP del furto d'identità finalizzata a impersonare un utente e perpetrare azioni malevole con lo scopo di arrecare danni; ad esempio, furto di informazioni aziendali riservate.
Spear phishing	*Phishing* mirato verso specifici soggetti.
Spoofing	Modifica di una informazione, ad esempio l'indirizzo mittente di un pacchetto IP.
Spyware	*Malware* che raccoglie informazioni sul comportamento della vittima trasmettendole all'attaccante.
SQL injection	Tecnica di attacco basata sull'uso di query indirizzate a database SQL che consentono di ricavare informazioni ed eseguire azioni anche con privilegi amministrativi.
SSDP (Simple Service Discovery Protocol)	*Protocollo* che consente di scoprire e rendere disponibili automaticamente i dispositivi di una rete.
SSH (Secure Shell)	*Protocollo* cifrato che consente l'interazione remota con apparati di rete o di server permettendone, ad esempio, l'amministrazione.
STIX (Structured Threat Information eXpression)	Linguaggio strutturato che consente la descrizione e condivisione automatizzata di cyber threat intelligence (CTI) fra organizzazioni, utilizzando il protocollo *TAXII*.

TAXII (Trusted Automated eXchange of Indicator Information)	Protocollo che consente lo scambio (in HTTPS) di CTI (cyber threat intelligence) descritti mediante ***STIX***.
TCP Synflood	Tipo di attacco nel quale tramite pacchetti SYN in cui è falsificato l'IP mittente (spesso inesistente) si impedisce la corretta chiusura del three-way handshake, in quanto, nel momento in cui il server web vittima invia il SYN/ACK, non ricevendo alcun ACK di chiusura, essendo l'IP destinatario inesistente, lascerà la connessione "semi-aperta". Con un invio massivo di pacchetti SYN in concomitanza ad un alto tempo di timeout delle connessioni, il buffer del server verrebbe presto saturato, rendendo il server impossibilitato ad accettare ulteriori connessioni TCP, anche se legittime.
TDM (Time-division multiplexing)	Tecnica che consente la condivisione, da parte di più dispositivi, di un canale di comunicazione per un tempo limitato predefinito.
Tecniche di riflessione degli attacchi (DRDoS – Distributed Reflection Denial of Service)	La tecnica più diffusa sfrutta host esposti sulla Big Internet come riflettori del traffico a loro indirizzato sfruttando le vulnerabilità intrinseche ad alcuni protocolli quali NTP o DNS.
Tecniche di amplificazione degli attacchi	Sfruttando lo ***spoofing*** dell'indirizzo IP di una vittima, un utente malintenzionato può inviare piccole richieste ad un host vulnerabile inducendolo ad indirizzare le risposte alla vittima dell'attacco. Ad esempio nel caso del ***protocollo NTP*** si può amplificare la potenza dell'attacco anche di 600 volte.
Telnet	Protocollo utilizzato per la gestione di host remoti, accessibile da riga di comando.

TLS (Transport Layer Security)	Protocollo per la comunicazione sicura su reti TCP/IP successivo al SSL (Secure Sockets Layer).
TOR	Rete di dispositivi che consente l'uso dei servizi internet in modalità anonima (www.torproject.org).
Trojan horse	*Malware* che si installa in modo occulto su un dispositivo con diverse finalità, quali ad esempio raccogliere informazioni.
TSP (Trust Service provider)	Una persona fisica o giuridica che presta uno o più servizi fiduciari, o come ***prestatore di servizi fiduciari qualificato*** o come prestatore di servizi fiduciari non qualificato.
UDP Flood	Il *protocollo* UDP non prevede l'instaurazione di una connessione vera e propria e possiede tempi di trasmissione/risposta estremamente ridotti. Tali condizioni offrono maggiori probabilità di esaurire il buffer tramite il semplice invio massivo di pacchetti UDP verso l'host target dell'attacco.
UpnP (Universal Plug and Play)	*Protocollo* di rete che consente la connessione e condivisione automatica di dispositivi ad una rete.
UBA (User Behavior Analytics)	Tecnologia atta ad apprendere il "normale" comportamento degli utenti di un sitema informativo mediante l'analisi di rilevanti quantità di dati (log…), e di segnalare successivamente il verificarsi di attività anomale messe in atto dagli stessi.
Volume Boot Record	Il VBR è una piccola porzione di disco allocata all'inizio di ciascuna partizione che contiene codice per caricare in memoria e avviare il sistema operativo contenuto nella partizione.
Vulnerabilità	Debolezza intrinseca di un asset (ad esempio un'applicazione software o un *protocollo* di rete) che può essere sfruttata da una minaccia per arrecare un danno.
Watering Hole	Attacco mirato nel quale viene compromesso un sito web al quale accede normalmente l'utente target dell'attacco.

Weaponization	Modifica di file e documenti per trasformali in vere e proprie armi per colpire i sistemi e gli utenti e per favorire l'installazione di codice malevolo.
Web Injects	Tecnica che consente di mostrare nel browser dell'utente informazioni diverse rispetto a quelle originariamente presenti sul sito consultato.
Whaling	Letteralmente "caccia alla balena"; è un'ulteriore specializzazione dello ***spearphishing*** che consiste nel contattare una persona interna all'azienda spacciandosi per un dirigente della stessa. Di solito si tratta di truffe finanziarie e il bersaglio è l'amministrazione con l'obiettivo di indurre la vittima a eseguire, con l'inganno, un pagamento a beneficio del truffatore.
XSS (Cross Site Scripting)	Vulnerabilità che sfrutta il limitato controllo nell'input di un form su un sito web mediante l'uso di qualsiasi linguaggio di scripting.
Zero-day attach	Attacco compiuto sfruttando ***vulnerabilità*** non ancora note/risolte.
Zero Trust	Paradigma i cui principi fondamentali sono: si assuma che l'ambiente sia ostile, non si distingua tra utenti interni ed esterni, non si assuma "trust" (da cui il nome), si eroghino applicazioni solo a device e utenti riconosciuti e autenticati, si effettuino analisi dei log e dei comportamenti utente. In pratica occorre trattare tutti gli utenti nello stesso modo, utenti della stessa azienda o esterni, che siano nel perimetro della rete aziendale o meno, che i dati a cui vogliono accedere siano dentro l'azienda o da qualche parte nel cloud.

