Rapporto Clusit 2020

sulla sicurezza ICT in Italia

Indice

Prefazione di Gabriele Faggioli 5

Introduzione al Rapporto 7

Panoramica dei cyber attacchi più significativi del 2019 e tendenze per il 2020 . . . 9

- Analisi dei principali cyber attacchi noti a livello globale del 2019 15
- Analisi Fastweb della situazione italiana in materia di cyber-crime e incidenti informatici 39
- Stato della Cybersecurity nel Sud Italia 53
- Attività e segnalazioni della Polizia Postale e delle Comunicazioni nel 2019 65
- Le attività del Nucleo Speciale Tutela Privacy e Frodi Tecnologiche della Guardia di Finanza nel 2019 73
- Attività e segnalazioni del CERT Nazionale 77
- Il punto di vista del CERT-PA 87

Speciale FINANCE

- Elementi sul cybercrime nel settore finanziario in Europa 95
- Profilazione delle minacce e scambio di informazioni nelle attività di cyber intelligence 115

Il mercato italiano della Sicurezza IT: analisi, prospettive e tendenze secondo IDC 129

La sicurezza in ambito industriale 141

FOCUS ON 2020

- L'impatto dei deepfake sulla sicurezza delle organizzazioni economiche 149
- Business Continuity & Resilienza, leve fondamentali per una società sempre più globalizzata e digitalizzata 162
- Mobile App italiane: una lente di ingrandimento sul loro stato di salute e sulle vulnerabilità più diffuse 171
- Sicurezza nel settore sanitario – Perché gli ospedali sono così violabili 183
- Tendenze IT che avranno un impatto sui professionisti italiani nel 2020 187
- Email security: i trend rilevati in Italia nel corso del 2019 192

Glossario 203

Gli autori del Rapporto Clusit 2020 231

Descrizione CLUSIT e Security Summit 244

ASTREA Advanced Security, Training Research, Events Agency
Via Copernico, 38 - 20125 Milano

Prefazione

Scrivo queste righe in un momento drammatico per l'Italia e per molte zone del mondo.
Stiamo assistendo a una crisi senza precedenti che nessuno si sarebbe mai aspettato.
Mai avremmo pensato, anche solo un mese fa, che avremmo avuto di colpo scuole chiuse, attività commerciali ferme, necessità di rimanere chiusi in casa.
Si tratta di una prova senza precedenti.
Si tratta di una situazione senza precedenti. O perlomeno senza precedenti in cui una situazione di tale portata viene affrontata con le capacità di rilevazione e analisi, con le tecnologie, con le medicine, con il sistema sanitario, con i media, con i social dei giorni nostri.
È una grande lezione che servirà a tutto il mondo.
E aiuterà anche il nostro settore: la sicurezza informatica.
Aiuterà perché adesso si comprende appieno l'importanza del digitale.
Grazie al digitale le aziende stanno ancora, seppur solo alcune e magari a ritmo ridotto e ridottissimo, lavorando e producendo.

Grazie al digitale ognuno di noi ogni giorno mantiene relazioni non solo vocali, ma anche in "presenza" video.
Mai avrei pensato di organizzare dei video aperitivi né di insegnare a mia madre a giocare a carte online con i suoi amici.
Ma neanche avrei pensato di vedere mio figlio, e migliaia e migliaia di giovani fare lezione online, con una capacità di adattamento del sistema e delle persone incredibile.
Nella tragedia di chi muore, stiamo assistendo a una rivoluzione.
Il digitale è fondamentale per le imprese e per i cittadini.
E la sicurezza del digitale è essenziale ed è elemento base della nostra vita.
Questa crisi ci porta avanti di anni e ci insegna anche un'altra cosa: i peggiori scenari possono accadere. E potranno accadere anche sotto il profilo degli incidenti informatici.
Le crisi gravi, globali con impatto drammatico sulla salute e sulla economia possono accadere.
Questo è il motivo per cui bisogna arrivare pronti.
Essere pronti allo scenario peggiore.

Sono certo che usciremo da questo periodo più consapevoli dei punti di debolezza del paese e della economia mondiale ma sono anche certo che ne usciremo con maggiore capacità di comprensione della strada da percorrere anche sotto il profilo della sicurezza informatica.
Ed è per questo che anche in tempi di grave crisi noi del CLUSIT vogliamo dare un senso di continuità e di volontà di non fermare la macchina produttiva del paese ed è per questo motivo che per la prima volta presenteremo il nostro Rapporto non con la solita splendida plenaria al Security Summit ma online da remoto.

*** *** ***

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 ci fa giungere a una conclusione: il 2019 è stato un anno estremamente critico.

I dati li leggerete dalla introduzione in poi e al testo Vi lascio.
Ma quest'anno provate a leggere i dati pensando allo scenario peggiore. Pensando a quello che potrebbe accadere se quanto a volte si paventa come rischio estremo accadesse veramente.

I dati dicono chiaramente che i casi aumentano e i danni anche. E dicono che gli sciacalli purtroppo ci sono anche nei momenti più drammatici e approfittano anche di questa situazione che stiamo vivendo.

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 2020 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 300 articoli pubblicati nel 2019, 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

Nell'anno appena passato si è consolidata una discontinuità, si è oltrepassato un punto di non ritorno, tale per cui ormai ci troviamo a vivere ed operare in una dimensione differente, in una nuova epoca, in un "altro mondo", del quale ancora non conosciamo bene la geografia, gli abitanti, le regole e le minacce.
Gli attaccanti non sono più "hackers", e nemmeno gruppetti effimeri (più o meno pericolosi) di "artigiani" del cybercrime: sono decine e decine di gruppi criminali organizzati transnazionali che fatturano miliardi, multinazionali fuori controllo dotate di mezzi illimitati, stati nazionali con i relativi apparati militari e di intelligence, i loro fornitori e contractors, gruppi state-sponsored civili e/o paramilitari ed unità di mercenari impegnati in una lotta senza esclusione di colpi, che hanno come *campo di battaglia, arma e bersaglio* le infrastrutture, le reti, i server, i client, i device mobili, gli oggetti IoT, le piattaforme social e di instant messaging (e la mente dei loro utenti), su scala globale, 365 giorni all'anno, 24 ore al giorno. Una situazione di *inaudita gravità*, che mette in discussione ed a repentaglio tutti i presupposti sui quali si basa il buon funzionamento dell'Internet commerciale e di tutti i servizi (online e offline) che su di essa fanno affidamento.

Il Rapporto CLUSIT 2020, giunto ormai al suo nono anno di pubblicazione, inizia con una panoramica degli eventi di cyber-crime più significativi avvenuti a livello globale nel 2019, confrontandoli con i dati raccolti nei 5 anni precedenti.
Lo studio si basa su un campione che al 31 dicembre 2019 è costituito da **10.087** attacchi noti di particolare gravità (di cui **1.670** nel 2019), 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 l'Italia) dal primo gennaio 2011.

Rispetto al 2018, in termini assoluti nel 2019 il numero maggiore di attacchi gravi si osserva verso le categorie "Multiple Targets" (**+29,9%**), "Online Services / Cloud" (**+91,5%**) ed "Healthcare" (**+17,0%**), seguite da "GDO/Retail" (**+28,2%**), "Others" (**+76,7%**), "Telco" (**+54,5%**) e "Security Industry" (**+325%**).
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 43 milioni di eventi di sicurezza.

L'analisi degli attacchi in Italia è poi completata dalle rilevazioni e segnalazioni della **Polizia Postale e delle Comunicazioni**, del Nucleo Speciale Tutela Privacy e Frodi Tecnologiche della **Guardia di Finanza**, del **CERT Nazionale** e del **CERT PA**.
Segue quindi uno studio realizzato da ricercatori dell'Università degli Studi di Bari e di Exprivia/Italtel sullo **stato della cybersecurity nel sud d'Italia**.

Presenteremo a questo punto l'abituale capitolo dedicato al settore FINANCE, con un'analisi sugli "Elementi sul **Cyber-crime nel settore finanziario in Europa**", a cura di IBM ed un contributo inedito del **CERT di Banca d'Italia**.
Segue uno studio realizzato dall'Osservatorio Information Security & Privacy della School of Management del Politecnico di Milano sulla **sicurezza in ambito industriale**.

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

Questi saranno infine i temi trattati nella sezione FOCUS ON:
- "**L'impatto dei deepfake** sulla sicurezza delle organizzazioni economiche", di Federica Bertoni.
- "**Business Continuity & Resilienza**, leve fondamentali per una società sempre più globalizzata e digitalizzata", di Federica Maria Rita Livelli.
- "**Mobile App italiane**: una lente di ingrandimento sul loro stato di salute e sulle vulnerabilità più diffuse", a cura di CryptoNet Labs.
- "Sicurezza nel settore sanitario – **Perché gli ospedali sono così violabili**" a cura di Bitdefender.
- "**Tendenze IT che avranno un impatto sui professionisti italiani nel 2020**", a cura di Netwrix.
- "**Email security**: **i trend** rilevati **in Italia** nel corso del 2019", a cura di Libraesva.

Panoramica dei cyber attacchi più significativi del 2019 e tendenze per il 2020

Introduzione alla nona edizione

Come di consueto in questa prima sezione del Rapporto CLUSIT 2020, giunto ormai al suo nono anno di pubblicazione[1], analizziamo i più gravi cyber attacchi noti avvenuti a livello globale (Italia inclusa) negli ultimi 12 semestri[2] e li confrontiamo con l'analisi degli attacchi noti degli ultimi 12 mesi.
Da quando nel lontano 2011 abbiamo iniziato a svolgere questa raccolta di "incidenti notevoli" di dominio pubblico abbiamo individuato, classificato e valutato oltre **10.000**[3] attacchi avvenuti tra il gennaio 2011 e il dicembre 2019 (dei quali **1.670** analizzati nel 2019).
A partire da questi dati proviamo a fornire un'interpretazione neutra e ragionata sull'evoluzione delle minacce cibernetiche nel mondo ed a delineare le tendenze in atto, volutamente espressa con un taglio divulgativo, in modo da risultare fruibile al maggior numero possibile di lettori.

Considerazioni sul campione

Va sottolineato da un lato che le nostre analisi ed i relativi commenti si riferiscono ad attacchi *reali*, che hanno superato tutte le difese in essere e sono effettivamente andati a segno provocando danni importanti (e non all'analisi di attacchi tentati e/o bloccati), e dall'altro che il nostro campione è necessariamente *parziale*, per quanto ormai statisticamente piuttosto 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.

In merito a quest'ultima fonte di *disclosure obbligatoria* dobbiamo rilevare che, nonostante l'entrata in vigore del Regolamento GDPR[4] e della Direttiva NIS[5], nel secondo semestre 2018 e nel corso del 2019 non abbiamo rilevato (come ci saremmo aspettati) un aumento

---

1 Ovvero alla quindicesima edizione, considerando anche gli aggiornamenti semestrali

2 Confrontando i dati degli ultimi 6 anni, in questo caso dal 2014 al 2019

3 10.087 per la precisione

4 https://it.wikipedia.org/wiki/Regolamento_generale_sulla_protezione_dei_dati

5 https://clusit.it/wp-content/uploads/2017/02/direttiva_nis.pdf

di attacchi gravi di pubblico dominio verso bersagli europei, il che alla luce dell'aumento degli attacchi gravi registrati a livello globale nel 2018 (**+37,7%** rispetto al 2017) e nel 2019 (**+7%** rispetto al 2018) appare statisticamente improbabile, portandoci a concludere che una quota significativa di questi attacchi *non siano ancora emersi*, nonostante gli obblighi di notifica vigenti.
La natura giornalistica delle fonti pubbliche utilizzate per realizzare questo studio (notizie ricavate da testate specializzate ed agenzie di stampa online, blog, post su social media etc.) introduce inevitabilmente un *bias*[6] nel campione, all'interno del quale sono certamente meglio rappresentati gli attacchi più visibili, cioè solitamente quelli realizzati per finalità *cyber criminali* (o di *hacktivism*, anche se ormai in quantità residuale) rispetto a quelli derivanti da attività di *cyber espionage* ed *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 (tipicamente quelli potenzialmente più gravi) 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 2011 abbiamo iniziato questa ricerca, poi pubblicata nella prima edizione del Rapporto Clusit del 2012, definendo (ingenuamente, in retrospettiva) 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 menzionati all'interno del *Global Risk Report* del World Economic Forum[7], mentre nel 2019 sono assurti al primo posto per impatto e probabilità di accadimento, insieme ai disastri naturali ed 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 ed 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 situa-

[6] https://it.wikipedia.org/wiki/Bias_(statistica)

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

zione 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 ad evolversi, trasformandosi da una semplice cronaca ragionata degli attacchi noti più significativi in un vero e proprio strumento di lavoro e di supporto decisionale.

Per questa ragione, oltre ad analizzare 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 e nel 2018 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 ad una migliore "fotografia" dei rischi attuali resa possibile da questo ulteriore elemento di valutazione.

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, ed alle sue ricadute sul benessere del Paese, auguriamo a tutti una buona lettura.

2019, "Hic sunt Leones"

Anticipando alcune delle conclusioni che seguono possiamo affermare che il 2019 è stato l'anno *peggiore di sempre* in termini di evoluzione delle minacce "cyber" e dei relativi impatti, sia dal punto di vista quantitativo che da quello qualitativo, evidenziando un trend persistente di crescita degli attacchi, della loro gravità e dei danni conseguenti.

Per sintetizzare in una frase il nostro giudizio in merito alla situazione, due anni fa abbiamo scritto (non senza attirare qualche sberleffo, purtroppo immotivato) che il 2017 aveva rappresentato un "salto quantico" nei livelli di cyber-insicurezza globali, e nel 2018 abbiamo insistito affermando che fossimo ormai giunti a "due minuti dalla mezzanotte".

Essendo rimasti a corto di frasi ad effetto, quest'anno abbiamo deciso di distillare il nostro giudizio sull'evoluzione della situazione utilizzando il celebre motto latino "Hic Sunt Leones"[8], inserito sulle antiche carte geografiche ad indicare un territorio sconosciuto e pericoloso, popolato da mostri e chimere.
Con questo vogliamo indicare che dopo il "salto quantico" annunciato nel 2017, la "mezzanotte" di cui parlavamo nel 2018 *è stata superata* nel corso del 2019.

La nostra reazione analizzando l'incredibile varietà, pervasività ed efficacia degli attacchi del 2019 è stata simile a quella di Dorothy del film "Il mago di Oz"[9], che trasportata da un tornado nella magica terra di Oz esclama: "*decisamente non siamo più nel Kansas*"[10].
Nell'anno appena passato si è consolidata una discontinuità, si è oltrepassato un punto di non ritorno, tale per cui ormai ci troviamo a vivere ed operare in una dimensione differente, in una nuova epoca, in un "altro mondo", del quale ancora non conosciamo bene la geografia, gli abitanti, le regole e le minacce.

Gli attaccanti non sono più "hackers", e nemmeno gruppetti effimeri (più o meno pericolosi) di "artigiani" del cybercrime: sono decine e decine di gruppi criminali organizzati transnazionali che fatturano miliardi, multinazionali fuori controllo dotate di mezzi illimitati, stati nazionali con i relativi apparati militari e di intelligence, i loro fornitori e contractors, gruppi state-sponsored civili e/o paramilitari ed unità di mercenari impegnati in una lotta senza esclusione di colpi, che hanno come *campo di battaglia, arma e bersaglio* le infrastrutture, le reti, i server, i client, i device mobili, gli oggetti IoT, le piattaforme social e di instant messaging (e la mente dei loro utenti), su scala globale, 365 giorni all'anno, 24 ore al giorno. Una situazione di *inaudita gravità*, che mette in discussione ed a repentaglio tutti i presupposti sui quali si basa il buon funzionamento dell'Internet commerciale e di tutti i

[8] https://it.wikipedia.org/wiki/Hic_sunt_leones

[9] https://it.wikipedia.org/wiki/Il_mago_di_Oz_(film_1939)

[10] Celebre frase pronunciata da Dorothy ne "Il Mago di Oz": "We're Not In Kansas Anymore!"

servizi (online e offline) che su di essa fanno affidamento.
In questo senso vogliamo trasmettere un messaggio forte e chiaro: Hic sunt Leones, non siamo più in Kansas, la situazione è cambiata *drasticamente*, siamo in un territorio sconosciuto e questo "new normal" in termini di rischi "cyber", è *diverso* e va gestito diversamente rispetto anche solo a 2-3 anni fa.

Osservando la situazione dal punto di vista quantitativo, a parità dei criteri di classificazione che applichiamo al nostro campione (aggiornati nel 2014 e mantenuti invariati da allora) confrontando i numeri del 2014 con quelli del 2019 la crescita degli attacchi gravi di pubblico dominio è stata del **+91,2%** (da 873 a 1.670).
Mentre nel triennio 2017-2019 il numero di attacchi gravi che abbiamo analizzato è cresciuto del **+48%** (da 1.127 a 1.670 all'anno), la crescita registrata nel triennio 2014-2016 era stata "solo" del +20% (da 873 a 1.050), ovvero *nell'ultimo triennio il tasso di crescita del numero di attacchi gravi è più che raddoppiato rispetto al triennio precedente*. Non solo, la valutazione della Severity media di questi attacchi (indice che abbiamo introdotto dal 2017) nei confronti di alcune categorie di vittime è contestualmente peggiorata, agendo da moltiplicatore dei danni.
Questi trend avvalorano la nostra convinzione che sia avvenuto un vero e proprio *cambiamento epocale* nei livelli globali di cyber-insicurezza, causato dall'evoluzione rapidissima degli attori, delle modalità, della pervasività e dell'efficacia degli attacchi. Dobbiamo *sforzarci* di tenere presente che il Cybercrime, il Cyber Espionage e l'Information Warfare del 2019 non sono certamente più quelli del 2014, e nemmeno quelli del 2017, anche se continuiamo ad utilizzare le stesse denominazioni.
Come previsto, nel 2019 si sono realizzate appieno le tendenze più pericolose individuate già nel 2017 e proseguite nel 2018, che avevamo descritto come "l'anno del trionfo del malware, degli attacchi industrializzati realizzati su scala planetaria contro bersagli multipli, dell'alterazione di massa della percezione e della definitiva discesa in campo degli Stati come attori di minaccia".
Queste dinamiche nell'ultimo triennio hanno causato conseguenze molto concrete, da un lato spingendo sempre più soggetti (statuali e non) ed entrare nell'arena, accelerando la "corsa agli armamenti" in atto ed esacerbando il livello dello scontro, e dall'altro impattando in modo ormai inequivocabile sulla società civile (singoli cittadini, istituzioni ed imprese), che sta *cambiando* in conseguenza di questa enorme pressione (tipicamente non in meglio). Siamo cioè di fronte a fenomeni che per natura e dimensione travalicano ormai *costantemente* i confini dell'IT e della stessa cyber security, ed hanno impatti profondi, duraturi e sistemici su ogni aspetto della società, della politica, dell'economia e della geopolitica.

Per fare un esempio eclatante della *mutazione sostanziale delle minacce cyber* avvenuta negli ultimi 3 anni, il Cybercrime, pur rappresentando senz'altro un problema enorme e facendo la parte del leone nel nostro campione dal punto di vista quantitativo (per le ragioni esposte nel capitolo precedente), ormai dal punto di vista qualitativo (ovvero della Severity, secondo

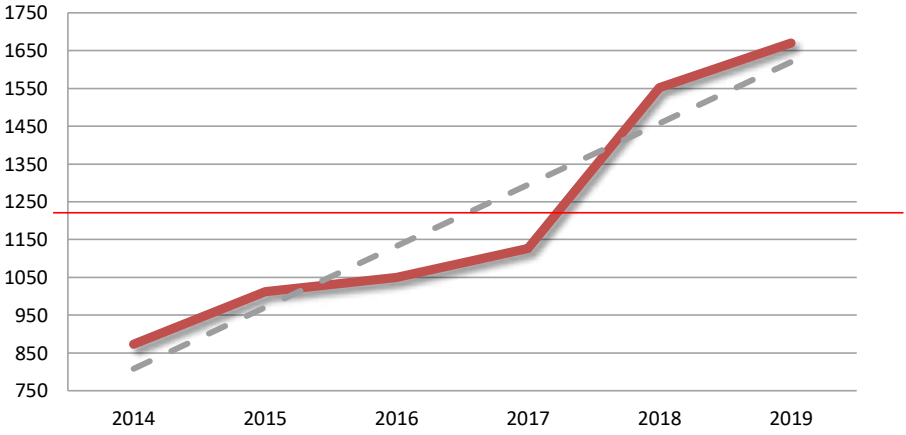
la nostra analisi) è paradossalmente diventato *un rischio secondario,* nel senso che ormai ci troviamo a fronteggiare *quotidianamente* minacce *ben peggiori,* nei confronti delle quali le contromisure disponibili sono particolarmente inefficaci.

Analisi dei principali cyber attacchi noti a livello globale del 2019

In questa prima sezione del Rapporto CLUSIT 2020, come di consueto, proponiamo una dettagliata panoramica degli incidenti di sicurezza più significativi avvenuti a livello globale nel 2019, confrontandoli con i dati raccolti nei 5 anni precedenti[11].

Lo studio si basa su un campione che al 31 dicembre 2019 è costituito da **10.087** attacchi noti di particolare gravità (di cui **7.284** dal 2014), 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 l'Italia) dal primo gennaio 2011, di cui **1.670** nel 2019 (**+48%** rispetto al 2014, **+ 7,6%** rispetto al 2018).) Il numero di attacchi rilevati nel 2019 segna una differenza del **+37,5%** rispetto alla media degli attacchi per anno degli ultimi 6 anni (1.214), visualizzata con una linea rossa orizzontale nel grafico seguente.

Numero di attacchi rilevanti per anno (2014 - 2019)



© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia

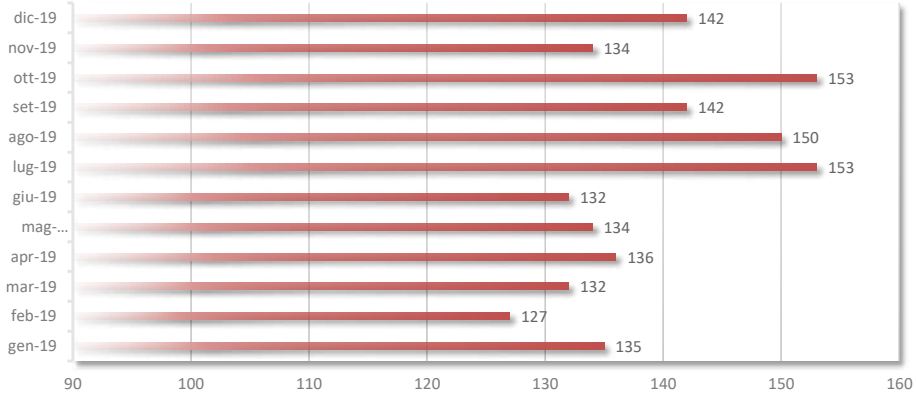
Anche quest'anno, per definire un cyber attacco come "grave" abbiamo impiegato gli stessi criteri di classificazione già applicati ai dati del periodo 2014-2018, più restrittivi rispetto ai criteri che avevamo applicato negli anni 2011-2013, dal momento che nell'arco di questi

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

108 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).

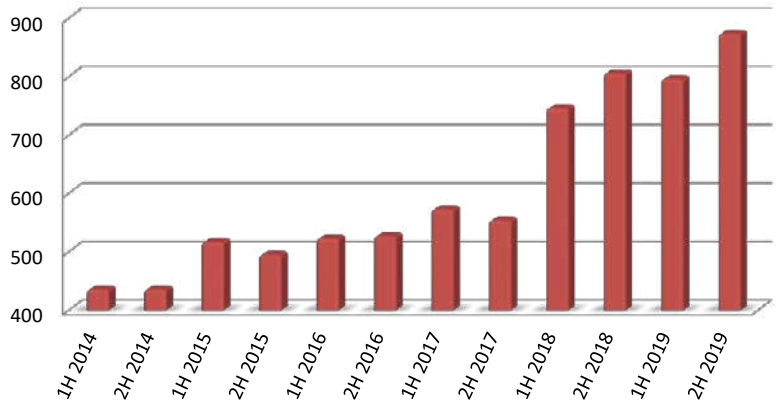
A parità di criteri, quest'anno abbiamo classificato come gravi un numero di attacchi superiore rispetto a tutti gli anni analizzati a partire dal 2014.
Dal punto di vista numerico, dei 10.087 attacchi gravi di pubblico dominio che costituiscono il nostro database di incidenti degli ultimi 9 anni, nel 2019 ne abbiamo raccolti e analizzati 1.670, contro i 1.552 del 2018 (**+7,6%**), con una media di **139 attacchi gravi al mese** (rispetto ad una media di 73 al mese nel 2014, e di 94 al mese sui 9 anni). Il picco massimo mensile di sempre si è avuto nel novembre 2018 (157 attacchi). I mesi peggiori nel 2019 sono stati luglio ed ottobre con **153** attacchi.

Numero di attacchi per mese (2019)



Questa la distribuzione degli attacchi registrati nel periodo 2014-2019, suddivisi per semestre:

Numero di attacchi per semestre (2014 - 2019)



© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia

Le tre tabelle seguenti rappresentano una sintesi dei dati che abbiamo raccolto e analizzato. Come in passato abbiamo evidenziato nella colonna più a destra le tendenze osservate.

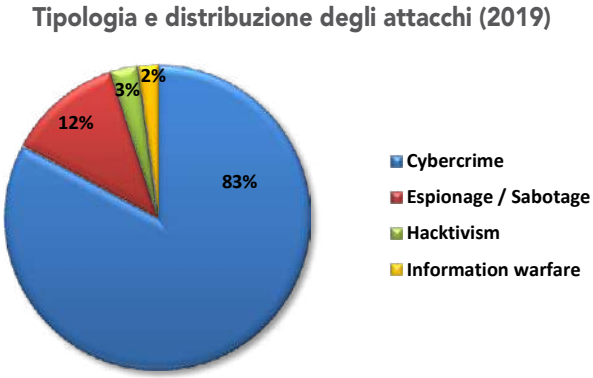
Da qui in avanti, per comodità di consultazione e omogeneità dei criteri di classificazione degli attacchi, presentiamo il confronto solo dei dati degli ultimi 6 anni, rimandando alle edizioni precedenti del Rapporto Clusit per i dati relativi al triennio 2011-2013.

Distribuzione degli attaccanti per tipologia

ATTACCANTI PER TIPOLOGIA	2014	2015	2016	2017	2018	2019	2019 su 2018	Trend
Cybercrime	526	684	751	857	1232	1383	12.3%	↑
Hacktivism	236	209	161	79	61	48	-21.3%	↓
Espionage / Sabotage	69	96	88	129	203	204	0.5%	→
Cyber Warfare	42	23	50	62	56	35	-37.5%	↓
Espionage / Sabotage + Cyber Warfare	111	119	138	191	259	239	-7.7%	→
TOTALE	**873**	**1012**	**1050**	**1127**	**1552**	**1670**	**+7,6%**	→

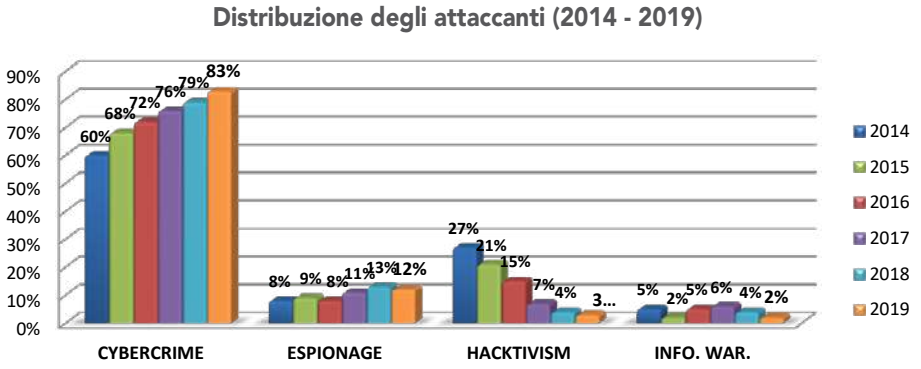
Complessivamente, rispetto al 2018, il numero di attacchi gravi che abbiamo raccolto da fonti pubbliche per il 2019 cresce del **+7,6%**. In termini assoluti, nel 2019 la categoria "Cybercrime" fa registrare il numero di attacchi più elevato degli ultimi 9 anni, con una crescita del **+162%** rispetto al 2014 (1383 contro 526).

Dal campione emerge chiaramente che, mentre le attività riferibili ad attacchi della categoria "**Hacktivism**" diminuiscono ancora sensibilmente (**-21,3%**) rispetto al 2018, nel 2019 sono in ulteriore aumento gli attacchi gravi compiuti per finalità di "**Cybercrime**" (**+12,3%**), mentre rimangono stabili quelli riferibili ad attività di "**Cyber Espionage**" (**+0,5%**) e sembrano diminuire quelli appartenenti alla categoria "Cyber Warfare" (**-37,5%**).
Va sottolineato che, rispetto al passato, oggi risulta più difficile distinguere nettamente tra "Cyber Espionage/Sabotage" e "Cyber Warfare": sommando gli attacchi di entrambe le categorie, nel 2019 si assiste ad una diminuzione del **7,7%** rispetto all'anno precedente (239 contro 259).



© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia

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 ed infine al 79% nel 2018, mostrando una tendenza inequivocabile. Nel 2019 tale percentuale cresce ulteriormente all'**83%**.



© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia

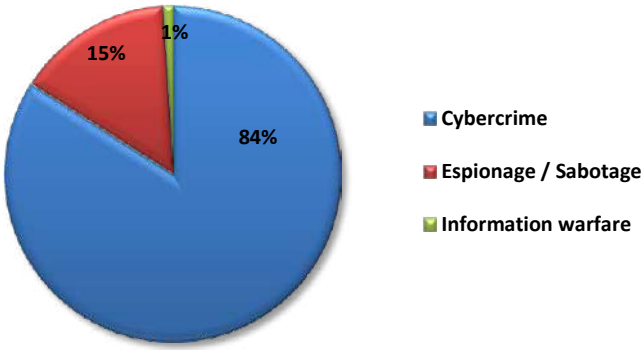
L'Hacktivism diminuisce ulteriormente, passando da quasi un terzo (27%) dei casi analizzati nel 2014 al **3%** del 2019.

Per quanto riguarda le attività di Espionage (anche a causa della scarsità di informazioni pubbliche in merito) la loro percentuale rispetto al totale degli attacchi rilevati nel 2018 passa dal 13% al **12%**, mentre l'Information Warfare passa dal 4% al **2%**. Nel 2019 queste due categorie sommate valgono il **14%** degli attacchi noti totali (ma hanno una Severity più alta della media, vedi poi).

Distribuzione degli attaccanti rispetto alle categorie più colpite da attacchi

Nel 2019 le categorie più colpite sono state **Multiple Targets** (395 attacchi, **+29,9%** rispetto al 2018), **Online Services** (247 attacchi, **+91,5%**), **Government** (203 attacchi, **-19,4%**) ed **Healthcare** (186 attacchi, **+17%**).
Dal punto di vista della distribuzione degli attaccanti che le hanno prese di mira, dalla nostra analisi emergono differenze molto significative, il che conferma che ogni categoria di bersagli ha un suo particolare *threat landscape* dal quale deve proteggersi, e che (di conseguenza) non esistono soluzioni universali ma anzi, ogni settore dovrebbe schierare un mix di soluzioni difensive specifico.

Tipologia e distribuzione degli attaccanti vs MULTIPLE TARGET (2019)

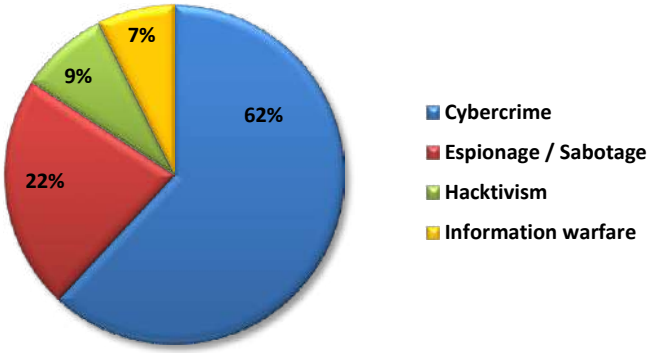


© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia

La distribuzione degli attaccanti verso la categoria Multiple Target (che è quella più numerosa ormai) ricalca la distribuzione generale, con un lieve incremento della componente cyber criminale, dovuta al fatto che compiere attacchi contro bersagli multipli in parallelo è ormai uno dei pilastri del "modello di business" di questo tipo di attaccanti.
Per ragioni analoghe, anche la componente di Espionage risulta leggermente più alta della media generale verso questa categoria di vittime, a causa di campagne massive di furto di dati personali e di business, utilizzati poi per ulteriori elaborazioni / campagne mirate.

Significativamente diversa la distribuzione degli attaccanti verso il settore Governativo. La diversa composizione percentuale degli attaccanti incide anche fortemente sul tipo di tecniche di attacco utilizzate verso le diverse categorie di vittime (vedi oltre). Interessante notare che la quota di attacchi compiuti per finalità di Espionage è quasi il doppio rispetto alla media generale, e quelli realizzati per finalità di Hacktivism sono addirittura il triplo, così come quelli con finalità di Information Warfare.

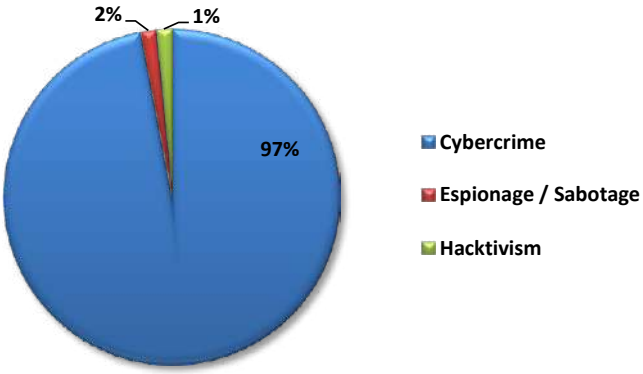
Tipologia e distribuzione degli attaccanti vs GOV / MIL / LE (2019)



© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia

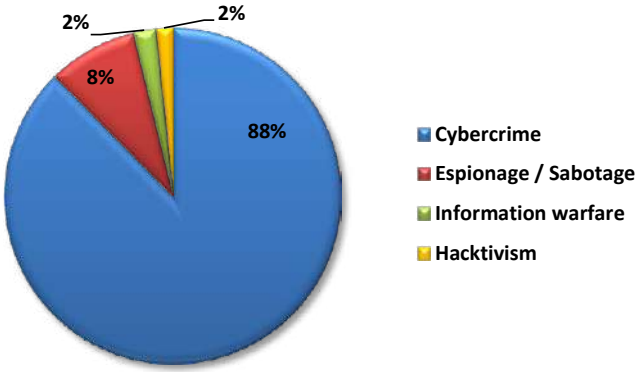
Ancora diversa la distribuzione degli attaccanti che hanno colpito il settore Healthcare, prevalentemente con finalità cybercriminali, in particolare estorsioni (ransomware) e furti di dati personali, da utilizzare per compiere ulteriori attacchi.