Gli autori del Rapporto Clusit 2019

Andrea Antonielli, laureato in Giurisprudenza presso l'Università degli Studi di Milano nel 2016, è Ricercatore presso gli Osservatori Digital Innovation del Politecnico di Milano e si occupa dei temi connessi all'Information Security & Privacy, con particolare focus sulla normativa europea in materia di protezione dei dati personali.

Liviu Arsene è un Senior E-threat Analyst per Bitdefender con una grande esperienza nella sicurezza. Ha lavorato a stretto contatto e si è interfacciato spesso con team di sviluppo di più società, mentre il suo precedente ruolo di Product Manager gli ha consentito di approfondire le sue conoscenze sullo stack tecnologico di Bitdefender. Segnalando le tendenze globali e gli sviluppi nella sicurezza informatica, si concentra soprattutto sulle epidemie di malware e gli incidenti di sicurezza, mentre coordina gli uffici tecnici e di ricerca. Grande appassionato di tecnologie e gadget innovativi, ma anche di applicazioni di sicurezza e del loro impatto strategico a lungo termine. Come orgoglioso proprietario del segreto dell'energia eterna, tra le sue passioni principali possiamo annoverare le nuove tecnologie e smontare i gadget per scoprire come funzionano. Quando non è online, adora nuotare o fare jogging.

Luca Bechelli, Information Security & Cyber Security Advisor, svolge dal 2000 consulenza per progetti nazionali ed internazionali su tematiche di Compliance, Security Governance, Risk Management, Data Protection, Privilege Management, Incident Handling e partecipa alla progettazione ed al project management per attività di system integration. Svolge attività di ricerca e sviluppo tramite collaborazioni con enti di ricerca e associazioni, nell'ambito delle quali ha svolto docenze per master post-laurea. Ha collaborato alla realizzazione di numerosi studi e pubblicazioni di riferimento per il settore. Membro del Consiglio Direttivo del Clusit dal 2007 al 2018, è membro del Comitato Scientifico Clusit, con delega su Tecnologie e Compliance. Svolge attività di divulgazione su tematiche di sicurezza IT,

mediante la partecipazione a convegni, la pubblicazione di articoli su testate generaliste o di settore e la partecipazione a gruppi di lavoro.

Danilo Benedetti inizia la sua carriera nel 1998 come consulente, occupandosi principalmente di telecomunicazioni a larga banda, su reti fisse e mobili. Inizia ad occuparsi di temi di sicurezza nel nel 2005 e nel 2010 consegue la certificazione CISM. Nel 2009 inizia a lavorare come Solution Architect IT per HP ES (oggi DXC Techology), e dal 2013 si occupa principalmente di sicurezza all'interno dell'organizzazione Enterprise Security Services, con il compito di disegnare soluzioni di sicurezza per i clienti DXC, sia in ambito consulenziale che tecnologico. In anni recenti ha partecipato al dibattito sulla sicurezza presentando diversi articoli per Limes, Agenda Digitale e Cybersecurity 360° e partecipando, in qualità di speaker a diversi eventi sulla sicurezza informatica. Danilo ha sviluppato i suoi 15+ anni di esperienza anche in contesti internazionali, con esperienze consulenziali e progettuali in Italia, Francia, Germania, Indonesia ed Africa Occidentale. Le aree di maggiore focalizzazione riguardano il monitoraggio e la risposta agli incidenti di sicurezza ed il rispetto della compliance, in particolare negli ambiti Privacy e PCI-DSS, oltre ai temi legati al legame tra scurezza ed Intelligenza Artificiale.

Battista Biggio è ricercatore presso il PRA Lab, nel Dipartimento di Ingegneria Elettrica ed Elettronica dell›Università di Cagliari. È socio fondatore di Pluribus One s.r.l., azienda che sviluppa soluzioni innovative per la cybersecurity basate su algoritmi di intelligenza artificiale robusti e trasparenti. I suoi interessi di ricerca riguardano lo studio della sicurezza delle tecniche di machine learning in diversi contesti applicativi, tra i quali la sicurezza informatica e il riconoscimento biometrico. Su questi argomenti, ha pubblicato oltre 70 articoli su atti di conferenza e riviste internazionali, collaborando con svariati gruppi di ricerca a livello internazionale, È membro dei comitati di programma delle conferenze più prestigiose del suo settore di ricerca (ICML, IJCAI, AAAI, ACM CCS, IEEE Symp. S&P) e svolge regolarmente attività di revisore per le riviste e le conferenze principali nell'ambito dell'intelligenza artificiale e della sicurezza informatica. È Editore Associato delle riviste IEEE TNNLS e IEEE CIM, Chair del comitato tecnico IAPR su Statistical Pattern Recognition Techniques, Senior Member dell'IEEE e membro dell'ACM e dello IAPR.

Piero Bologna, attualmente consulente legale presso p4i - partners4innovation, dopo la laurea in giurisprudenza a Trieste ed un master ad Hong Kong ha lavorato come in-house counsel per un gruppo multinazionale italiano. Da sempre appassionato di nuove tecnologie, scrive articoli sul tema blockchain e smart contracts.

Giancarlo Butti ha acquisito un master in Gestione aziendale e Sviluppo Organizzativo presso il MIP Politecnico di Milano. Si occupa di ICT, organizzazione e normativa dai primi anni 80. Auditor ed esperto di sicurezza e privacy ha all'attivo oltre 700 articoli e collaborazioni con oltre 30 testate. Ha pubblicato 21 fra libri e white paper alcuni dei quali utilizzati come testi universitari; ha partecipato alla redazione di 11 opere collettive. Già docente del percorso professionalizzante ABI - Privacy Expert e Data Protection Officer in Banca di cui ha curato l'impianto ed il test finale è docente/relatore presso eventi di ISACA/AIEA, ORACLE/CLUSIT, ITER, INFORMA BANCA, CONVENIA, CETIF, IKN, Università Statale di Milano, Università degli Studi Suor Orsola Benincasa – Napoli…Partecipa ai gruppi di lavoro di ABI LAB, ISACA/AIEA, Oracle Community for Security, UNINFO, Assogestioni... È fra i coordinatori di europrivacy.info e socio di CLUSIT, ISACA, BCI. Ha inoltre acquisito le certificazioni/qualificazioni LA BS7799, LA ISO/IEC27001, CRISC, ISM, DPO, CBCI, AMBCI.