Tipologia e distribuzione degli attaccanti vs HEALTHCARE (2019)



© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia

Tipologia e distribuzione degli attaccanti vs ONLINE SERVICES (2019)



© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia

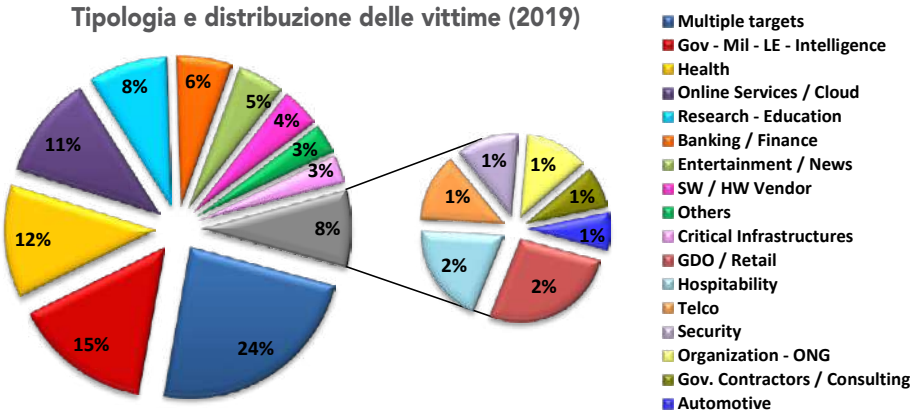
Per la categoria "Online Services" (che include anche le piattaforme Social) la distribuzione degli attaccanti è simile a quella rilevata per la categoria "Multiple targets", per quanto con una percentuale più bassa di Espionage, una percentuale maggiore di Cybercrime e una piccola quota di attacchi legati ad operazioni di Hacktivism.

Distribuzione delle vittime per tipologia

VITTIME PER TIPOLOGIA	2014	2015	2016	2017	2018	2019	2019 su 2018	Trend
Gov - Mil - LEAs - Intel	213	223	220	179	252	203	-19.4%	
Multiple targets	-	-	49	222	304	395	29.9%	
Healthcare	32	36	73	80	159	186	17.0%	
Banking / Finance	50	64	105	117	156	141	-10.2%	
Online Services / Cloud	103	187	179	95	129	247	91.5%	
Research - Education	54	82	55	71	110	100	-8.3%	
Software / Hardware Vendor	44	55	56	68	109	83	-23.9%	
Entertainment / News	77	138	131	115	102	70	-31.4%	
Critical Infrastructures	13	33	38	40	57	37	-35.1%	
Hospitability	-	39	33	34	45	27	-40.0%	
GDO / Retail	20	17	29	24	39	50	28.2%	
Others	172	51	38	40	30	53	76.7%	
Org / ONG	47	46	13	8	18	18	0.0%	-
Gov. Contractors / Consulting	13	8	7	6	14	11	-21.4%	
Telco	18	18	14	13	11	17	54.5%	
Automotive	3	5	4	4	9	10	11.1%	
Security Industry	2	3	0	11	4	17	325.0%	
Religion	7	5	6	0	3	3	0.0%	-
Chemical / Medical	5	2	0	0	1	2	100.0%	
TOTALE	**873**	**1012**	**1050**	**1127**	**1552**	**1670**		

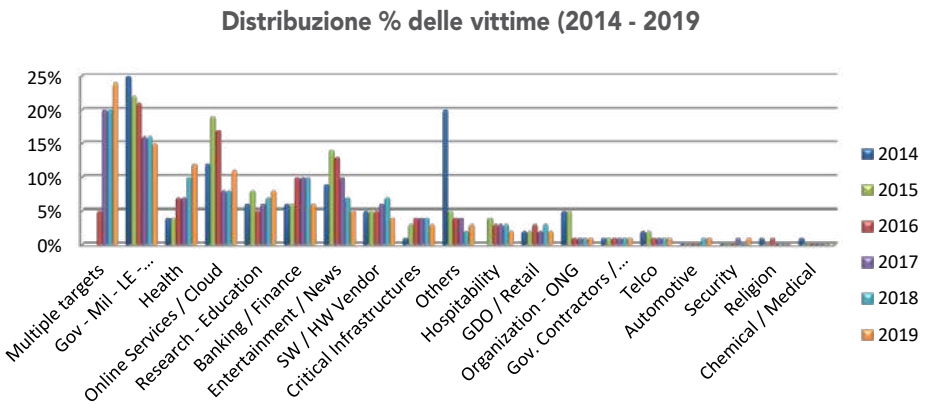
Rispetto al 2018, in termini assoluti nel 2019 il numero maggiore di attacchi gravi si osserva verso le categorie "Multiple Targets" (**+29,9%**), "Online Services / Cloud" (**+91,5%**) ed "Healthcare" (**+17,0%**), seguite da "GDO/Retail" (**+28,2%**), "Others" (**+76,7%**), "Telco" (**+54,5%**) e "Security Industry" (**+325%**).

Interessante sottolineare l'aumento di attacchi verso la categoria "Others", nonostante molti di questi attacchi rientrino solitamente nella categoria "Multiple targets" da quando l'abbiamo introdotta nel 2016. Ciò è dovuto ad un aumento di *attacchi mirati* (cioè non su larga scala) verso nuove categorie di bersagli non esplicitamente classificate nella nostra tassonomia, che aggiorneremo di conseguenza nelle prossime edizioni.
All'interno della categoria "Multiple Targets", che numericamente costituisce ormai quasi *un quarto degli attacchi registrati*, sono compresi attacchi verso vittime appartenenti a *tutte le altre categorie, colpite dallo stesso attacco in parallelo*, a dimostrazione del fatto che gli attaccanti sono 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.
Degna di nota anche la diminuzione in termini assoluti degli attacchi verso le categorie "Critical Infrastructures" (**-35,1%**), "Entertainment/News" (**-31,4%**) e "Hospitability" (**-40,0%**) rispetto al 2018.



© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia

Per i motivi sopra illustrati, anche nel 2019 al primo posto assoluto si conferma la categoria "Multiple Targets" (**24%,** era il 20% nel 2018), superando per il terzo anno di fila il settore "Gov", in diminuzione al **15%**, che dal 2011 al 2016 è sempre stato al primo posto nel nostro studio.
Come nel 2018 "Healthcare" è al terzo posto (**12%**), seguita da "Online Services / Cloud" (**11%**), Reseach/Education (**8%**), "Banking/Finance" (**6%**) e "Entertainment/News" (**5%**).



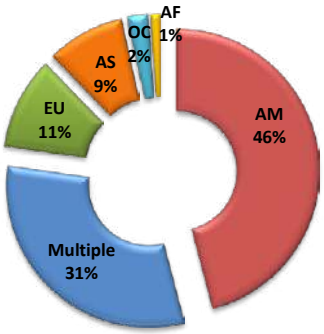
© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia

Tramite questo grafico si può apprezzare facilmente l'incremento degli attacchi gravi condotti in parallelo verso Multiple Targets (quindi con impatti potenzialmente sistemici, data la scala), Healthcare e Online Services occorso nel 2019.

Distribuzione delle vittime per area geografica

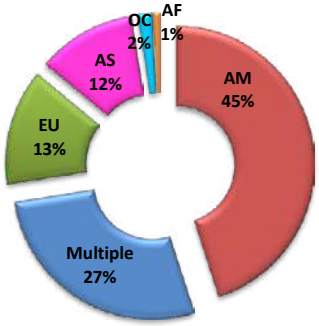
La classificazione delle vittime per nazione di appartenenza viene qui rappresentata su base continentale.
Premesso che rispetto al 2018 le variazioni percentuali sono minime, nel 2019 aumentano le vittime di area americana (dal 45% al **46%**), mentre, in attesa che GDPR e NIS facciano emergere attacchi ad oggi non noti in area europea, gli attacchi verso realtà basate in Europa sembrano addirittura diminuire (dal 13% al **11%**) e diminuiscono anche quelli rilevati contro organizzazioni asiatiche (dal 12% al **9%**).
Percentualmente aumentano gli attacchi gravi verso bersagli multipli distribuiti globalmente (categoria "Multiple"), dall'27% del 2018 al **31%** del 2019.

Appartenenza geografica delle vittime per continente (2019)



© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia

Appartenenza geografica delle vittime per continente (2018)



© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia

Distribuzione delle tecniche di attacco

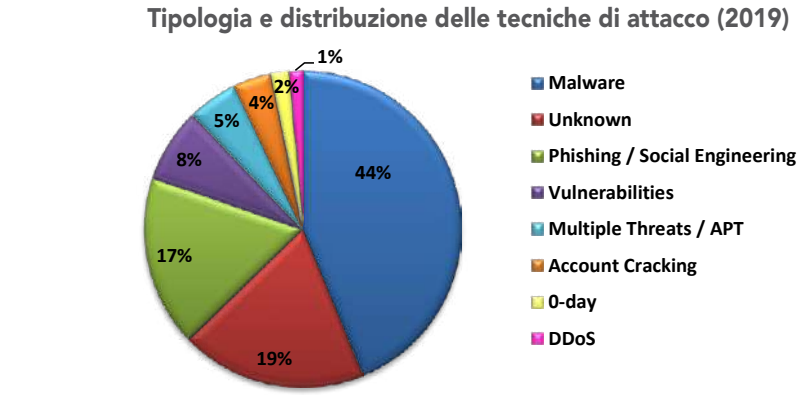
TIPOLOGIA TECNICHE DI ATTACCO	2014	2015	2016	2017	2018	2019	2019 su 2018	Trend
Malware	127	106	229	446	585	730	24.8%	↑
Unknown	199	232	338	277	408	317	-22.3%	↓
Known Vulnerabilities / Misconfig.	195	184	136	127	177	126	-28.8%	↓
Phishing / Social Engineering	4	6	76	102	160	291	81.9%	↑
Multiple Techniques / APT	60	104	59	63	98	65	-33.7%	↓
Account Cracking	86	91	46	52	56	86	53.6%	↑
DDoS	81	101	115	38	38	23	-39.5%	↓
0-day	8	3	13	12	20	30	50.0%	↑
Phone Hacking	3	1	3	3	9	1	-88.9%	↓
SQL Injection	110	184	35	7	1	1	0.0%	-
TOTALE	**873**	**1012**	**1050**	**1127**	**1552**	**1670**		

Per la terza volta dal 2011, nel 2019 le tecniche sconosciute (categoria "Unknown") sono al secondo posto, diminuendo del **22,3%** rispetto al 2018, superate dalla categoria "Malware", stabile al primo posto, che cresce ulteriormente del +**24,8%** e rappresenta ormai il **44%** del totale.

Al terzo posto la categoria "Phishing/Social Engineering", che cresce del **+81,9%** rispetto al 2018 e rappresenta il **17%** del totale. Una quota crescente di questi attacchi basati su Phishing si riferisce a "BEC scams"[12], che infliggono danni economici sempre maggiori alle loro vittime.

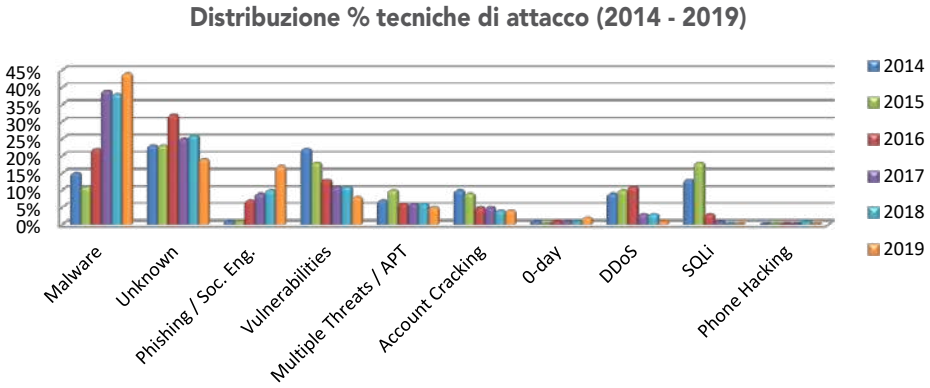
Tutte le altre tipologie di tecniche di attacco sommate rappresentano nel 2019 solo il **12,3%** del totale. Notevole l'incremento percentuale delle categorie "0day" (**+50%**) e "Account Cracking" (**+53,6%**), mentre appaiono in diminuzione gli attacchi realizzati sfruttando vulnerabilità note (**-28,8%**), DDos (**-39,5%**) e tecniche multiple/APT (**-33,7%**). Queste ultime sono in parte confluite nella categoria "Malware", sempre più utilizzato anche da attori statuali e state-sponsored.

[12] https://en.wikipedia.org/wiki/Business_email_compromise



© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia

In sostanza si conferma anche nel 2019 una tendenza inequivocabile e molto pericolosa: gli attaccanti possono fare affidamento sull'efficacia del Malware "semplice", prodotto industrialmente a costi decrescenti in infinite varianti, e su tecniche di Phishing / Social Engineering relativamente semplici, per conseguire la gran maggioranza dei loro obiettivi. Questo dato è evidenziato anche dall'inedita polarizzazione delle tecniche d'attacco, tale per cui ormai le prime 4 categorie (su un totale di 10) rappresentano l'**87,6%** del campione.



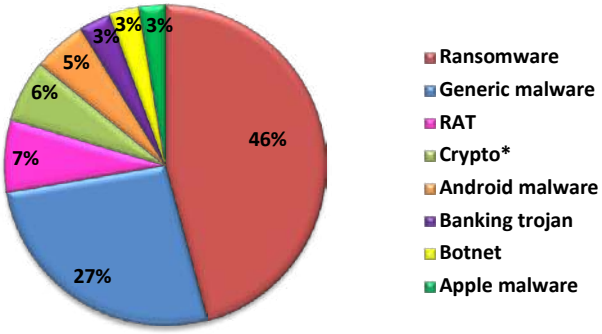
© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia

Nel grafico si può apprezzare visivamente la crescita netta di Malware e Phishing nel 2019, che raggiungono i valori più alti mai registrati dall'inizio di questa analisi.

Analisi delle principali categorie di malware

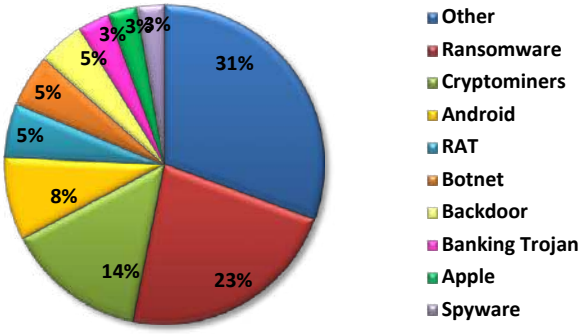
Dato che la categoria "Malware" si conferma per il terzo anno di fila la più numerosa, anche per il 2019 presentiamo un'analisi di dettaglio relativa alle tipologie di malware osservate nel nostro campione, confrontandola con l'anno precedente:

Tipologia e distribuzione Malware (2019)



© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia

Tipologia e distribuzione Malware (2018)



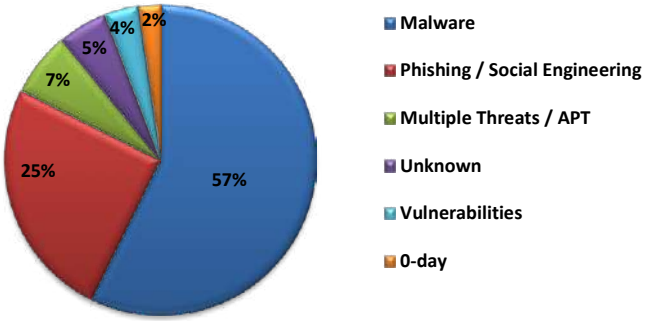
© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia

Dal grafico si possono osservare alcuni fenomeni interessanti, tra questi che i Ransomware rappresentano nel 2019 quasi la metà del totale (erano un quarto nel 2018), e che i Cryptominers sono diminuiti dal 14% al 6%, più che dimezzandosi in percentuale.

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

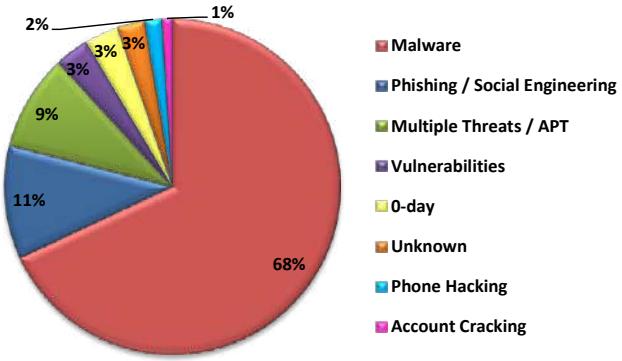
Riportiamo di seguito le statistiche relative alla distribuzione percentuale delle tecniche di attacco impiegate contro i 4 settori più colpiti da attacchi nel 2019 ("Multiple Targets", "Gov", "Healthcare" e "Online Services").
Anche in questo caso si può osservare chiaramente come la distribuzione delle 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). È anche interessante osservare la variazione di queste percentuali rispetto al 2018, in alcuni casi particolarmente significativa, il che suggerisce un cambio di strategie, di tattiche e di obiettivi da parte degli attaccanti.

Tipologia e distribuzione tecniche di attacco vs MULTIPLE TARGET (2019)



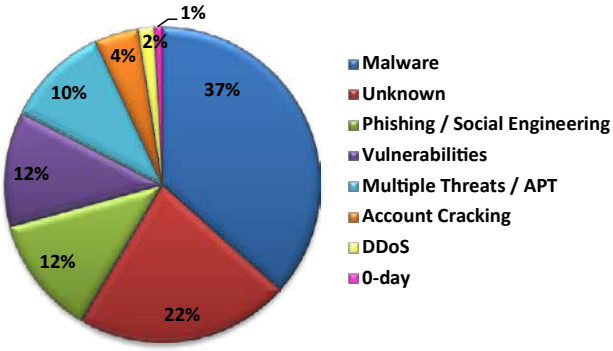
© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia

Tipologia e distribuzione tecniche di attacco vs MULTIPLE TARGET (2018)



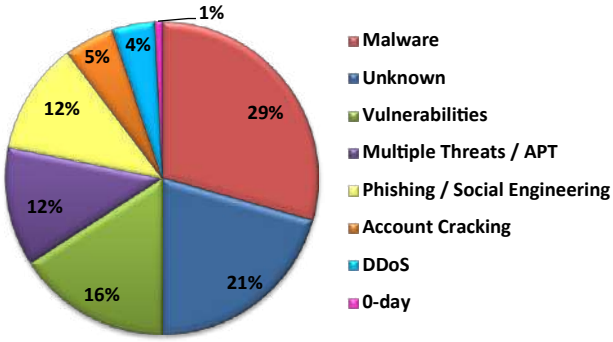
© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia

Distribuzione delle tecniche di attacco vs GOV / MIL / LE (2019)



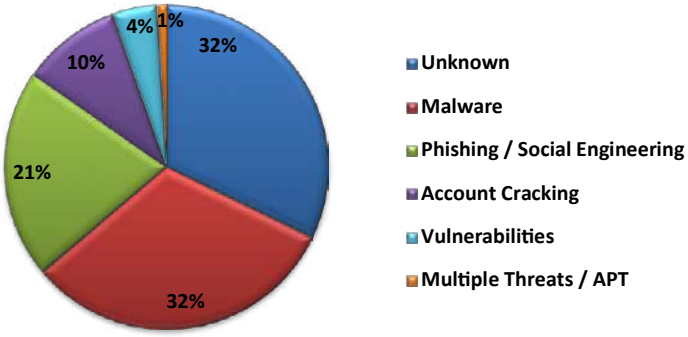
© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia

Distribuzione delle tecniche di attacco vs GOV / MIL / LE (2018)



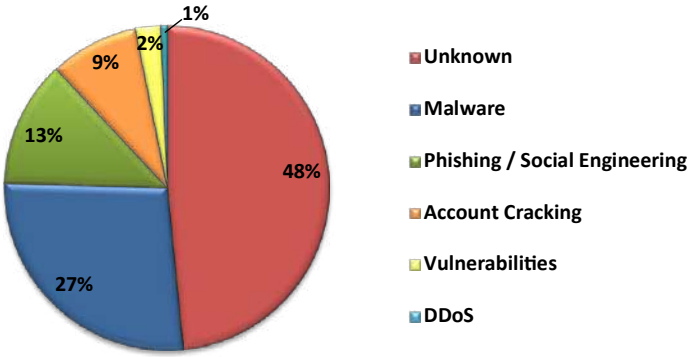
© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia

Tipologia e distribuzione tecniche di attacco vs HEALTHCARE (2019)



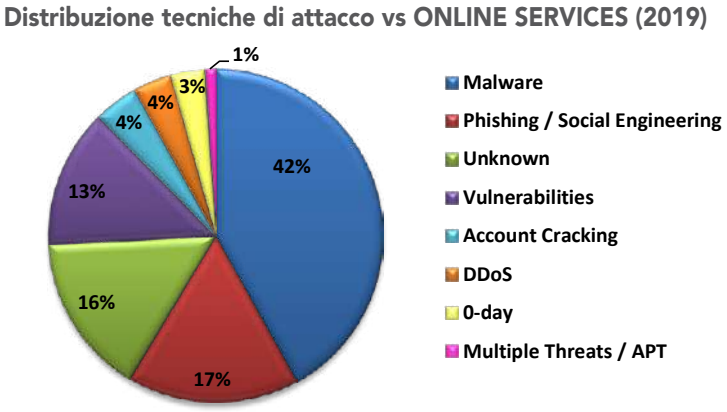
© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia

Tipologia e distribuzione tecniche di attacco vs HEALTHCARE (2018)



© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia

Questa infine è la distribuzione delle tecniche di attacco utilizzate nei confronti della categoria "Online Services":

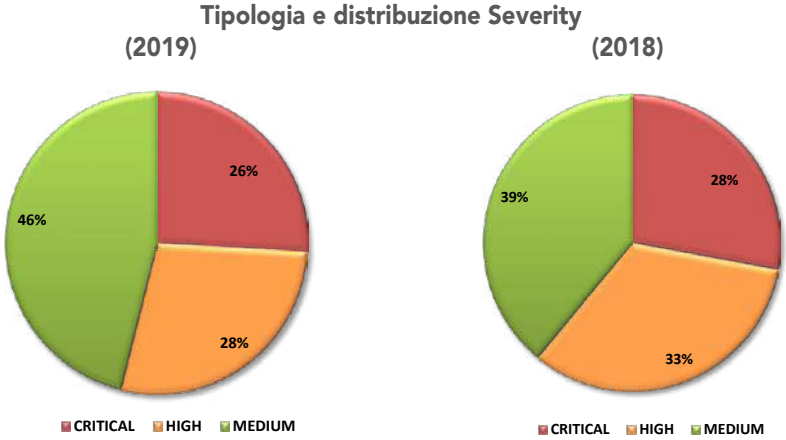


© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia

Analisi della "Severity" degli attacchi

Come anticipato nell'introduzione di questa analisi, anche per il 2019 presentiamo una valutazione della Severity degli attacchi analizzati.
Per distinguere tra attacchi di differente natura e pericolosità all'interno del campione abbiamo definito tre macrocategorie o livelli di **impatto** (considerato che stiamo comunque analizzando un campione di incidenti tutti definiti come "gravi"): Medio, Alto e Critico.
Va premesso che questo genere di analisi si scontra inevitabilmente con la scarsità di informazioni dettagliate di dominio pubblico relative ai singoli incidenti, e che pertanto deve considerarsi una stima ad alto livello.

Le variabili che contribuiscono a comporre la valutazione dell'impatto per ogni singolo attacco analizzato sono molteplici ed includono: impatto geopolitico, sociale, economico (diretto e indiretto) e di immagine.
Per il campione 2019, l'analisi degli impatti stimati ci presenta questo quadro generale:

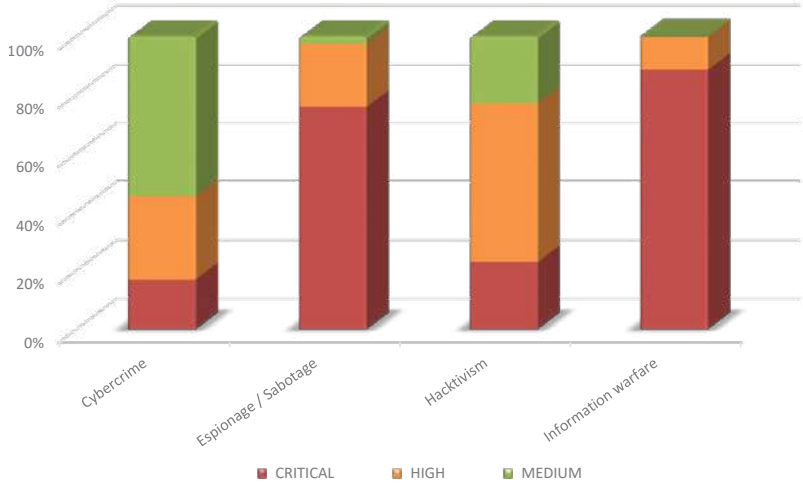


Interessante confrontare i risultati della stessa analisi relativi al 2018.

Nel 2019 gli attacchi con impatto "Medio" rappresentano il **46%** del totale (erano il 39% nel 2018 ed il 49% nel 2017), quelli di livello "Alto" il **28%** (erano 33% nel 2018 e il 31% nel 2017) e quelli di livello "Critico" oltre un quarto con il **26%** (erano il 28% nel 2018 ed il 21% nel 2017).
Anche nel 2019 quindi il numero di attacchi di livello "Critical" e "High" supera il 50% del totale (**54%**) per un totale di 902 attacchi, per quanto in leggera diminuzione rispetto al 61% del 2018 (per un totale di 946).

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

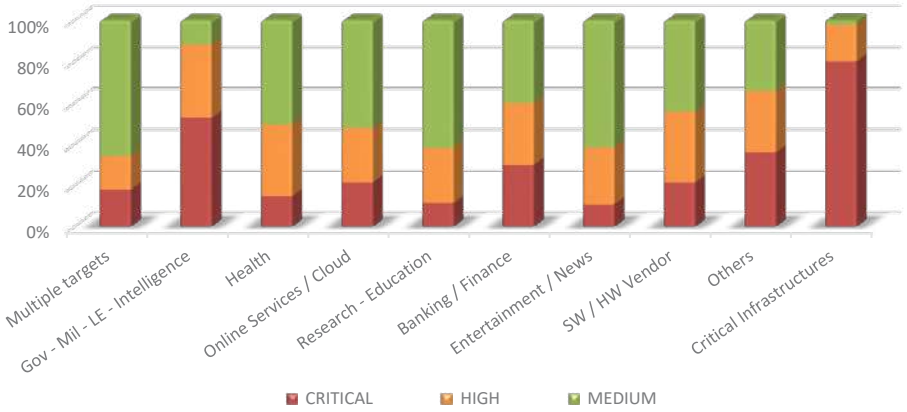
Distribuzione Severity per categoria di attaccante (2019)



© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia

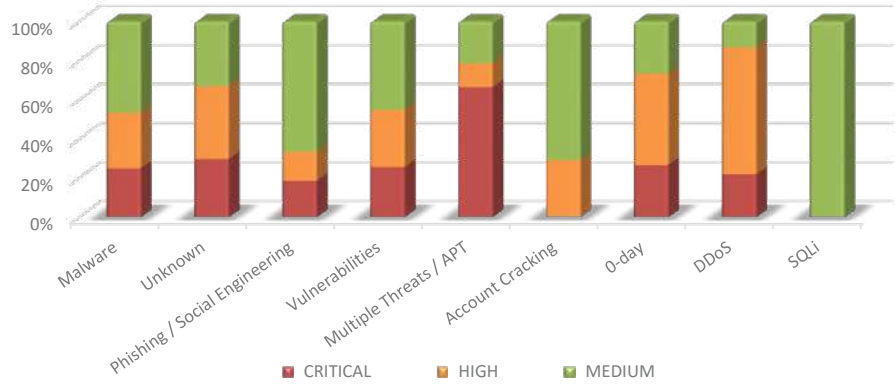
Non sorprende che il maggior numero di attacchi classificati come "Critici" riguardino le categorie di attaccanti "Espionage" ed "Information Warfare", mentre la prevalenza di attacchi con impatto di tipo "Medio" e (in misura minore) "Alto" riferiti ad attività cybercriminali si spiega con la necessità, 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" ed abbia un valore medio della Severity peggiore rispetto alla categoria Cybercrime (pur essendo numericamente molto meno rappresentato nel campione).

Distribuzione Severity per i 10 target più colpiti nel 2019



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

Distribuzione Severity per tecnica di attacco nel 2019



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).

In percentuale gli attacchi con impatto "Critico" realizzati tramite Malware sono meno di quelli realizzati tramite Vulnerabilità note o con tecniche sconosciute, 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 2018 e quella del 2019, 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", quindi un numero più basso indica una situazione peggiore), la Severity media degli attacchi nel 2019 è peggiorata nei confronti di "SW/WH vendor", "Research / Education", "Entertainment/News", "Hospitability" (in modo sensibile), "GDO / Retail", "Others", "Organizations/ONG", "Automotive" (in modo sensibile), "Religion" (in modo sensibile) e "Security Industry".

Severity 2019 vs 2018	CRITICAL	HIGH	MEDIUM	TOT	MEDIA 2018	MEDIA 2019	TREND
Multiple targets	71	64	260	395	2,3	2,5	↘
Gov - Mil - LE - Intelligence	130	88	29	247	1,5	1,6	↘
Healthcare	30	70	103	203	1,9	2,4	↘
Banking / Finance	40	49	97	186	2,3	2,3	-
Online Services / Cloud	16	38	87	141	2,4	2,5	↘
SW / HW Vendor	30	30	40	100	2,3	2,1	↗
Research - Education	9	23	51	83	2,6	2,5	↗
Entertainment / News	15	24	31	70	2,6	2,2	↗
Critical Infrastructures	19	16	18	53	1,2	2,0	↘
Hospitability	40	9	1	50	2,6	1,2	↑
GDO / Retail	3	15	19	37	2,6	2,4	↗
Others	2	11	14	27	2,5	2,4	↗
Organization - ONG	9	4	5	18	2,0	1,8	↗
Gov. Contractors / Consulting	3	9	5	17	1,1	2,1	↘
Telco	2	7	8	17	1,7	2,4	↘
Automotive	6	4	1	11	2,2	1,5	↑
Religion	7	3	0	10	2,3	1,3	↑
Security Industry	0	3	0	3	2,3	2,0	↗
Chemical / Medical	1	0	1	2	1,0	2,0	↘

Questo tipo di confronto consente di evidenziare alcuni fenomeni "nascosti" nei dati del campione.
Per esempio, si evince che il settore "Hospitability", pur avendo ricevuto meno attacchi rispetto al 2018 (-40%), ha visto più che raddoppiare la Severity media degli attacchi subiti (da 2,6 a 1,2), mentre le categorie "Gov" e "Multiple targets", pur avendo subito in assoluto il numero di attacchi maggiore nel 2019, mostrano un leggero miglioramento in termini di Severity media degli attacchi subiti.

Nelle prossime edizioni del Rapporto Clusit raffineremo e dettaglieremo ulteriormente questo tipo di analisi sul campione, al fine di fornire elementi più precisi di valutazione in un'ottica di supporto alle attività di risk management.

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

Introduzione e visione d'insieme

Anche quest'anno la situazione italiana in ambito cyber security è stata fotografata da Fastweb che nel corso del 2019 ha raccolto ed esaminato attraverso il proprio Security Operations Center oltre 43 milioni di attacchi informatici (in aumento dell'1% rispetto agli eventi rilevati per il Report 2019) transitati sulla sua infrastruttura.

Dall'analisi degli attacchi sulla propria rete (l'Autonomous System di Fastweb è costituito da oltre 6,5 milioni di indirizzi IP pubblici su ognuno dei quali possono comunicare fino a centinaia di dispositivi e server attivi presso le reti dei clienti) Fastweb ha così potuto rilevare alcuni macro trend.

Accanto a una forte crescita dei malware che coinvolgono per la maggior parte le utenze domestiche si evidenzia, rispetto agli anni scorsi, una importante e positiva riduzione (dal 30% al 7%) degli attacchi di natura DDoS verso le Pubbliche Amministrazioni, verosimilmente un effetto derivante dell'introduzione di strumenti di difesa acquisiti dagli enti pubblici attraverso l'adesione alla convenzione SPC per i servizi di cybersecurity.

A fronte dell'aumento del numero di attacchi DDoS, soprattutto verso il mondo del gaming e dei settori finance/insurance si rileva però che il progressivo consolidamento delle tecniche di difesa e dei metodi di mitigazione all'interno delle aziende così come delle pubbliche amministrazioni ha influito positivamente sulla durata degli attacchi che si è sensibilmente ridotta. La diminuzione delle durata a meno di 3 ore per il 95% degli attacchi costituisce un chiaro indicatore dell'efficacia delle misure adottate dai centri di competenza per il contrasto al cybercrime.

Dall'analisi sulla situazione italiana appare inoltre evidente un cambiamento nella "geografia" degli attacchi. Attraverso l'utilizzo di proxy "ponte" diventa infatti sempre più difficile individuare il Paese "nativo" da cui realmente proviene l'attacco, un fenomeno sempre più diffuso che richiede l'adozione di strumenti di difesa sempre più sofisticati a contrasto.
Nei paragrafi a seguire il dettaglio dei fenomeni rilevati.

Dati analizzati

I dati raccolti dal Security Operation Center di Fastweb sono stati arricchiti, analizzati e correlati con l'aggiunta di quelli forniti da organizzazioni esterne come ad esempio la Shadowserver Foundation, fonte autorevole 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 dervice, 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.

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 ha avuto una leggera flessione rispetto alla precedente rilevazione dell'anno 2018. Infatti quest'anno sono state individuate 165 famiglie di software malevoli (-23% rispetto all'anno precedente).
Andromeda raggiunge il 28% delle minacce riscontrate. A livello di comportamento questa è una piattaforma che è utilizzata per distribuire una galassia di varianti di malware (80 famiglie circa) tra cui ransomware, trojan bancari, robot spam, malware antifrode e altro ancora. Ciò che ha reso Andromeda un prodotto estremamente interessante è stata la sua natura modulare.

Un primo modulo, per poche centinaia di dollari consente di acquistare il plug-in keylogger per leggere i dati della tastiera della vittima oppure, per una cifra poco superiore, il plug-in Formgetter, con il compito di acquisire i dati inviati dal browser web del computer infettato. 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".
Al terzo posto troviamo invece Qsnatch. È impressionante come questo malware abbia avuto una forte campagna di diffusione nei mesi di novembre e dicembre e sia già ai primi posti della classifica dei malware più diffusi per il 2019.
Tale malware che si diffonde sulle unità NAS (network access storage) prende il controllo completo del dispositivo ed è in grado di bloccare patch e aggiornamenti software. Ancora non è noto come sarà utilizzata questa nuova arma, anche se i ricercatori pensano che potrà essere usata per campagne di tipo DDoS o per criptomining.
Infine rileviamo una piccola percentuale di software malevoli (0,34%) che non sono ancora stati catalogati di cui non si conoscono tutti i dettagli.

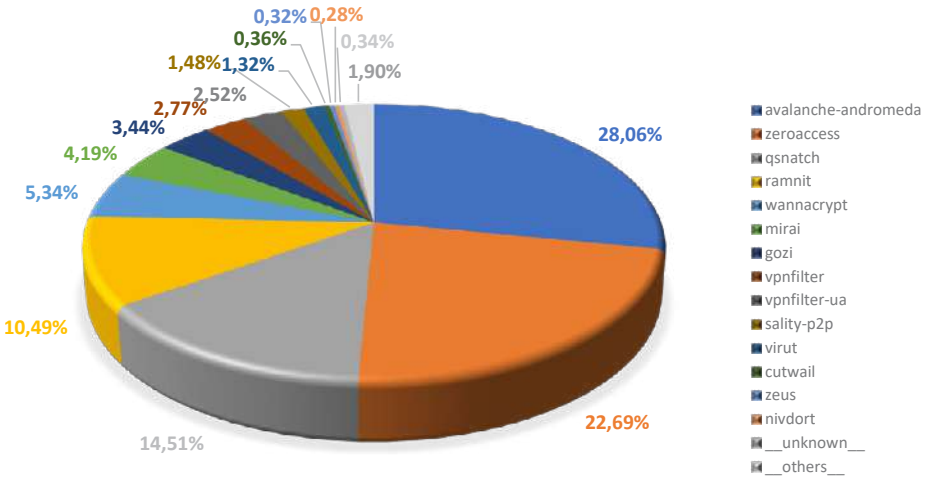


Figura 1 - *Analisi dei Malware rilevati (Dati Fastweb relativi all'anno 2019)*

Andamento temporale

Il grafico della **Figura 2** mostra la diffusione temporale degli host infetti e parte di botnet per l'anno 2019. Come si può notare, dopo il calo registrato nel 2018, il trend 2019 è in forte ascesa.