Davide Carboni è un consulente informatico e dottore di ricerca specializzato in innovazione della finanza e nelle nuove applicazioni della crittografia in ambiti finanziari e sociali. Ricopre anche il ruolo di senior blockchain architect presso Smart Valor AG, una società svizzera che sta sviluppando un digital marketplace per investimenti alternativi su blockchain. È stato senior technologist del CRS4 e in questa veste è stato anche il lead organizer della prima Blockchain and DLT Scientific School organizzata in Italia, che si è svolta a Pula dal 12-15 Giugno 2018. Ha svolto attività di ricerca e sviluppo per conto degli Intel Labs Europe, all'interno dello staff dell'Internet of Things System Research Lab (IOTSRL) di Dublino e distaccato presso l'Imperial College London si è occupato anche di machine learning nel settore nel settore della domotica. Ha pubblicato oltre trenta tra articoli scien-

tifici e paper in atti di conferenze internazionali di tipo peer reviewed. È molto attivo nella divulgazione del fenomeno criptovalute presso il grande pubblico ed è autore di alcuni libri sul tema.

Nunzia Ciardi La Dott.ssa Nunzia CIARDI, Dirigente Superiore della Polizia di Stato, è il Direttore del Servizio Polizia Postale e delle Comunicazioni. Laureata in giurisprudenza, con una pregressa pluriennale esperienza, maturata prima come Direttore della I Divisione del Servizio Polizia Postale e successivamente come Dirigente del Compartimento Polizia Postale e delle Comunicazioni del Lazio, coordina attualmente le unità specializzate della Polizia di Stato nel contrasto al cyberterrorismo, al financial cybercrime, alla pedopornografia on-line, alla tutela delle infrastrutture critiche informatiche nazionali, all'hacking e ai crimini informatici in generale. Partecipa, come membro nazionale in rappresentanza dell'Italia, alle riunioni dell'European Union Cybercrime Taskforce di Europol; ha preso parte alla realizzazione del progetto europeo EU-OF2CEN per l'adozione di strategie comuni contro il crimine organizzato nel settore delle frodi on-line. È rappresentante del Ministero dell'Interno in seno al Nucleo Sicurezza Cibernetica ed al Tavolo Tecnico Cyber. È membro dell'Unità Informativa Scommesse Sportive, del "Gruppo Nazionale di Cybersecurity per i Servizi Sanitari" e del Comitato Scientifico del Master Universitario di II Livello in "Homeland Security - X edizione" - Università Campus Bio-Medico di Roma. È componente dell'Organismo permanente di supporto al "Centro di coordinamento per le attività di monitoraggio, analisi e scambio permanente di informazioni sul fenomeno degli atti intimidatori nei confronti dei giornalisti".
Ha svolto attività di docenza presso diverse scuole di Polizia, presso la scuola Ufficiali dei Carabinieri, presso l'Istituto Alti Studi per la Difesa, nonché presso diverse università ed enti, sulle principali attività di competenza della Specialità. Autrice di libri e pubblicazioni a carattere scientifico in materia di cybercrime, ha collaborato alla redazione del Rapporto Clusit 2018 e 2019.

Garibaldi Conte, dopo aver conseguito la Laurea in Scienze della Informazione, ha lavorato per circa 20 anni in CSELT, Telecom Italia, Tibercom ed Elitel dove ha sviluppato una significativa esperienza professionale in ambiti ICT e Sicurezza ICT gestendo progetti complessi e partecipando allo start up di numerose iniziative. Da circa 15 anni opera come consulente freelance nell'ambito della Sicurezza ICT collaborando con le principali società di consulenza operanti in tale mercato. Ha gestito importanti progetti di sicurezza ICT su varie tematiche quali Compliance, Risk Management, Incident Handling per conto di grandi aziende na-

zionali e internazionali operanti in vari settori (Finanza, Telecomunicazioni, Pubblica Amministrazione, …). È membro del Comitato Scientifico del Clusit.

Rodolfo D'Agostino, nato nel 1979, si laurea in Informatica presso il Polo Didattico e di Ricerca di Crema. Inizia la carriera nel mondo IT occupandosi di architetture di networking ad alte prestazioni e load balancing, VoIP carrier-grade e MPLS. Successivamente sviluppa un interesse per il mondo della sicurezza che si è evoluto nel tempo. Nel 2008 entra a far parte del team di Akamai come Solutions Engineer per il mercato italiano e attualmente ricopre il ruolo di Principal Partner Enablement Manager per il Sud Europa con funzioni di Subject Matter Expert per i prodotti di Sicurezza Web e Applicativa.

Pasquale Digregorio (GCIH, GCTI) è un ex Ufficiale dell'Esercito Italiano, attualmente vice capo del CERT della Banca d'Italia. Ha frequentato la Scuola Militare Teuliè, l'Accademia Militare di Modena e la Scuola di Applicazione di Torino, dove si è laureato a pieni voti in Ingegneria delle Telecomunicazioni. Ha conseguito un master di secondo livello in Sistemi avanzati di comunicazione e localizzazione satellitare ed uno in Protezione Strategica del Sistema Paese. È autore di alcune pubblicazioni e di un brevetto internazionale sviluppato in collaborazione con il Centro Ricerche Telecom Italia Lab. Durante la sua ventennale esperienza militare ha prestato servizio presso l'11° Rgt. Trasmissioni, presso il Comando C4 Difesa occupandosi di Cyber Defence e controlli di sicurezza e presso la Presidenza del Consiglio dei Ministri in ambito Cyber Intelligence. Ha fatto parte di diverse commissioni ed organismi permanenti in seno alla NATO. Ha svolto attività di docenza presso la Scuola di Telecomunicazioni delle Forze Armate, la Scuola del DIS e la Società Italiana per l'Organizzazione Internazionale.

Luca Dinardo, laureato in Sicurezza dei sistemi e delle reti informatiche presso l'Università degli Studi di Milano nel 2008, è consulente in ambito Cyber Security da 10 anni. Lavora in Lutech dal 2015, specializzato in tematiche di Cyber Security in contesti CERT e SOC, si occupa attivamente di Cyber Threat Intelligence, Malware & Threat Analysis, Incident Response e Cyber Deception. Svolge attività di ricerca e sviluppo mirate all'analisi ed al contrasto di fenomeni legati al Cyber Crime.

Luca Dozio, laureato in Ingegneria Gestionale al Politecnico di Milano, oggi lavora come ricercatore alla School of Management del Politecnico di Milano negli Osservatori Digital Innovation sui temi della Cloud Transformation e Information Security. Aiuta le imprese e le pubbliche amministrazioni a comprendere le implicazioni del digitale, affiancandole nei processi decisionali con analisi di mercato e progetti di consulenza dedicati.