Da evidenziare il picco di circa 6000-7000 host infetti durante il mese di novembre/dicembre dovuto proprio alla vulnerabilità identificata su alcuni dispositivi NAS e che ha portato alla forte diffusione di QSnatch descritta nel paragrafo precedente.

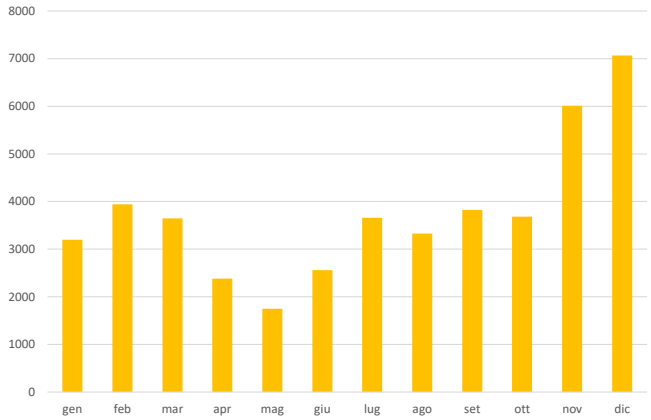


Figura 2 - *Distribuzione temporale del numero di Malware rilevati (Dati Fastweb relativi all'anno 2019)*

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 infezioni legate ad Andromeda e Qsnatch.
È importante evidenziare come, nella prima metà dell'anno si siano rilevati eventi relativi a minacce da malware e botnet legate a Nivdort, Zeroaccess e Ramint. 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 febbraio 2019.

Per quanto concerne le tipologie di attacco zero-day il trend è stato abbastanza costante e in forte calo rispetto al 2018 anche se per nostra esperienza la tipologia, la potenza e l'efficacia di tali attacchi sono comunque da non sottovalutare.
Tali tipologie di attacchi sono infatti più pericolose della media perché non rilevabili da sistemi di protezione tradizionali che necessitano il rilascio di signature per identificarli (ad esempio gli antivirus).

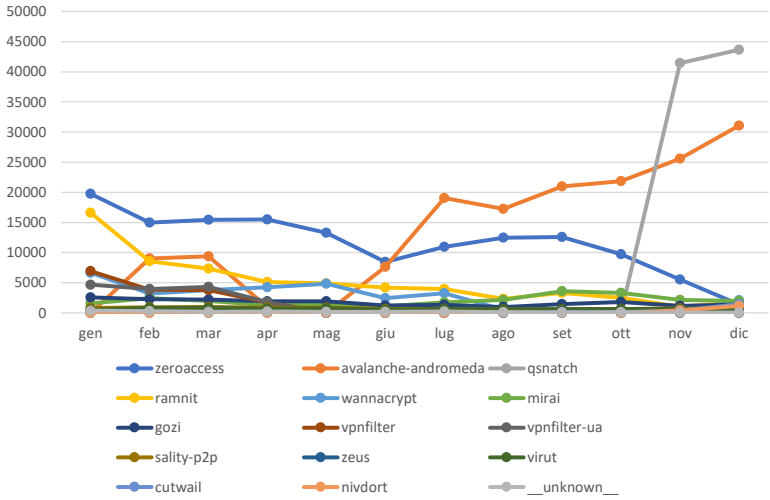


Figura 3 - *Rilevazione mensile dei Malware (Dati Fastweb relativi all'anno 2019)*

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.

Quest'anno oltre l'82% dei centri di C&C relativi a macchine infette appartenenti all'AS di Fastweb si trovano negli Stati Uniti. Tale dato è in forte crescita rispetto all'anno scorso (+30 p.p.) principalmente dovuto alla altissima presenza di datacenter/server farm che si concentrano negli Stati Uniti. Al secondo posto, con l'8% circa dei centri di comando e controllo si trova la Germania.

Conseguentemente perdono efficacia le logiche di difesa basate sulla provenienza geografica degli attacchi, perché le organizzazioni cyber-criminali impiegano indirizzi IP distribuiti opportunisticamente in reti che generano grandi volumi di traffico legittimo. Non è pertanto rilevante da dove proviene l'attacco ma come proteggersi. Risulta quindi necessario attuare meccanismi di protezione che si basino su tecnologie all'avanguardia e centri di competenza specifici come ad esempio l'utilizzo di Security Operation Center o personale specializzato.

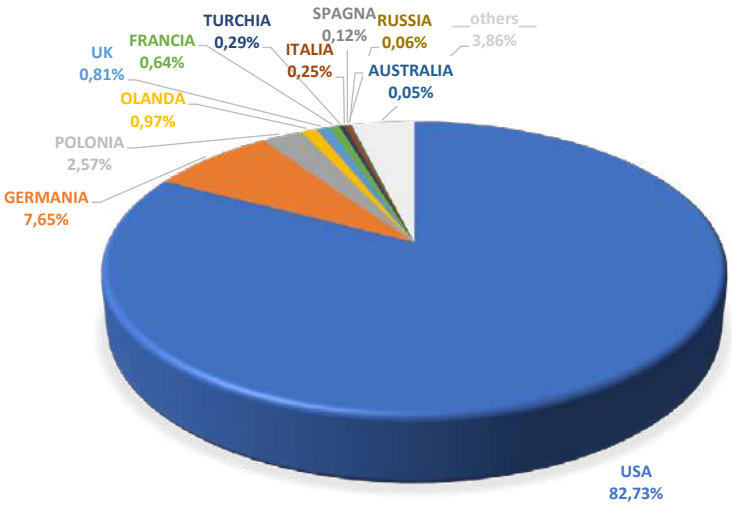


Figura 4 - *Dislocazione dei centri di Comando e Controllo (Dati Fastweb relativi all'anno 2019)*

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 ed il costo del servizio si aggira sui 5-10$ mese per botnet in grado di erogare un attacco di 5-10 minuti ad oltre 100Gbps.
Quanti sono stati gli attacchi DDOS nel 2019?
Nel 2019 sono state rilevate oltre 15.000 anomalie riconducibili a possibili attacchi DDoS diretti verso i Clienti Fastweb (+58% rispetto allo stesso periodo del 2018).

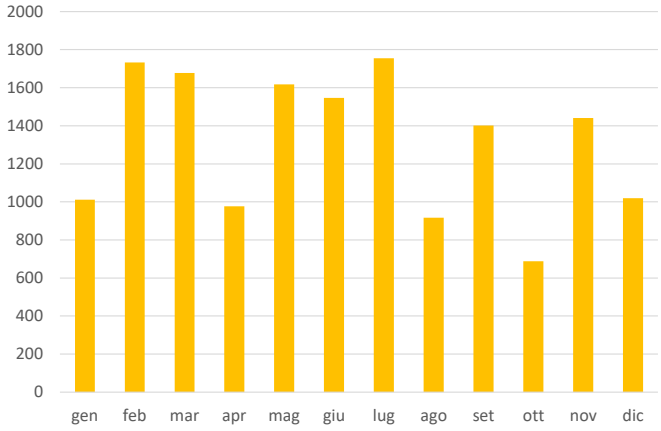


Figura 5 - *Distribuzione mensile delle anomalie DDoS (Dati Fastweb relativi all'anno 2019)*

Quali sono i settori più colpiti

Abbiamo voluto fornire maggiori dettagli in merito alla distribuzione dei target degli attacchi DDoS andando ad esplicitare i settori merceologici maggiormente colpiti da questo tipo di attacchi.

Come si evince dal grafico di **Figura 6**, il fenomeno riguarda senza esclusione un esteso numero di settori tra i quali i più esposti risultano essere il mondo del gaming e il mondo del Finance/Insurance che sono obiettivo nel 40% dei casi, a seguire il mondo dei servizi, quindi il settore Media, Service Provider e il mondo della pubblica amministrazione.

Quest'ultima registra un forte calo rispetto all'anno scorso passando dal secondo settore più attaccato con il 30% degli attacchi complessivi al 7% degli attacchi nel 2019, verosimilmente per effetto del consolidamento delle tecniche di difesa introdotte dalla Pubblica amministrazione che la rendono un bersaglio meno remunerativo per il cyber crime.

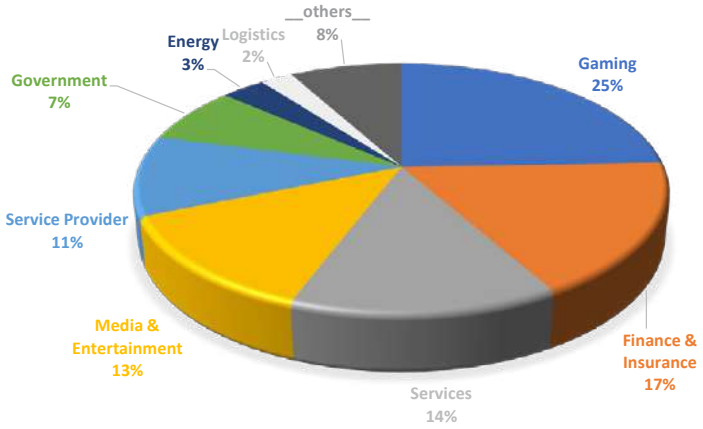


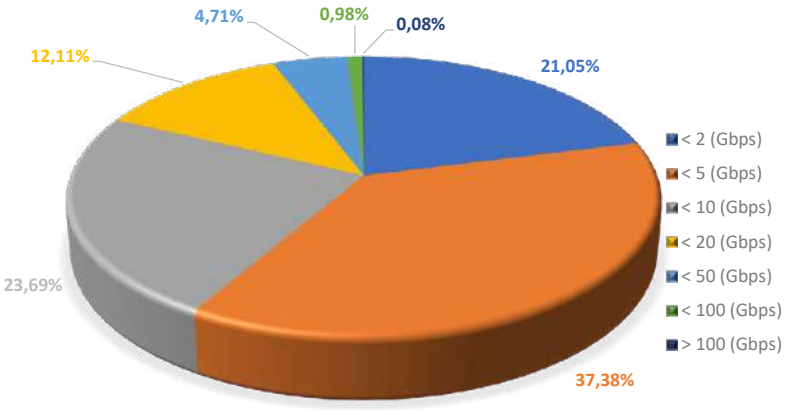
Figura 6 - *Target di possibili attacchi DDoS (Dati Fastweb relativi all'anno 2019)*

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 700 Gbps e i 1.8 Tbps.
Come si può notare il trend è costante, con una leggera flessione nella seconda metà dell'anno.

Figura 7 - *Banda totale mensile impegnata negli attacchi DDoS (Dati Fastweb relativi all'anno 2019)*

Di seguito invece riportiamo la distribuzione della banda media di un attacco DDoS nel 2019.



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. Anche quest'anno tale trend è confermato, risulta quindi evidente come ci sia una crescente consapevolezza da parte delle vittime degli attacchi e come queste utilme investano per garantire alla propria azienda la protezione da attacchi di tipo DDoS.

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 solo una piccola parte degli attacchi dura oltre le 24 ore consecutive. Rispetto all'anno precedente non si notano particolari differenze, soprattutto se si considerano gli attacchi di piccola durata.

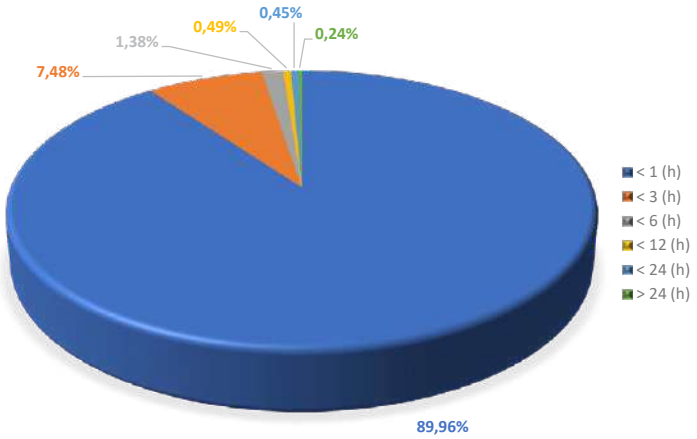


Figura 8 - *Durata dei possibili attacchi DDoS (Dati Fastweb relativi all'anno 2019)*

Tecniche di attacco utilizzate

Le tecniche di attacco utilizzate possono essere diverse, nell'anno 2019 abbiamo rilevato tre principali tipologie ricorrenti con una prevalenza di attacchi di tipo "DNS Amplification". Tale attacco che quest'anno ha registrato il 25% 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 invece è "NTP Amplification" che raggiunge circa il 12% 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.

La terza tecnica di attacco più utilizzata (10%) è "IP Fragmentation" ovvero un tipo di attacco Distributed Denial of Service (DDoS) che sfrutta il principio di frammentazione del protocollo IP. In effetti, il protocollo IP è previsto per frammentare i pacchetti di grandi dimensioni in differenti pacchetti IP che possiedano ognuno un numero sequenziale e un numero di identificazione comune. Una volta ricevuti i dati, il destinatario riordina i pacchetti grazie ai valori di spaziatura (in inglese offset) da questi contenuti. L'attacco da frammentazione più conosciuto è l'attacco Teardrop. Il principio dell'attacco Teardrop consiste nell'inserire in alcuni pacchetti frammentati delle informazioni di spaziatura sbagliate. In questo modo, al momento dell'assemblaggio vi saranno dei vuoti o degli

intervalli (overlapping), che possono provocare un'instabilità di sistema o una saturazione delle risorse.

Infine è da evidenziare come gli attacchi combinati (tecnica mista) sono aumentati sensibilmente dall' 8% del 2018 al 40% del 2019. Tale fenomeno è indice del fatto che attacchi diversificati hanno maggiore probabilità di essere efficaci a causa della loro maggiore complessità per gestire la controparte difensiva.

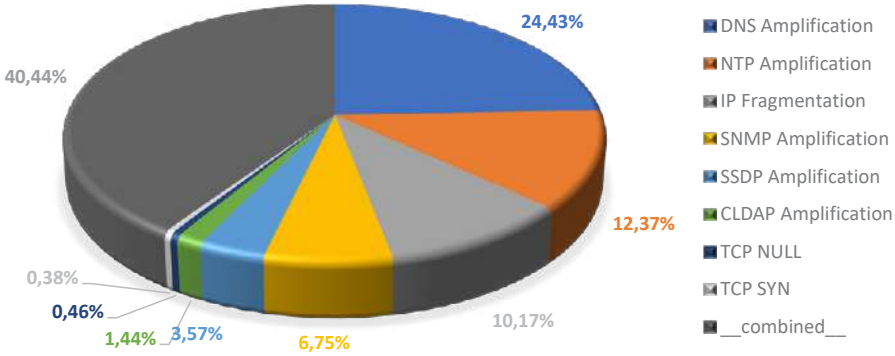


Figura 9 - *Tipologie di attacchi DDoS (Dati Fastweb relativi all'anno 2019)*

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 2019 riportano circa 66.000 macchine che espongono servizi critici direttamente su Internet con un incremento rispetto all'anno scorso di circa il 14%.
Al primo 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, al secondo posto troviamo Telnet, protocollo utilizzato per la gestione di host remoti, accessibile da riga di comando.
Di rilievo è anche la quantità di macchine che espongono RDP, utilizzato per la connessione remota ad un PC. Un attaccante potrebbe sfruttare questo protocollo per prendere il controllo completo della macchina.

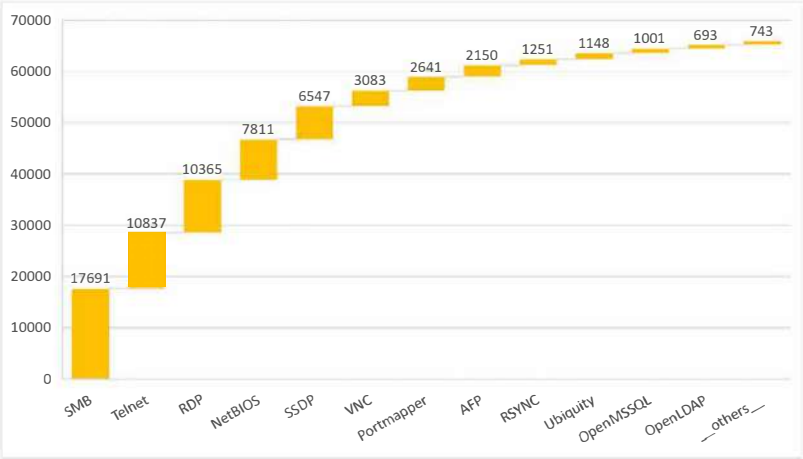


Figura 10 - *Servizi esposti direttamente su Internet (Dati Fastweb relativi all'anno 2019)*

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 7.374 IP sono stati inseriti almeno una volta nelle blacklist durante il 2019. Il dato è in sensibile calo rispetto al 2018 dove avevamo registrato oltre 10.500 azioni di blacklisting. Il grafico di seguito rappresenta le città maggiormente colpite.

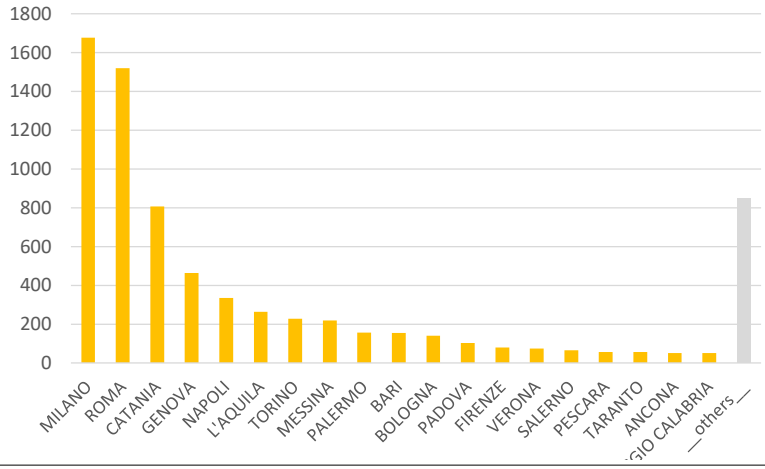


Figura 11- *Host in Blacklist per città (Dati Fastweb relativi all'anno 2019)*

Stato della cybersecurity nel sud Italia

[Uno studio realizzato da Vita Santa Barletta (Università degli Studi di Bari), Danilo Caivano (Università degli Studi di Bari) e Domenico Raguseo (Exprivialltaltel S.p.a.)].

Introduzione

Il rapporto Clusit 2019 ha evidenziato come il numero di attacchi sia cresciuto notevolmente nel 2018, +37,7 % rispetto al 2017, con una media di 129 attacchi al mese.
Uno scenario piuttosto preoccupante, considerando anche le differenti tipologie di attacco: *attacchi comuni* che sfruttano le vulnerabilità note, *attacchi avanzati* che sfruttano invece vulnerabilità complesse e talvolta sconosciute (zero-day), *attacchi emergenti* che vengono eseguiti da aggressori sofisticati che studiano nuovi pattern di attacco su nuove tecnologie.
Le organizzazioni devono essere resilienti in tale contesto ed avere una chiara percezione del rischio che caratterizza gli attacchi informatici ai quali far fronte.
Partendo da tale considerazione e analizzando i dati forniti dal Clusit lo scorso anno sulla sicurezza ICT in Italia, abbiamo condotto uno studio quali-quantitativo sullo stato della sicurezza informatica nel Sud Italia.

Obiettivo dello studio

Esfiltrazione dati mediante accesso non autorizzato ai sistemi o perdita di dati dovuta ad un'infezione da cryptolocker, vittime di phishing o truffe online, sono solo alcuni degli scenari possibili e in continuo aumento. Un fattore su tutti emerge con chiarezza: "**Una percezione errata della sicurezza informatica**".
Per molte persone installare un antivirus equivale a garantire la sicurezza dei propri dati e del proprio dispositivo; per molte aziende, invece, tale garanzia di sicurezza è estesa ad un firewall perimetrale e ad un antivirus sui pc; per tanti studi professionali è superflua *"…Il rischio che la mia azienda subisca un attacco informatico è quasi nullo, perché mi occupo solo di trattamenti osteopatici…"*, o ancora *"…Perché investire in sicurezza quando il mio lavoro è generare benessere del corpo?..."*, oppure *"Non sono a contatto con la tecnologia per la maggior parte della giornata, e ciò porta la mia azienda a non subire attacchi"*.
Questa è solo una percezione e il più delle volte completamente errata in quanto ad esempio il trattamento osteopatico somministrato ad un paziente, sottende l'uso di una cartella clinica i cui dati sono memorizzati su un pc o su cloud. Questi sono dati sensibili, che potrebbero essere utilizzati per diversi scopi, anche per ulteriori attacchi.
La sicurezza informatica è spesso erroneamente considerata come una prerogativa di grandi imprese, di istituti governativi o banche. Non è così, anche la piccola impresa, il professionista o il singolo ente rientrano a pieno titolo nel perimetro di potenziale attacco.
Ciò premesso l'obiettivo dello studio è quello di valutare la percezione che gli stakeholder hanno della sicurezza informatica al fine di poter definire strategie di contenimento del rischio applicabili non solo all'infrastruttura IT, ma anche al software utilizzato e all'organizzazione tutta.

A tale scopo è stato realizzato un survey utile a fornire una caratterizzazione quali-quantitativa del fenomeno. Le aree di investigazione sono state:

- tipologia di azienda rispondente;
- attacchi informatici subiti ed eventuali danni rilevati;
- capacità di difendersi in caso di attacco informatico;
- grado di consapevolezza dei dipendenti circa i rischi conseguenti un attacco;
- conformità a standard e regolamenti in ambito privacy e security.

Al survey hanno risposto 212 aziende/enti. Per la sua promozione e somministrazione sono stati utilizzati differenti canali social, Linkedin, Twitter e Facebook, con lo scopo di massimizzare il numero di soggetti coinvolti e potere così fornire una panoramica ampia del fenomeno, soprattutto con riferimento al Sud Italia. Il survey è accessibile al seguente link https://forms.gle/XZ7akxzVRYNGEi7A6.

Analisi dei risultati

Delle 212 risposte raccolte (**Fig. 1**), il 54,5% si riferisce a piccole imprese (fino a 50 dipendenti), il 18,2% a medie (da 51 a 250 dipendenti) e il 27,3% a grandi (oltre 250 dipendenti).

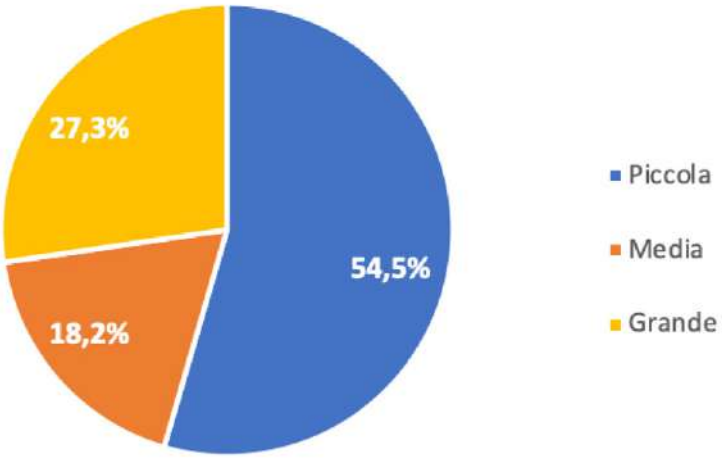


Figura 1 - *Ripartizione del campione intervistato per dimensione*

Il 5,5% si riferisce a soggetti pubblici, l'81,8% privati e, infine, il 12,7% a soggetti pubblico-privato (**Fig. 2**).

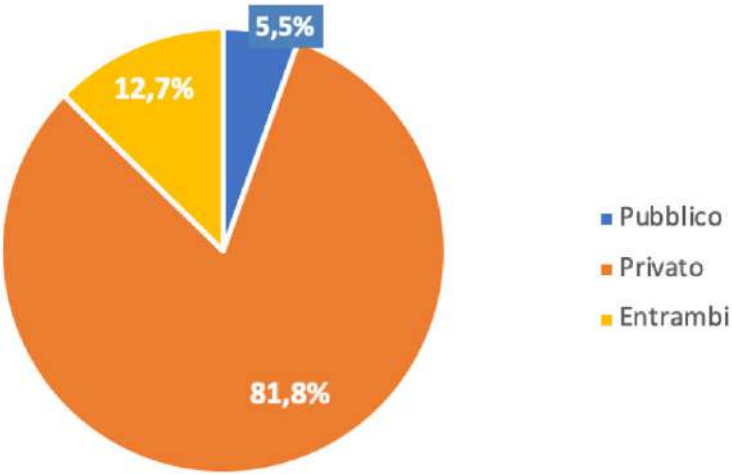


Figura 2 - *Ripartizione del campione intervistato per tipologia*

La **figura 3** presenta invece la distribuzione dei soggetti intervistati per settore di riferimento. Il 32% operano nel settore "Consulting e Software/Hardware Vendor", il 15% in "Governo-Militare", il 9% in "Servizi Online/Cloud", il 10% in "Logistica/Trasporto" e "Turismo". Seguono rispettivamente con il 4% ciascuno, "Banca/Finanza", "Grande Distribuzione e Vendita al dettaglio" e "Studi di Ingegneria", e con il 2% ciascuno i settori "Critical Infrastructures", "Cyber Security", "Energia", "Estetica", "Industria", "Osteopatia", "Pubblica Amministrazione", "Rappresentanza politico sindacale", "Research-Education", "Ristorazione", "Servizi alle imprese" e "Social".

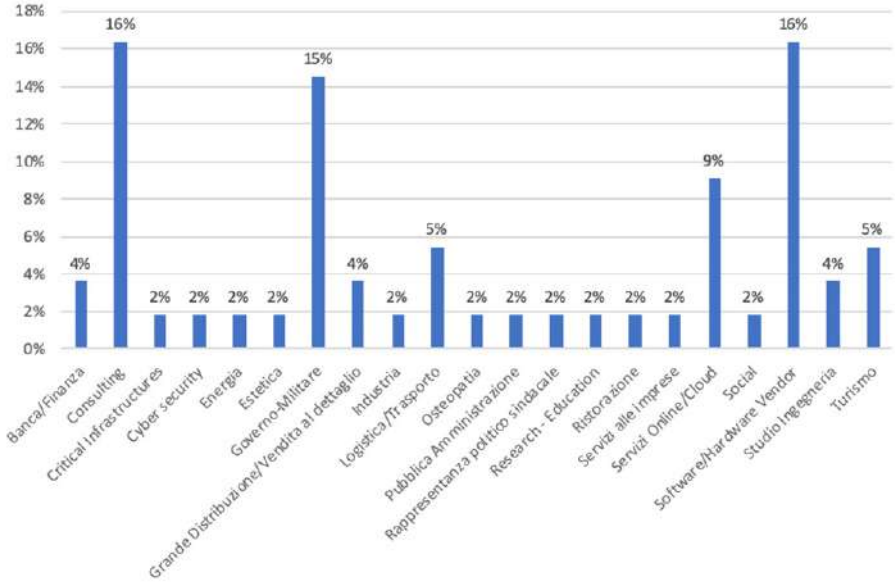


Figura 3 - *Ripartizione del campione intervistato per settore di appartenenza*

Procedendo con l'investigare gli attacchi nel corso del 2019, si ha che il 34,5% del campione ha subito attacchi informatici. Il 65,5% ha dichiarato, invece, di non essere stato soggetto ad attacchi informatici (**Fig. 4**).

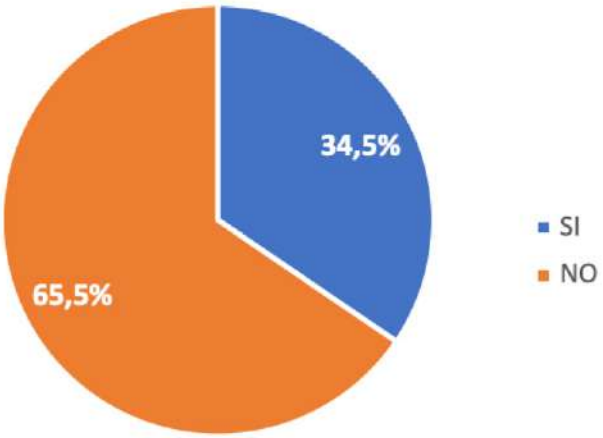


Figura 4 - *Distribuzione dei soggetti vittima di attacchi nel corso del 2019*

I danni subiti sono stati valutati trascurabili per il 52,5% dei soggetti coinvolti, bassi per il 15,8%, di media entità per il 21,1%, alti e molto alti per il 10,6% (**Fig. 5**).
La tipologia di danni subiti (**Fig. 6**) risulta essere per il 26,2% riconducibile ad una perdita/esfiltrazione di dati, per il 21,7% ad un danno di immagine, per il 17,4% di natura economica, il 13% di tempo, l'8,7% di tipo fisico/infrastrutturale. Mentre il 13% non ha rilevato alcun danno a seguito dell'attacco ricevuto.

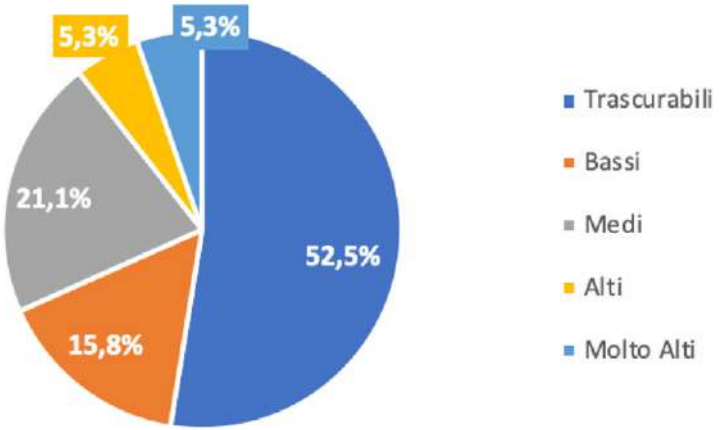


Figura 5 - *L'azienda/ente come valuta i danni subiti*

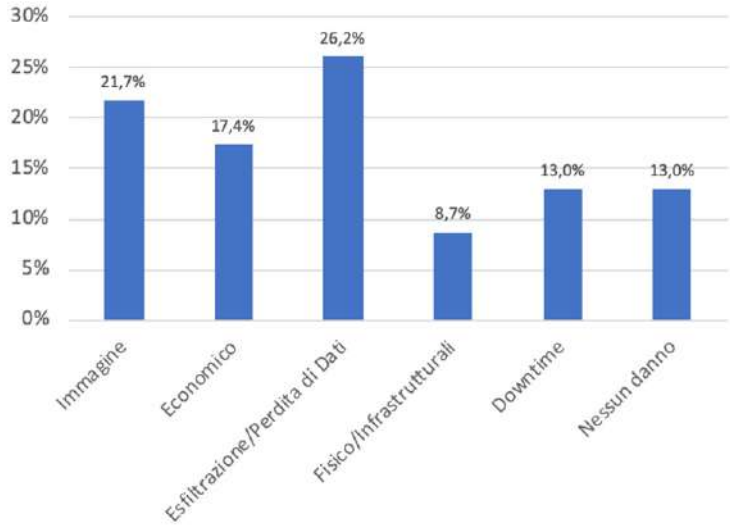


Figura 6 - *Ripartizione del campione per tipo di danni subiti*

Per quanto riguarda la capacità dei soggetti intervistati di difendersi in caso di attacco informatico, il 43,7% si ritengono pienamente in grado di difendersi, il 21,8% sufficientemente capaci, il 23,6% poco e solo il 10,9% dei soggetti si ritiene incapace di difendersi (**Fig. 7**).

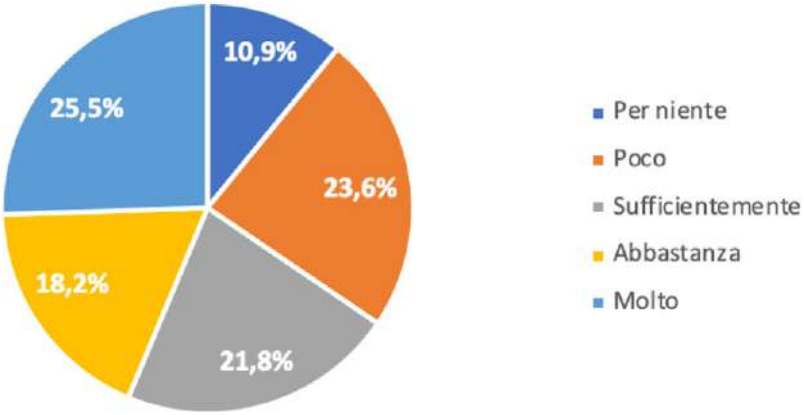


Figura 7 - *Ripartizione del campione per capacità di difesa da attacchi informatici*

La **figura 8** mostra la ripartizione del campione intervistato per grado di conformità a standard e regolamenti in ambito privacy e security. Il 27,3% si dichiara completamente conforme, il 29% di esserlo abbastanza. Il 30,9% ritiene di esserlo sufficientemente, il 7,3% poco e il 5,5% per niente. Di conseguenza è possibile affermare che la maggioranza del campione si ritiene conforme a regolamenti e standard in ambito privacy e security.

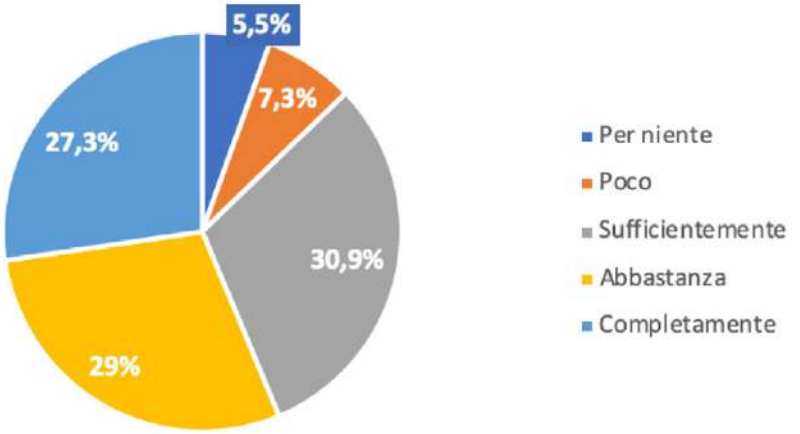


Figura 8 - *Ripartizione del campione intervistato per grado di conformità a standard e regolamenti in ambito privacy e security*

Per quanto concerne la percezione circa la probabilità di un attacco informatico, il 32,7% lo ritiene altamente possibile il 34,5% sufficientemente probabile. Mentre il 25,5% lo ritiene poco probabile e solo il 7,3% ritiene nulla la probabilità (Fig. 9).
In contro tendenza sono invece i dati relativi al grado di consapevolezza dei dipendenti circa i rischi conseguenti ad un attacco informatico (Fig. 10). Solo il 18,2% e il 12,7% dei soggetti intervistati dichiarano rispettivamente una consapevolezza molto alta e abbastanza alta. Il 32,7% e il 36,4%si dicono invece poco o per niente consapevoli.