Giorgia Dragoni si è laureata in Ingegneria Gestionale al Politecnico di Milano, indirizzo Manufacturing & Management, con una Tesi sull'evoluzione di ruoli e competenze all'interno delle Direzioni ICT. È Ricercatrice presso gli Osservatori Digital Innovation del Politecnico di Milano e si occupa dei temi connessi all'Information Security & Privacy e ai Big Data Analytics.

Gabriele Faggioli, legale, è amministratore delegato di Partners4innovation S.r.l. (a Digital 360 Company di cui è socio e amministratore). È Presidente del Clusit. È Responsabile Scientifico dell'Osservatorio Security&Privacy del Politecnico di Milano. È Adjunct Professor del MIP – Politecnico di Milano. È membro del Gruppo di Esperti sui contratti di cloud computing della Commissione Europea. È specializzato in contrattualistica informatica e telematica, in information & telecommunication law, nel diritto della proprietà intellettuale e industriale e negli aspetti legali della sicurezza informatica, in progetti inerenti l'applicazione delle normative inerenti la responsabilità amminstrativa degli enti e nel diritto dell'editoria e del markerting. Ha pubblicato diversi libri fra cui, da ultimo, "I contratti per l'acquisto di servizi informatici" (Franco Angeli), "Computer Forensics" (Apogeo), "Privacy per posta elettronica e internet in azienda" (Cesi Multimedia) oltre a innumerevoli articoli sui temi di competenza ed è stato relatore a molti seminari e convegni.

Roberto Fontana è informatico, nasce come analista programmatore nel 2001 per poi specializzarsi nella Information Security. Da oltre 15 anni è nel settore TLC e dal 2008 fa parte dell'unità antifrode di Fastweb, dove si occupa di prevenzione e gestione delle frodi in ambito telefonico, con una particolare attenzione alle tematiche di Cyber Security.

Sergio Fumagalli è Partner di P4I, società di management consulting del Gruppo Digital360, con responsabilità per le relazioni istituzionali. È membro del Comitato Scientifico di Clusit e responsabile delle relazioni con l'Autorità di Controllo. In precedenza ho ricoperto ruoli di responsabilità in diverse realtà aziendali e istituzionali, tra cui: Vice-Presidente del Cda e Membro e poi Presidente dell'OdV, d.lgs. 231/01, di Webank Spa, oggi Gruppo BancoBPM; Consulente del Garante per la protezione dei Dati Personali (2002-2004); Deputato alla Camera dei Deputati nella XIII Legislatura, Segretario della Commissione Attività Produttive; Project manager, team manager e sales manager - Digital Equipment Corporation. (1984-2001). È autore di diverse pubblicazioni sui temi legati alla protezione dei dati personali. Si è laureato in Fisica presso l'Università di Milano.

Boris Giannetto lavora nel CERT della Banca d'Italia e si occupa di *cyber intelligence*. Ha *expertise* su analisi strategica e *public policy*. Sempre in Banca d'Italia, si è occupato di *cyber resilience* e ha ricoperto il ruolo di esperto per il rischio operativo; per un breve periodo è stato impiegato presso l'UIF. In precedenza, ha lavorato, tra l'altro, alcuni anni per Telecom Italia S.p.A. (TIM) – *Public & Regulatory Affairs*, occupandosi di strategia regolamentare e *public policy*. Precedenti esperienze professionali nel settore privato in ambito *Legal* e Affari Esteri. *Background* in Istituzioni quali MAECI-UNODC, Parlamento Italiano e UNICRI, con *focus* su temi di sicurezza. Quanto agli studi, ha conseguito la Laurea con Lode in Scienze Politiche Internazionali presso La Sapienza di Roma, con tesi su regolamentazione e comunicazioni elettroniche; maturità classica con massima votazione; parla alcune lingue. Negli ultimi anni, ha approfondito in particolare tematiche relative a sistemi complessi adattativi (CAS), OSINT, HUMINT e *cyber counterintelligence*.

Paolo Giudice è segretario generale del CLUSIT. Negli anni 80 e 90 ha svolto attività di consulenza come esperto di gestione aziendale e rischi finanziari. L'evoluzione del settore IT, che ha messo in evidenza le carenze esistenti in materia di Security, lo ha spinto ad interessarsi alla sicurezza informatica e, nel luglio 2000, con un gruppo di amici, ha fondato il CLUSIT. Dal 2001 al 2008 ha coordinato il Comitato di Programma di Infosecurity Italia e dal 2009 coordina il Comitato Scientifico del Security Summit. Dal 2011 coordina il Comitato di Redazione del Rapporto Clusit. Paolo è Partner di C.I.S.C.A. (Critical Infrastructures Security Consultants & Analysts) a Ginevra.

Federico Griscioli è Information and Cyber Security Advisor. Ha conseguito una laurea in Ingegneria delle Telecomunicazioni e svolto un dottorato di ricerca in Ingegneria Informatica inerente alla sicurezza informatica di sistemi di controllo industriali. Ha esperienze di ricerca che lo hanno portato a pubblicazioni nazionali ed internazionali su tematiche di cybersecurity e networking. Si occupa anche di ethical hacking e blockchain. Ha una passione per il project management che lo porta a collaborare attivamente con il PMI (Project Management institute) Central Italy Chapter.

Ettore Guarnaccia Manager strategico e professionista di ICT e cyber security, certificato CGEIT, CISSP, C|CISO, M_o_R e Lead Auditor EN ISO 27001, esperto di normative e vigilanza bancaria in ambito IT, opera da oltre 20 anni nel settore e ha ricoperto incarichi di responsabilità in importanti realtà bancarie italiane e internazionali. Attualmente Senior Manager della funzione cyber security nella più grande banca italiana, in precedenza è stato CISO e responsabile del governo del sistema informativo e delle esternalizzazioni IT del Gruppo Banca Popolare di Vicenza. Da anni è educatore e formatore sulla sicurezza dei minori negli istituti scolastici, nonché divulgatore e sensibilizzatore in eventi pubblici indirizzati agli adulti. Padre di un nativo digitale, nel 2016 ha lanciato il progetto "Generazione Z" per la rilevazione dell'esperienza online e dei fattori di rischio dei minori nell'uso delle moderne tecnologie digitali e nel 2018 ha pubblicato il libro "Generazione Z – Fotografia statistica e fenomenologica di una generazione ipertecnologica e iperconnessa" su cyberbullismo, dipendenza tecnologica, adescamento online e molto altro ancora, con il contributo di altri professionisti e la prefazione di Gigi Tagliapietra, presidente onorario del Clusit.

Paola Meroni è entrata in Vodafone Italia nel 2000 passando nel 2006 nel dipartimento di Corporate Security, ICT Security and Fraud Management e nel 2013 nel dipartimento di Technology Security, dove si è occupata di ICT Security, di Governance e di Compliance alla normativa Privacy e Sox. Dall'aprile 2017 è Information Security and Compliance Expert in Vodafone Automotive, dove, nel settore IoT e specificatamente Automotive, si occupa di misure di sicurezza infrastrutturali e applicative oltre che di Governance e Compliance normativa: attualmente è in particolare impegnata nel condurre le attività necessarie a garantire l'adeguamento al nuovo Regolamento Europeo in materia di Protezione dei Dati Personali (GDPR). Nelle sue precedenti esperienze professionali ha lavorato per anni nell'Information Technology come specialista di sistemi e networking e nel progetto di servizi e infrastrutture di sicurezza. Paola è laureata in Ingegneria Elettronica al Politecnico di Milano, ed è in possesso delle certificazioni CISSP, CCSK, CEH, CHFI, Cobit5 e dei requisiti necessari per l'attività di ISO 27001 Lead Auditor. È socio Clusit dal 2006 e Isaca dal 2016.

Gastone Nencini vanta una carriera significativa nel settore IT, iniziata oltre 25 anni fa con un'esperienza come programmatore presso Elsi Informatica e proseguita in Genesys come Technical Manager. Nel 1998 Nencini approda in Trend Micro Italia dove viene nominato Senior Sales Engineer per il Centro e Sud Italia, per passare successivamente a un ruolo di maggiore responsabilità e prestigio, diventando prima Technical Manager Developing BU (Italia, Benelux e Paesi Scandinavi) per poi focalizzarsi sul mercato Italiano con l'incarico di Senior Technical Manager Italy. Nel 2012 Gastone diventa Technical Director Southern Europe e a Gennaio 2015 è ufficialmente nominato anche Country Manager Italia. Durante questi anni in Trend Micro, Gastone Nencini ha gestito e supervisionato una serie di importanti progetti di sicurezza per i maggiori clienti, fra cui, a livello italiano, si possono citare: Telecom, Fiat, Poste, Vodafone, Ferrari, Banca Nazionale del Lavoro, Banca Intesa San Paolo, Telethon. Nencini ha, inoltre, introdotto servizi innovativi di assistenza e supporto per i clienti Enterprise e per il canale di rivenditori.

Alessio L.R. Pennasilico, Information & Cyber Security Advisor, Security Evangelist, noto nell'hacker underground come -=mayhem=-, è internazionalmente riconosciuto come esperto dei temi legati alla gestione della sicurezza delle informazioni e delle nuove tecnologie. Per questa ragione partecipa da anni come relatore ai più rilevanti eventi di security italiani ed internazionali ed è stato intervistato dalle più prestigiose testate giornalistiche, radio e televisioni nazionali ed internazionali. All'interno di P4I, per importanti Clienti operanti nei più diversi settori di attività, sviluppa progetti mirati alla riduzione dell'impatto del rischio informatico/cyber sul business aziendale, tenendo conto di compliance a norme e standard, della gestione del cambiamento nell'introduzione di nuovi processi ed eventuali tecnologie correlate. Credendo che il cyber risk sia un problema organizzativo e non un mero problema tecnologico, Alessio da anni aiuta il top management, lo staff tecnico e l'organizzazione nel suo complesso a sviluppare la corretta sensibilità in merito al problema, tramite sessioni di awareness, formazione e coaching. Alessio è inoltre membro del Comitato Scientifico di Clusit, Presidente di Associazione informatici Professionisti - AIP, membro del Comitato di Schema UNI 11506 di Kiwa Cermet e Vice Presidente del Comitato di Salvaguardia per l'Imparzialità di LRQA, l'ente di certificazione dei Lloyd's.

Andrea Piazza ricopre il ruolo di WW Cybersecurity Architect, Chief Security Advisor in Microsoft, collaborando allo sviluppo dei servizi di cybersecurity di consulenza e supporto, alla formazione dei team di consulenza e al miglioramento della qualità dei progetti di sicurezza e delle attività di risposta agli incidenti. Nei 17 anni in cui ha lavorato in Microsoft, ha svolto il ruolo di Technical Account Manager e successivamente di Security Premier Field Engineer, dove ha ricoperto mansioni di crescente responsabilità da Tech Lead Italia, a Tech Lead EMEA, a Technology Manager EMEA. Dal 2014 è stato National Security Officer della filiale italiana di Microsoft, dove ha coordinato le attività volte a promuovere la consapevolezza e l'adozione delle tecnologie di sicurezza da parte dei clienti, gestendo i rapporti sulle tematiche di sicurezza e cybersecurity con le government élites, i leader accademici e i decisori pubblici, nonché con i responsabili e i team di sicurezza delle aziende italiane. A livello EMEA ha coordinato i servizi di sicurezza del supporto Microsoft, come Security Assessment, Workshop, attività di risposta agli incidenti e di remediation, si è occupato in prima persona dell'attività di formazione e aggiornamento degli engineer di sicurezza, e collaborato con i team di sviluppo dei servizi di sicurezza Microsoft. In Microsoft ha collaborato al whitepaper "Mitigating Pass-the-Hash Attacks and Other Credential Theft-Version 2". Collabora al Comitato di Redazione de "Il Documento Digitale", ed ha

partecipato alla redazione delle linee guida UNICRI 2015 per le PMI e ai rapporti CLUSIT 2016 e 2017. È certificato CISSP, ISO27001 Lead Auditor e ITIL.

Alessandro Piva si occupa da oltre dieci anni di ricerca sui temi dell'innovazione digitale. Dopo essersi laureato in Ingegneria delle Telecomunicazioni ed Ingegneria Gestionale al Politecnico di Milano, ha conseguito un Executive Master in Business Administration presso il MIP. Attualmente è Direttore di svariati Osservatori del Politecnico, quali l'Osservatorio Information Security & Privacy, l'Osservatorio Cloud Transformation, l'Osservatorio Artificial Intelligence e Responsabile della Ricerca dell'Osservatorio Big Data Analytics & Business Intelligence.