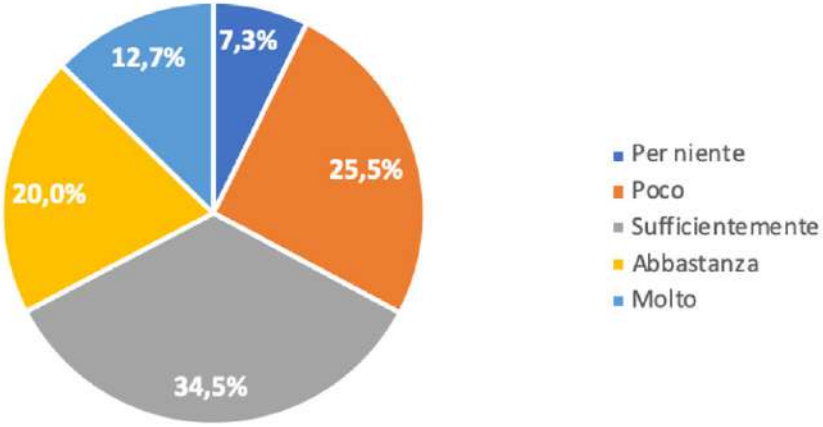


Figura 9 - *Ripartizione del campione intervistato per probabilità di attacco informatico*

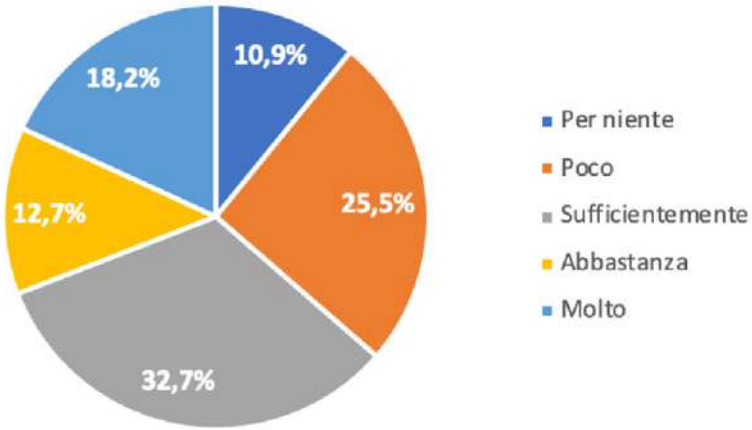


Figura 10 - *Ripartizione del campione intervistato per grado di consapevolezza sui rischi conseguenti un attacco*

Il 43,6% dei soggetti intervistati dichiara che all'interno della propria azienda si tengono corsi di formazione specifici sulla sicurezza mentre i restanti 56,4% dichiara di no (**Fig.11**). Analizzando, invece, la percezione del campione circa la necessità di formazione specifica sulla sicurezza informatica, si evince che l'89,1% valuta positivamente la frequenza a corsi, a differenza del 10,9% (**Fig. 12**).

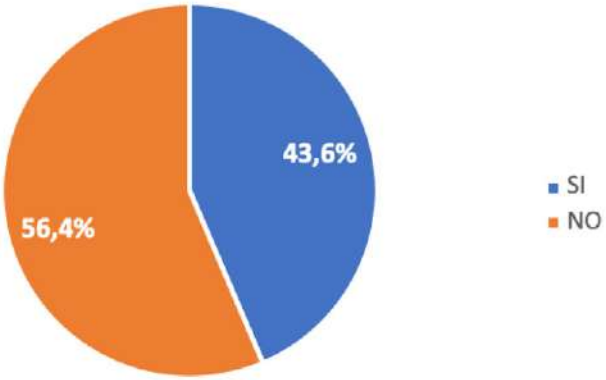


Figura 11 - *Ripartizione del campione intervistato rispetto all'attività formativa svolta sulla sicurezza informatica*

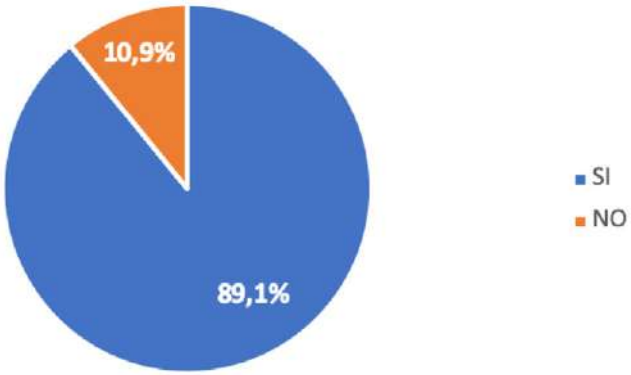


Figura 12 - *Ripartizione del campione intervistato rispetto all'utilità percepita di corsi di formazione sulla sicurezza informatica*

Per quanto riguarda le misure di prevenzioni adottate (**Fig. 13**) dai soggetti intervistati, il 34,8% ricorrono a "Firewall e Data Firewall", il 28,6% ad "Antivirus", il 13,7% a strumenti di "Data Loss Prevention", il 13% utilizzano "Intrusion Prevention System e Intrusion Detection System", l'8,7% SIEM, ed infine l'1,2% non adotta alcun metodo o strumento o non ne è a conoscenza.

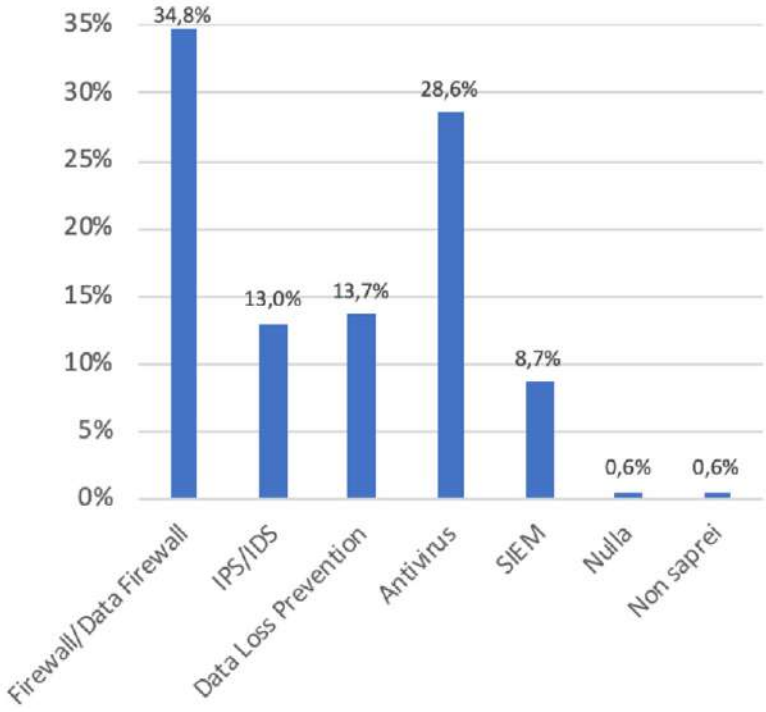


Figura 13 - *Ripartizione del campione intervistato per misure di prevenzione adottate*

Il 61,8% dei soggetti, più della metà del campione, si preoccupa di verificare i requisiti di sicurezza sia durante la fase di acquisto di software/servizi da terze parti, che all'interno dei termini e condizioni di sottoscrizione dei servizi cloud. Il 38,2%, invece, non opera alcuna verifica (**Fig. 14**).

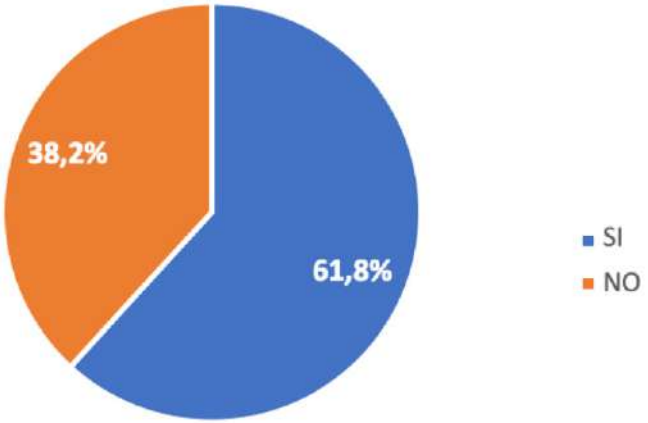


Figura 14 - *Ripartizione del campione intervistato rispetto all'attività di verifica sicurezza in fase di procurement*

Conclusioni

Lo studio condotto sullo stato della sicurezza informatica nel Sud Italia ha complessivamente coinvolto un campione di 212 aziende/enti.
Va evidenziato che i risultati, per quanto significativi, vanno interpretati con cautela e certamente in chiave pessimistica. Coloro che hanno partecipato al survey, per le modalità con cui quest'ultimo è stato promosso ed erogato, hanno un livello di alfabetizzazione informatica medio-alto e rappresentano una percentuale modesta di coloro che giornalmente fanno uso inconsapevole di sistemi e tecnologie digitali.

Molto interessante è lo spaccato dei soggetti intervistati. Si nota, infatti, una grande presenza di piccole aziende (54,5%) di settori estremamente diversificati. Ciò è esattamente quello che con il survey si voleva fare emergere. La sicurezza è un valore non solo per la grande azienda, ma anche le piccole e medie.
Emerge inoltre che la maggior parte del campione analizzato, non ha percezione di aver subito attacchi informatici. Un risultato che suggerisce diverse considerazioni, visto anche quanto emerge dall'attività della Polizia di Stato: molti soggetti tendono a non denunciare un attacco per un senso di vergogna o per non perdere tempo, consapevoli che risalire e punire i colpevoli è molto difficile, oppure perché consapevoli di non adottare colpevolmente quei processi e quelle politiche alla base dalle certificazioni di settore acquisite.
Un altro elemento di confusione è rappresentato dall'assimilare l'attacco all'incidente non distinguendoli. In assenza di un incidente rilevato si tende a considerare inesistente l'attacco. Un attacco potrebbe durare mesi, durante i quali i sistemi vengono compromessi e utilizzati anche per ulteriori attacchi verso terzi, come è accaduto ad esempio per MIRAI.

Di conseguenza, se tale compromissione non è rilevata, la vittima inconsapevole riterrà erroneamente di non aver mai subito un attacco.
Tra coloro che dichiarano di aver subito attacchi, si nota come nella maggior parte dei casi (52,5%) i danni subiti vengano ritenuti di poco conto o irrilevanti. Ciò probabilmente quale effetto degli investimenti operati in sicurezza informatica, il più delle volte a seguito di incidenti subiti in passato o dettati dalla necessità di compliance a certificazioni e regolamenti di settore, che hanno contribuito a limitare gli impatti.
Investimenti che se estemporanei e non inquadrati in una strategia coerente, spesso tendono a rendere estremamente complesse le infrastrutture da gestire, soprattutto in assenza di competenze specifiche. Non a caso l'elevata percentuale (89,1%) di soggetti che ritengono utile la frequenza di corsi di formazione sulla sicurezza informatica malgrado in molti si ritengano comunque esperti nel difendersi. Questa considerazione denota un campione estremamente maturo.

Ringraziamenti

Questo lavoro è stato possibile grazie al prezioso contributo di Antonio De Chirico e Andrea Carnimeo (Polizia di Stato).

Attività e segnalazioni della Polizia Postale e delle Comunicazioni nel 2019

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 2019 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.

C.N.C.P.O.

Il ritmo frenetico delle innovazioni tecnologiche e dei nuovi mezzi di comunicazione, conseguenti alla diffusione di Internet su larga scala e, in particolare, la progressiva diffusione di *smartphones* e *tablets* tra i minori, sono solo alcuni degli elementi che agevolano le forme di aggressione in rete verso l'infanzia e l'adolescenza, determinando, di conseguenza, un notevole incremento non solo di reati che vedono coinvolti i minori online, quali la pornografia minorile e il *cyberbullismo*, ma anche della diffusione di altre forme di aggressione nei loro confronti, come le condotte autolesioniste, le c.d. *challenges* (es.: *Blue Whale, Binge Drinking), etc.*

Considerato che uno degli aspetti propri del web che caratterizzano tali fenomeni, nonché tutte le comunità virtuali, è l'assenza di confini e, quindi, la sopranazionalità, che implica la presenza di utenti che si connettono dall'estero con server attestati in altri Paesi, l'attività di cooperazione internazionale, instaurata nel corso degli anni dal *Centro Nazionale per il Contrasto alla Pedopornografia Online* (C.N.C.P.O.) tramite EUROPOL e INTERPOL, sia con paesi dell'UE, sia extraeuropei, è di assoluta importanza, in quanto consente uno scambio info investigativo, nonché di condivisione di nuove tecniche di indagine e buone prassi nella materia.

In tale contesto, di assoluto rilievo risulta il ruolo svolto dalla Polizia Postale e delle Comunicazioni, in particolare, nell'ambito dei reati relativi allo **sfruttamento sessuale dei minori online**. Nel 2019 sono state indagate **663** persone.

Le indagini relative al fenomeno dell'**adescamento di minori online**, invece, hanno consentito di indagare **189** soggetti.

Per quanto riguarda il preoccupante fenomeno del cyberbullismo, la Polizia Postale e delle Comunicazioni ha trattato 460 casi e indagato 136 minori.

Nell'ambito di tale fenomeno, dal 2017 al 2019 si è registrato un incremento delle vittime con una età inferiore ai 9 anni pari al 300%.

Tra le citate attività di polizia giudiziaria, sono state eseguite **8 operazioni** di particolare rilievo, condotte dagli Uffici territoriali della Specialità e coordinate dal Centro, alcune delle quali svolte in modalità sotto copertura online e scaturite da segnalazioni pervenute nell'ambito dell'attività di cooperazione internazionale svolta dal C.N.C.P.O. che, complessivamente, hanno consentito di indagare in stato di libertà **152** soggetti.

Un fenomeno particolarmente insidioso che ha fatto breccia tra giovani e giovanissimi è rappresentato dagli *stickers*, fenomeno in crescente diffusione, che consiste nella condivisione, sulle piattaforme di messaggistica istantanea, di *adesivi digitali* gratuiti, a contenuto offensivo, violento, discriminatorio, antisemita, nonché pedopornografico.
Le piattaforme di messaggistica istantanea hanno offerto agli utenti la possibilità di utilizzare, accanto a *emoji* (simboli pittografici, simili agli emoticon e utilizzati negli SMS, nelle e-mail, nonché nei social), pacchetti di *stickers* messi a disposizione dai sistemi di messaggistica istantanea che offrono la possibilità di crearne di personalizzati e modificati ricavandoli da fotografie reali, tramite diverse "Applicazioni" gratuite, disponibili per IOS e Android.
Negli ultimi tempi, questo tipo di servizio sta ricevendo il consenso degli utenti preadolescenti e adolescenti, i quali, tuttavia, spesso ne fanno un uso improprio, diffondendo adesivi digitali dai contenuti illeciti (pedopornografici, xenofobi, discriminatori, etc.) ed esponendosi a responsabilità penali relative alla diffusione e divulgazione di materiale pedopornografico.
Negli ultimi mesi del 2019 sono stati rilevati **7** casi di *stickers* trattati da questa Specialità, conclusisi con altrettanti minori indagati per diffusione e detenzione di materiale pedopornografico.

Inoltre, tra le indagini più significative avviate direttamente dal Centro nell'ambito dei reati di sfruttamento sessuale dei minori, si segnala una complessa operazione, svolta in modalità sotto copertura online nelle ***Dark Net***, che ha consentito di trarre in arresto un 60enne per detenzione di materiale di sfruttamento sessuale dei minori, aggravato dall'ingente quantità, dall'utilizzo di mezzi di anonimizzazione e criptazione, nonché dalla particolare violenza di alcune immagini rinvenute, raffiguranti abusi sessuali su minori anche in tenerissima età. L'uomo è risultato di particolare interesse, anche a livello internazionale, per i ruoli di amministratore e moderatore che nel tempo ha ricoperto nelle comunità virtuali pedofile.

Per quanto concerne l'attività di prevenzione svolta dal C.N.C.P.O. attraverso una continua e costante attività di monitoraggio della rete, sono stati individuati **47.267** siti internet, di cui **2.295** inseriti in *black list* e oscurati in quanto presentavano contenuti pedopornografici.

Sezione operativa

Nell'ambito dei **reati contro la persona** perpetrati sul web, nel 2019 sono state indagate **1129** persone di cui **361** per aver commesso estorsioni a sfondo sessuale, stalking, molestie e minacce sui social network.
Risultano in costante aumento le **diffamazioni on line**, soprattutto ai danni di persone che ricoprono incarichi istituzionali o comunque conosciute dal grande pubblico: **2502** i casi trattati e **770** le persone indagate.
Una particolare rilevanza ha assunto l'attività di contrasto al **revenge porn**, un fenomeno

in continua crescita, per il quale sono **24** le persone indagate. Purtroppo i dati non rispecchiano la gravità e l'estensione del fenomeno, a causa della ritrosia a denunciare di molte persone.

Grande impegno è stato profuso al contrasto dei reati d'incitamento all'odio: sono oltre **2000** gli spazi virtuali monitorati nel 2019 per condotte discriminatorie di genere, antisemite, xenofobe e di estrema destra.

Si registra la continua crescita delle **truffe on line**: nel 2019 sono state ricevute e trattate oltre **196.000** segnalazioni che hanno consentito di indagare **3730** persone. Sempre più sofisticate sono state le condotte fraudolente commesse sulle piattaforme di e-commerce.
Sono aumentate le cosiddette **truffe romantiche**, che vedono come vittime delle donne di età compresa tra i 40 e i 60 anni, circuite da uomini conosciuti in rete e indotte con stratagemmi sentimentali a versare ingenti somme di denaro a truffatori senza scrupoli.
Si è evidenziato un significativo aumento del fenomeno delle **truffe** legate al **trading online**: molti utenti della rete, allettati dalla prospettiva di facili guadagni derivanti da investimenti "sicuri", sono caduti nella rete di abili truffatori e finti intermediari finanziari investendo centinaia di migliaia di euro.

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 nel 2019, rispetto al 2018, ha visto un aumento di oltre il 30%, sino a raggiungere **82484** alert.
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 dalla costante attività di monitoraggio in contesti di interesse.
Il C.N.A.I.P.I.C. - Centro Nazionale Anticrimine Informatico nell'ambito del complessivo Sistema Informativo Nazionale per il Contrasto al Cyber Crime, progetto SINC3 finanziato con fondi ISF, ancora in fase di completamento e che mira ad estendere la rete di protezione cibernetica anche alle realtà più sensibili del Paese, ha gestito complessivi **1181** attacchi cyber significativi, di cui:

- **243** attacchi informatici nei confronti di servizi internet relativi a siti istituzionali e infrastrutture critiche informatizzate di interesse nazionale;
- **938** attacchi informatici diretti verso aziende sensibili e pubbliche amministrazioni locali;
- **79** richieste di cooperazione nell'ambito del circuito "High Tech Crime Emergency".