Domenico Raguseo è CTO della divisione IBM Security nel sud europa. Ha 20 anni di esperienza manageriale e 28 nel campo della cybersecurity in diverse aree. Domenico collabora con alcune università nell'insegnamento di Service Management e del Cloud Computing. Domenico è IBM Master inventor grazie a una moltitudine di brevetti e pubblicazioni in diverse discipline (Business Processes, ROI, Messages and Collaborations, Networking). Infine, è stato speaker su Sicurezza delle Informazioni, Service Management, Cloud computing, Energy Optimization e Smarter Planet in eventi nazionali e internazionali.

Marco Raimondi, nato nel 1987, si laurea in Ingegneria delle Telecomunicazioni presso il Politecnico di Milano. Ha iniziato la sua carriera nell'ambito IT per poi orientare la sua attività nel mondo commerciale, con un focus particolare sul mercato Enterprise. Dal 2012 ha lavorato presso Vodafone Italia dove ha ricoperto nella Business Unit Enterprise dapprima il ruolo di Presales e successivamente il ruolo di Marketing Product Manager nel mercato delle PMI. Dal 2017 in Fastweb, ricopre dapprima il ruolo di Marketing Product Manager in ambito security, quindi il ruolo di Marketing Manager responsabile dello sviluppo dei prodotti di Sicurezza, Cloud e IoT.

Il Col. **Giovanni Reccia** nel corso della sua carriera oltre ad aver comandato reparti della Guardia di Finanza impegnati nel contrasto al contrabbando ed ad aver svolto delicate indagini in materia di anticorruzione, evasione fiscale, riciclaggio ed attività di polizia giudiziaria e tributaria a carattere nazionale ed internazionale anche nei confronti di organizzazioni criminali di spicco, è stato Ufficiale di Stato Maggiore al Comando Generale della Guardia di Finanza presso l'Ufficio Legislativo e l'Ufficio Telematica. Plurilaureato, ha conseguito Master accademici. È abilitato alla professione di Avvocato, Revisore Legale dei Conti e Giornalista Pubblicista. Responsabile della Sicurezza IT della Guardia di Finanza dal 2009 al 2013, è stato Project Manager di informatica operativa. Comandante della GdF della Provincia di Latina dal 2013 al 2016. È stato, altresì, docente presso gli Istituti di formazione del Corpo ed Atenei Universitari, in materia di antiriciclaggio e criminalità organizzata. Ha inoltre all'attivo pubblicazioni in materia giuridica ed articoli su riviste specializzate. É titolato IASD - Alti Studi della Difesa. Dal 2017 riveste l'incarico di Comandante del Nucleo Speciale Tutela Privacy e Frodi Tecnologiche della Guardia di Finanza.

Luigi Rocco, Senior Consultant presso Communication Valley Reply, si occupa delle attività di prevenzione, analisi e gestione degli incidenti informatici e contrasto al cyber crime. Attualmente responsabile dell'erogazione e dell'ingegnerizzazione dei servizi antifrode e antiphishing per i clienti di Communication Valley Reply, collabora alla stesura del report mensile ABI Lab focalizzato sui principali fenomeni di phishing e malware rilevati a livello italiano.

Fabio Roli è professore ordinario di ingegneria informatica presso la facoltà di ingegneria dell›Università di Cagliari. Si occupa da più di vent'anni di intelligenza artificiale e cyber security. È il Direttore del laboratorio di ricerca PRA Lab sulle tecnologie e applicazioni dell'intelligenza artificiale alla sicurezza delle persone e dei sistemi informatici. Nel PRA Lab lavorano trenta persone fra ricercatori e docenti universitari. È socio fondatore di Pluribus One s.r.l. che sviluppa prodotti basati sulle tecnologie dell'intelligenza artificiale per la cyber security. È stato membro del NATO advisory panel for Information and Communications Security, NATO Science for Peace and Security. Ha coordinato decine di progetti

di ricerca e sviluppo sull'intelligenza artificiale e la cyber security, fra i quali i progetti europei CyberRoad e ILLBuster. Si interessa da più di dieci anni dei temi della sicurezza, della privacy e della trasparenza delle tecnologie dell'intelligenza artificiale.

Pier Luigi Rotondo lavora per il team di Technical Enablement IBM, concentrandosi sull'Identity e Access Management. Ha contribuito a molti progetti internazionali su soluzioni di sicurezza per l'Identity e l'Access Management, il Single Sign-on e la Security Intelligence. Con una la laurea in Scienze dell'Informazione da Sapienza - Università di Roma, Pier Luigi è coinvolto in attività accademiche sui temi di Sicurezza delle Informazioni in Corsi di Laurea e Master presso Sapienza - Università di Roma e l'Università di Perugia. Pier Luigi Rotondo è autore per il Clusit, e contribuisce permanentemente dal 2015 al Rapporto Clusit sulla Sicurezza ICT in Italia su temi di malware per frodi finanziarie presentando i risultati IBM.

Rodolfo Saccani, Security R&D Manager in Libra Esva, vive l'IT dal 1994, in qualità di sviluppatore, sistemista, consulente e project manager. Ha vissuto e lavorato negli USA e in Danimarca. Da sempre interessato al mondo della *security*, ha un'esperienza tecnica eterogenea: sistemi linux embedded, avionica sperimentale, telecomunicazioni sicure in ambienti ostili, TV connessa, controllo di processo e automazione industriale, ricerca clinica, piattaforme web SaaS. Per passione si occupa anche di sicurezza nel volo libero: consigliere alla sicurezza in FIVL (Federazione Italiana Volo Libero) dal 2007, è expert presso il CEN (Comitato Europeo di Normazione) e partecipa alla stesura delle norme europee di certificazione delle attrezzature da volo libero. In Libraesva coordina la ricerca e sviluppo per l'e-mail security.

Guido Sandonà è il Chief Information e Data Protection Officer in Bulgari, ha una consolidata esperienza di lavoro nel settore dei beni di lusso. Esperto in ambito di cybersecurity, Internet of Things, information technology, data privacy e compliance, è certificato Lead Auditor ISO 27001 e Certified Information System Auditor. È membro del Consiglio Direttivo del Clusit, all'interno del quale è referente della practice Blockchain.

Luca Sangalli si è laureato in Sicurezza dei sistemi e delle reti informatiche presso l'Università degli Studi di Milano nel 2015 e da allora lavora presso Lutech, occupandosi di tematiche di Cyber Security come Cyber Threat Intelligence Analyst, Researcher & Developer, specializzandosi in particolare nell'ambito Finance- ed Ethical Hacking. Si occupa anche di attività di ricerca e sviluppo in contesto antifrode.

Federico Santi, prima di assumere il ruolo attuale di Security Practice Leader per DXC in Italia, si è occupato dello sviluppo del mercato Cyber Sud Europa in Hewlett Packard Enterprise ed in precedenza ha lavorato in Arthur Andersen e Deloitte fino ad assumere il ruolo di Director dei Security Services. Il background economico e la lunga esperienza Big4 spiegano bene il suo approccio alla Sicurezza orientato al business ed al Risk Management. Ha sviluppato i suoi 20+ anni di esperienza in contesti internazionali, in particolare Italia, Spagna, Francia ed Africa ed ha seguito con una particolare attenzione i contesti del Settore Pubblico e dell'Energy & Utilities. Numerose le docenze e collaborazioni accademiche (Università Nazionale di Milano, La Sapienza, Tor Vergata) e le pubblicazioni (CLUSIT, Tor Vergata). Attiva partecipazione ai principali tavoli europei (collaborazione con la Commissione Europea per la NIS Platform e l'Organizzazione Europea per la Cyber Security - ECSO) e nazionali (CLUSIT, ISACA, AIEA).

Sofia Scozzari si occupa con passione di informatica dall'età di 16 anni. Ha lavorato come consulente di sicurezza presso primarie aziende italiane e multinazionali, curando gli aspetti tecnologici ed organizzativi di numerosi progetti. Già Chief Executive Officer de iDIALOGHI, negli anni si è occupata di Social Media Security, ICT Security Training e di Servizi di Sicurezza Gestita, quali Vulnerability Management, Mobile Security e Threat Intelligence. Membro del Comitato Scientifico di CLUSIT, è autrice di articoli e guide in tema di Social Media Security. È tra gli autori del paper "La Sicurezza nei Social Media" pubblicato nel 2014 dalla Oracle Community for Security. Fin dalla prima edizione contribuisce alla realizzazione del "Rapporto Clusit sulla Sicurezza ICT in Italia" curando l'analisi dei principali attacchi a livello internazionale e nazionale.

Claudio Telmon, Adviser e consulente da più di vent'anni nel campo della sicurezza e della gestione del rischio IT, è membro del Comitato Direttivo di Clusit.

Girolamo Tesoriere si è laureato in Ingegneria delle Telecomunicazioni presso il Politecnico di Bari.
10+ anni di esperienza nel settore delle TLC con una specializzazione nella consulenza sui servizi di Network Security e Cyber Security. Dopo aver lavorato per diversi anni come Technical Consultant in ambito networking e reporting operativo, nel 2013 partecipa allo start-up del Security Operations Center Enterprise di Fastweb. Ha lavorato per Eni come Cyber Security Engineer e al momento occupa la posizione di Enterprise Security Architect in Fastweb. Contribuisce allo sviluppo delle nuove soluzioni di sicurezza da erogare ai clienti TOP, grandi aziende e pubblica amministrazione.

Giuseppe Vaciago è iscritto all'Ordine degli Avvocati di Milano dal 2002. Le aree di specializzazione sono il diritto delle nuove tecnologie con particolare riferimento alla protezione dei dati personali e il diritto penale societario. Ha prestato la sua attività professionale per alcune importanti società nazionali e internazionali nel settore dell'information technology. È founder della Legal Tech Company LT42 S.r.l. Ha conseguito nel 2011 un PHD in Scienze Giuridiche all'Università degli Studi di Milano Bicocca affrontando il tema della Digital Forensics e delle investigationi digitali. È lead auditor ISO/IEC 27001/20013 (Information Security Management) e ha conseguito la certificazione UNI 11697/2017 come Responsabile della Protezione dei Dati Personali (DPO). È docente di informatica giuridica presso l'Università degli Studi dell'Insubria dal 2007. Ha frequentato in qualità di Visiting Scholar la Stanford Law School e la Fordham Law School di New York. Ha partecipato a numerosi convegni presso le più prestigiose Università italiane ed estere. È fellow presso il Nexa Center di Torino e presso il Cybercrime Institute di Colonia.

È membro del comitato editoriale della Rivista Digital Investigation edita da Elsevier. È autore di numerose pubblicazioni di carattere universitario tra cui "Computer Crimes" "Digital Forensics" e "Modelli di organizzazione gestione e controllo ai sensi del D.lgs. 231/01".

Alessandro Vallega lavora in Partners4Innovation sui temi di Information & Cyber Security, Integration and Change, Community Management. Prima del novembre 2018, è stato Business Development Director, Security e GDPR, in Oracle EMEA con la responsabilità di un team centrale e regionale sul tema del GDPR. Alessandro è nel direttivo di Clusit da diversi anni, ed è il fondatore e chairman della Oracle Community for Security. È coautore, editor o team leader di una decina di pubblicazioni su diversi temi legati alla sicurezza (misure, rischio, frodi, ritorno dell'investimento, compliances, privacy, cloud...) liberamente scaricabili dal sito Clusit (http://c4s.clusit.it). Nel 2015 ha fondato insieme a Clusit e ad Aused un osservatorio sul GDPR chiamato Europrivacy.info. Contribuisce fin dal 2012 ai Rapporti Clusit sulla Sicurezza ICT in Italia. Collabora con AISIS e APIHM. È gold member di ISACA.

Giancarlo Vercellino è Senior Research & Consulting Manager in IDC Italia, dove si occupa di ricerca, consulenza e advisory per clienti nazionali e internazionali del settore IT/TLC e per gli End-User. Prima di IDC, Giancarlo ha lavorato come market analyst e business manager presso diverse fondazioni e centri di ricerca applicata. Giancarlo ha insegnato economia presso il Politecnico di Torino.

Andrea Zapparoli Manzoni si occupa con passione di ICT dal 1997 e di Information Security dal 2003, mettendo a frutto un background multidisciplinare in Scienze Politiche, Computer Science ed Ethical Hacking. È stato membro dell'Osservatorio per la Sicurezza Nazionale (OSN) nel 2011-12 e del Consiglio Direttivo di Assintel dal 2012 al 2016, coordinandone il GdL Cyber Security. Dal 2012 è membro del Consiglio Direttivo di Clusit, e Board Advisor del Center for Strategic Cyberspace + Security Science (CSCSS) di Londra. Per oltre 10 anni è stato Presidente de iDialoghi, società milanese dedicata alla formazione ed alla

consulenza in ambito ICT Security. Nel gennaio 2015 ha assunto il ruolo di Head of Cyber Security Services della divisione Information Risk Management di KPMG Advisory. Dal giugno 2017 è Managing Director di un centro di ricerca internazionale in materia di Cyber Defense. È spesso chiamato come relatore a conferenze ed a tenere lezioni presso Università, sia in Italia che all'estero. Come docente Clusit tiene corsi di formazione su temi quali Cyber Crime, Mobile Security, Cyber Intelligence e Social Media Security, e partecipa come speaker alle varie edizioni del Security Summit, oltre che alla realizzazione di white papers (FSE, ROSI v2, Social Media) in collaborazione con la Oracle Community for Security. Fin dalla prima edizione (2011) del "Rapporto Clusit sulla Sicurezza ICT in Italia", si è occupato della sezione relativa all'analisi dei principali attacchi a livello internazionale, ed alle tendenze per il futuro.

Il Clusit, nato nel 2000 presso il Dipartimento di Informatica dell'Università degli Studi di Milano, è la più numerosa ed autorevole associazione italiana nel campo della sicurezza informatica. Oggi rappresenta oltre 500 organizzazioni, appartenenti a tutti i settori del Sistema-Paese.

Gli obiettivi

- Diffondere la cultura della sicurezza informatica presso le Aziende, la Pubblica Amministrazione e i cittadini.
- Partecipare alla elaborazione di leggi, norme e regolamenti che coinvolgono la sicurezza informatica, sia a livello nazionale che europeo.
- Contribuire alla definizione di percorsi di formazione per la preparazione e la certificazione delle diverse figure professionali operanti nel settore della sicurezza.
- Promuovere l'uso di metodologie e tecnologie che consentano di migliorare il livello di sicurezza delle varie realtà.

Le attività e i progetti in corso

- Formazione specialistica: i Webinar e i Seminari CLUSIT.
- Ricerca e studio: Premio "Innovare la Sicurezza delle Informazioni" per la migliore tesi universitaria arrivato alla 14ª edizione.
- Le Conference specialistiche: Security Summit (Milano, Treviso, Roma e Verona).
- Produzione di documenti tecnico-scientifici: i Quaderni CLUSIT e le Pillole di Sicurezza.
- I Gruppi di Lavoro: con istituzioni, altre associazioni e community.
- Progetto Scuole: la Formazione sul territorio.
- Rapporti Clusit: Rapporto annuale sugli eventi dannosi (Cyber crime e incidenti informatici) in Italia; analisi del mercato italiano dell'ICT Security; analisi sul mercato del lavoro.
- Il Mese Europeo della Sicurezza Informatica, iniziativa di sensibilizzazione promossa e coordinata ogni anno nel mese di ottobre in Italia da Clusit, in accordo con l'ENISA e con l'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione del Ministero dello Sviluppo Economico (ISCOM).

Il ruolo istituzionale

In ambito nazionale, Clusit opera in collaborazione con: Presidenza del Consiglio, numerosi ministeri, Banca d'Italia, Polizia Postale e delle Comunicazioni, Arma dei Carabinieri e Guardia di Finanza, Agenzia per l'Italia Digitale, Autorità Garante per la tutela dei dati personali, Autorità per le Garanzie nelle Comunicazioni, CERT Nazionale e CERT P.A., Università e Centri di Ricerca, Associazioni Professionali e Associazioni dei Consumatori, Confindustria, Confcommercio e CNA.

I rapporti internazionali

In ambito internazionale, Clusit partecipa a svariate iniziative in collaborazione con: i CERT, i CLUSI, Università e Centri di Ricerca in oltre 20 paesi, Commissione Europea, ENISA (European Union Agency for Network and Information Security), ITU (Interna-

tional Telecommunication Union), OCSE, UNICRI (Agenzia delle Nazioni Unite che si occupa di criminalità e giustizia penale), le principali Associazioni Professionali del settore (ASIS, CSA, ISACA, ISC², ISSA, SANS) e le associazioni dei consumatori.

Security Summit è il più importante appuntamento italiano per tutti coloro che sono interessati alla sicurezza dei sistemi informatici e della rete e, più in generale, alla sicurezza delle informazioni.

Progettato e costruito per rispondere alle esigenze dei professionals di oggi, Security Summit è un convegno strutturato in momenti di divulgazione, di approfondimento, di formazione e di confronto. Aperto alle esperienze internazionali e agli stimoli che provengono sia dal mondo imprenditoriale che da quello universitario e della ricerca, il Summit si rivolge ai professionisti della sicurezza e a chi in azienda gestisce i problemi organizzativi o legali e contrattuali dell'Ict Security.

La **partecipazione è libera e gratuita**, con il solo obbligo dell'iscrizione online.
Il Security Summit è organizzato dal Clusit e da Astrea, agenzia di comunicazione e organizzatore di eventi di alto profilo contenutistico nel mondo finanziario e dell'Ict.
Certificata dalla folta schiera di relatori (più di 600 sono intervenuti nelle scorse edizioni), provenienti dal mondo della ricerca, dell'Università, delle Associazioni, della consulenza, delle Istituzioni e delle imprese, la manifestazione è stata frequentata da oltre 16.000 partecipanti, e sono stati rilasciati circa 12.000 attestati validi per l'attribuzione di oltre 42.000 crediti formativi (CPE).

L'edizione 2019

La 11esima edizione del Security Summit si tiene a **Milano** dal 12 al 14 marzo, a **Treviso** il 23 maggio, a **Roma** il 5 giugno e a **Verona** il 3 ottobre.
Tra i temi più in evidenza per il 2019: Cyber Crime, Sicurezza del e nel Cloud, Intelligenza Artificiale, Blockchain, IoT, Industria 4.0., Compliance, GDPR.

Informazioni

- Agenda e contenuti: info@clusit.it, +39 349 7768 882.
- Altre informazioni: info@astrea.pro
- Informazioni per la stampa: press@securitysummit.it
- Sito web: www.securitysummit.it/
- Foto reportage: www.facebook.com/groups/64807913680/photos/?filter=albums
- Video riprese e interviste: www.youtube.com/user/SecuritySummit

In collaborazione con

Akamai
Experience the Edge

DXC.technology

FASTWEB

IBM

ORACLE

panda

TREND MICRO

30 YEARS OF INNOVATION

Research Partner

IDC
ANALYZE THE FUTURE

SECURITY
SUMMIT

www.securitysummit.it