Tra le attività investigative condotte, in tale ambito, si segnalano **155** indagini avviate nel **2019,** per un totale di **117** persone indagate**.**

Nell'ottica di un'efficace condivisione operativa, nel 2019 il Centro ha proseguito la stipula di specifici Protocolli a tutela delle infrastrutture critiche nazionali.
Si rappresenta, altresì, che analoghe forme di collaborazione, nell'ambito del progetto SINC3, 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.

Cyberterrorismo

Nell'ambito della prevenzione e del contrasto al terrorismo internazionale di matrice jihadista e, in particolare, ai fenomeni di radicalizzazione sul web, il personale della Polizia Postale e delle Comunicazioni effettua quotidianamente il monitoraggio del web, affiancato da qualificati mediatori linguistici e culturali, il cui contributo, per la peculiarità della materia e dei relativi contenuti multimediali presenti sulla rete, fornisce un valore aggiunto di fondamentale importanza.

Come noto, infatti, il web assurge ad 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.

In tale contesto, la Specialità ha svolto attività sia di iniziativa, che su specifica segnalazione, anche grazie alle informazioni pervenute dai cittadini tramite il Commissariato di P.S. Online, al fine di individuare i contenuti illeciti presenti all'interno degli spazi e servizi di comunicazione *online* di ogni genere, come, ad esempio, siti, weblog, forum, board, social network e gruppi chiusi presenti su piattaforme di comunicazione.

L'attività, funzionale al contrasto dei fenomeni di radicalizzazione e cyberterrorismo, ha portato al monitoraggio di oltre **36.000** spazi web.
Appare opportuno evidenziare come l'attività di monitoraggio del web effettuata negli ultimi mesi da questa Specialità abbia permesso di riscontrare come l'attuale struttura centrale dell'apparato di propaganda del *Daesh*, con produzione mediatica più o meno costante nel tempo, risulti essere costituita da vari *Media Center* insistenti nelle province del Califfato che, mentre in passato risultavano dotati di canali di comunicazione propri, oggi si appoggiano ai c.d. *Supporter Generated Content* per la diffusione del materiale di propaganda.

Si tratta, dunque, di una struttura basata su una miriade di *account*, attivati quotidianamente da singoli *cyber mujahid* (supporter del Califfato sui media) o in forma automatizzata tramite apposite strutture dipendenti dal *Daesh* e deputate al mantenimento dell'operati-

vità mediatica, per fare fronte all'azione restrittiva messa in atto dagli amministratori delle piattaforme Social, con l'obiettivo di divulgare *magazine online* del Califfato, aggiornamenti sulle attività dei combattenti nei teatri operativi, video, documenti, manuali o pubblicazioni di esponenti di spicco della corrente radicale islamica, infografiche di minaccia etc.

Al fine di contrastare tale strategia di comunicazione dell'IS, personale del Servizio Polizia Postale e delle Comunicazioni ha partecipato agli "Action Day" che si sono svolti nel mese di novembre 2019 presso la sede di Europol, a L'Aia, e che hanno coinvolto, oltre a tutte le Forze dell'Ordine degli Stati Membri, anche i rappresentanti dei maggiori *Internet Service Provider*, tra cui *Telegram* – che è stato il fornitore di servizi online che ha ricevuto la maggior parte delle richieste di *referral* e che ha allontanato dalla propria piattaforma una parte significativa degli attori chiave all'interno della rete di diffusione della propaganda IS – nonché *Google, Files.fm, Twitter, Instagram* e *Dropbox*.

In tale contesto, dunque, le attività poste in essere hanno permesso di ottenere un massiccio "*take down*" di migliaia di gruppi, canali e *account* (molti dei quali oggetto di un precedente accesso abusivo e un successivo impiego come *bots*) che sono stati oggetto di preventiva segnalazione da parte del *law enforcement*, in quanto considerati responsabili della pubblicazione del settimanale di settore *al-Naba*.

Nella medesima circostanza, inoltre, mediante un rilevante lavoro di monitoraggio e *Open Source Intelligence,* si è provveduto all'analisi dei tentativi di reazione da parte dei *cyber mujahid*, e all'immediato contrasto delle prove di ricostruzione della macchina di propaganda *online* dell'IS.

Appare evidente, dunque, come il carattere transnazionale delle operazioni descritte, sia per la natura internazionale del fenomeno, che per la stessa connaturata struttura della rete, determini l'imprescindibile attivazione efficiente di strumenti di cooperazione sovranazionale che riescono ad apportare un indiscusso valore aggiunto alle attività di prevenzione messe in atto dalle diverse Forze di Polizia nazionali.

Ad ulteriore conferma della proiezione internazionale del Servizio Polizia Postale e delle Comunicazioni, quale 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), appare opportuno segnalare la partecipazione di propri operatori anche al "CBRNE Action Day", che si é svolto sempre presso la sede di Europol alla fine del mese di novembre 2019.

Financial cybercrime

Con riferimento al **financial cybercrime,** le statistiche del 2019 fanno registrare ben **6854** casi a livello nazionale.
Il fenomeno del phishing, finalizzato alla captazione illecita di codici personali e dati sensibili, conosce un notevole aumento soprattutto attraverso il ricorso a malware e siti-clone. In aumento, tuttavia, sono anche i casi riguardanti il cd. "Vishing" (phishing vocale) e "Smishing" (phishing attraverso messaggi ed sms).
La violazione dei sistemi bancari di privati e imprese vede un aumento nel ricorso alle tecniche criminali del cd. Sim-Swap (vedi *infra*).
Il tessuto economico-produttivo del Paese continua ad essere oggetto degli attacchi noti a livello mondiale con le espressioni BEC e CEO Fraud. Scopo delle organizzazioni criminali è quello di intromettersi nei rapporti commerciali tra aziende dirottando ingenti somme verso conti correnti nella disponibilità dei truffatori. 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 provento di frode informatica, 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 2019, la Specialità ha potuto bloccare e recuperare alla fonte, su una movimentazione di **21.333.990 €,** ben **18.000.000 €.**

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, con riferimento al fenomeno del **cyber-riciclaggio**, di rilievo è la recente operazione internazionale denominata "**Emma5"**, coordinata dal Servizio Polizia Postale e delle Comunicazioni con la collaborazione di **24 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 e denunciare **170 *money mules*.**

Le transazioni fraudolente sono state **374**, per un totale di circa **10 milioni di euro,** di cui **circa 3.5 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.

Attività di prevenzione

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 settima edizione della campagna itinerante della Polizia Postale e delle Comunicazioni "***Una Vita da Social***", grazie alla quale sino ad oggi sono stati incontrati oltre **2 milioni di studenti**, **220.000 genitori, 125.000 insegnanti** per un totale di **17.000 Istituti scolastici** e **300** 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 migliaia di studenti, attraverso la proiezione di un docufilm e le testimonianze dirette dei minori vittime di prevaricazioni, vessazioni e violenze online.

Inoltre nel corso del 2019 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.

Commissariato di PS online

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 e usufruire dei medesimi servizi di segnalazione, informazione e collaborazione che la Polizia Postale e delle Comunicazioni quotidianamente e 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	**22.853**
Segnalazioni ricevute dai cittadini	**23.311**
Denunce presentate dagli utenti	**10.571**

Le attività del Nucleo Speciale Tutela Privacy e Frodi Tecnologiche della Guardia di Finanza nel 2019

In un sempre più complesso contesto in cui la componente tecnologica permea senza soluzione di continuità le abitudini e la quotidianità dell'individuo, il Corpo della Guardia di Finanza e, nello specifico, il Nucleo Speciale Tutela Privacy e Frodi Tecnologiche è fortemente impegnato, nella sua funzione di polizia economico-finanziaria, nel contrasto ad ogni forma di illecito commesso in e attraverso la Rete. Altresì, quale polizia amministrativa a garanzia della tutela della protezione dei dati personali, indirizza i propri sforzi, nell'espletamento delle attività ispettive volte a constatare violazioni in ambito privacy, soprattutto alla luce dell'innovata normativa introdotta dal Regolamento UE nr. 2016/679, meglio noto come GDPR (General Data Protection Regulation). In dettaglio, nell'ambito della programmazione dell'attività ispettiva per l'anno 2019 definita dal Garante per la protezione dei dati personali, il Nucleo ha svolto, su delega della citata Autorità, nr. **105 ispezioni** nel settore alberghiero e marketing, nonché nei confronti di tour operator, circoli sportivi, agenzie immobiliari e dei titolari dei circuiti connessi alla fidelizzazione del cliente attraverso l'emissione di Fidelity card. Le criticità rilevate hanno riguardato principalmente **i tempi di conservazione** dei dati personali, la **pertinenza** dei dati acquisiti rispetto alle finalità dei trattamenti e le **inidonee informazioni** fornite agli interessati circa i trattamenti previsti. L'attenzione del Nucleo Speciale Tutela Privacy e Frodi Tecnologiche è costantemente mantenuta alta in ogni presidio rientrante nella mission istituzionale affidata al reparto. Tuttavia viene riservata particolare incisività in tutti quei settori in cui l'illegalità nel mondo cibernetico, oltre a danneggiare il corretto andamento dei mercati, mina gli interessi e la sicurezza economico-finanziaria a tutela dei consumatori.

In particolare, ha assunto un ruolo di centralità la tutela della proprietà intellettuale. Il monitoraggio della Rete condotto dal reparto è stato diretto a circoscrivere quelle realtà online, che, ponendosi come veri e propri portali e-commerce, propongono in vendita a prezzi stracciati ogni sorta di bene contraffatto delle più prestigiose griffe. È stato rilevato, nel tempo, che i canali "commerciali" maggiormente utilizzati, oltre alle consuete piattaforme web, sono le pagine create ad hoc sulle diverse reti social. A destare preoccupazione, senza voler considerare il danno economico inflitto ai rispettivi proprietari dei marchi violati e il mancato gettito fiscale, è che la massimizzazione degli illeciti profitti induce le aziende del fake a sfruttare manodopera a bassissimo costo e ad utilizzare materiale di infima qualità, spesso altamente dannoso per la salute.

Se la contraffazione non accenna a mostrare battute di arresto nonostante l'azione preventiva e repressiva, non è da meno il fenomeno del download e streaming illegale di contenuti multimediali quali prime visioni, eventi sportivi e prodotti editoriali di ogni genere. I servizi vengono offerti di sovente a fronte della sottoscrizione di forme di abbonamenti a prezzi irrisori, ma non di rado capita di incappare in portali che offrono gratuitamente i medesimi

prodotti. In quest'ultimo caso, gli introiti sono garantiti sia dalle agenzie pubblicitarie che acquistano spazi web da utilizzare per la propria clientela sia dalla profilazione dell'utente e la conseguente rivendita ad aziende di marketing dei dati dei cybernauti illecitamente acquisiti.

Le attività condotte nel 2019 dal Nucleo Speciale Tutela Privacy e Frodi Tecnologiche nel settore in parola hanno consentito di individuare e **deferire all'Autorità Giudiziaria** per violazioni in materia di proprietà intellettuale **27 soggetti** e sottoporre a **sequestro 551 risorse web** e pagine sui social network utilizzate per le illecite attività dinanzi trattate.
Una posizione di rilievo, per le attività del Nucleo Speciale Tutela Privacy e Frodi Tecnologiche, è stata assunta anche dalla protezione del consumatore, che, confrontandosi quotidianamente con il mondo virtuale, di sovente si vede violare i propri diritti. In relazione a ciò, il Nucleo ha, dapprima, inteso scandagliare il comparto dei giochi e delle scommesse online. Le attività sono state orientate ad individuare e disarticolare quelle organizzazioni criminali che, operando in Rete in contesti internazionali e quindi al di fuori dei circuiti autorizzati, oltre a danneggiare il sistema Paese, omettendo di versare ogni forma di imposta, non assicurano allo scommettitore la possibilità di concorrere con eque probabilità di vincita.
In tale ambito si segnala l'operazione "Galassia", durante la quale il Nucleo ha partecipato alle azioni investigative più articolate e delicate, in un contesto connotato dall'elevato tecnicismo connesso alle avanzate tecnologie delle architetture informatiche sottese alla funzionalità e gestione delle scommesse. Le indagini condotte con il Servizio Centrale Investigazione Criminalità Organizzata della Guardia di Finanza e il Nucleo di Polizia Economico - Finanziaria di Reggio Calabria, sotto il coordinamento della locale **Direzione Distrettuale Antimafia,** hanno permesso di disarticolare plurime associazioni per delinquere strumentali ad agevolare gli interessi criminali delle **cosche di *'ndrangheta*** nonché di accertare l'esistenza di una illecita attività di **gestione** e **raccolta di scommesse** attraverso **siti *on line*** completamente **illegali,** mediante la creazione di complessi **schermi giuridici,** anche di diritto estero, costituiti da **Centri di Trasmissione e Punti Vendita di Ricariche**. La ricostruzione del volume d'affari ingenerato dal meccanismo fraudolento di gestione dell'attività, che ha di fatto agevolato l'infiltrazione della criminalità organizzata nel tessuto economico nazionale con il relativo conseguimento di ingenti illeciti profitti, ha permesso di accertare **oltre 3 miliardi di euro** di ricavi totalmente sconosciuti al fisco. Sulla scorta dei gravi elementi indiziari complessivamente raccolti, si procedeva all'esecuzione di **20 ordinanze di custodia cautelare** nonché al **sequestro preventivo** nei confronti di **23 società estere, 15 imprese italiane** tutte operanti sul territorio nazionale nel settore dei giochi e delle scommesse, **24 immobili, automezzi, 33 siti web** nazionali e internazionali di "*gambling on line*", **conti correnti** nazionali ed esteri, innumerevoli **quote societarie** di imprese nazionali ed estere per un valore complessivo di **oltre 723 milioni di euro.**

Contestualmente il reparto ha anche effettuato un carotaggio nel panorama delle polizze assicurative veicolate attraverso il canale telematico. Gli esiti delle analisi svolte dal Nucleo hanno delineato uno scenario dal quale emerge come sia estremamente diffusa la presenza in Rete di innumerevoli proposte di falsi intermediari assicurativi che, vantando speciali condizioni contrattuali, promettono agevolazioni e premi vantaggiosissimi, tali da indurre il consumatore ad aderire senza esitazione. E' soltanto in una seconda fase che gli utenti si rendono conto di aver fornito i propri dati personali per l'emissione della polizza e aver corrisposto il premio richiesto, ricevendo un tagliando totalmente contraffatto ovvero senza ottenerlo affatto e trovandosi, pertanto, senza alcuna copertura assicurativa. A seguito di quanto emerso venivano svolti opportuni approfondimenti, anche attraverso l'interrogazione della banca dati del Registro unico degli intermediari assicurativi (R.U.I.), che sono sfociati nell'operazione "Fake Insurance" e i cui esiti hanno consentito di sottoporre a **sequestro 222 siti web** che proponevano le false assicurazioni online, contravvenendo alle prescrizioni imposte dal Codice delle assicurazioni private, nonché alla **denuncia di 74 persone** che a diverso titolo hanno partecipato al sistema truffaldino.
L'area di operatività del Nucleo si estende oltre la parte più superficiale del web, quella che normalmente si è abituati a navigare senza alcun tipo di accorgimento o conoscenza informatica, andando a penetrare anche quella porzione della Rete più oscura, luogo in cui ogni forma di attività compiuta è commessa nella totale illegalità e dove le risorse non vengono indicizzate dai comuni motori di ricerca e non risultano registrate presso i pubblici registri dei domini.
La costante presenza nel Dark Web consente al Nucleo di acquisire grandi quantità di dati inerenti i rapporti commerciali posti in essere nei Black Market, che vengono poi sottoposti ad una minuziosa analisi e successivamente confrontati con le informazioni ottenute nel Clear Web attraverso sofisticate tecniche di OSINT.
Recentemente il Nucleo, nell'ambito delle operazioni "Darknet.Drug" e "Berlusconi Market" ha inferto un duro colpo ad un'organizzazione criminale che, oltre ad essere dedita al traffico di sostanze stupefacenti nel citato market, è risultata anche esserne l'amministratrice.

L'attività di indagine ha preso avvio dall'analisi degli annunci di vendita di sostanze stupefacenti presenti su piattaforme Internet (cd. Black Market) del Dark Web.
Attraverso mirate analisi tecniche delle poche informazioni presenti nel Dark Web è stato possibile rilevare alcuni indizi che sono stati opportunamente isolati e analizzati. Tali elementi sono risultati a loro volta associati ad altre informazioni rintracciate nel Clear Web.
Gli investigatori hanno avviato indagini tecniche sul territorio, che hanno permesso di individuare un soggetto, successivamente tratto in **arresto**, risultato essere dedito alla vendita di sostanze stupefacenti sul Black Market denominato Berlusconi Market.
A partire da gennaio 2019, Berlusconi Market ha rappresentato il più importante mercato del Dark Web, sia per quantità ed eterogeneità di beni e servizi proposti in vendita, sia per il volume degli scambi con oltre 100.000 annunci di articoli illegali di ogni genere, tanto da

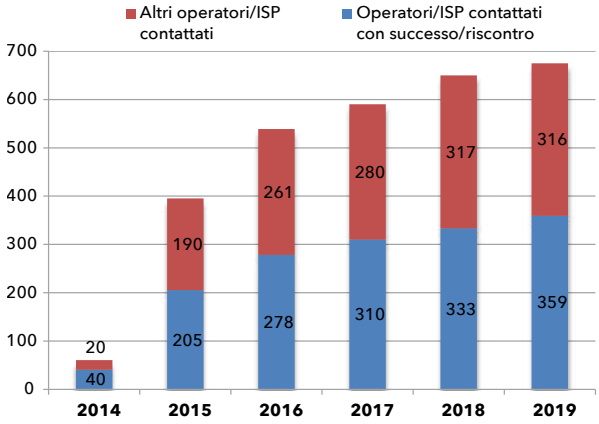
essere considerato dalla community dell'underground della Rete come il mercato di riferimento a livello globale nel Dark Web per l'acquisto di qualsivoglia tipologia di prodotti, il tutto nella completa anonimità.
Al soggetto, che, celandosi dietro al nickname ***g00d00,*** era riuscito a guadagnarsi la stima di diversi compratori in tutto il mondo per la qualità della droga posta in vendita on-line, , venivano **sequestrate,** oltre ad ingente quantitativo di materiale informatico, **2,2 Kg. di sostanze stupefacenti** (cocaina, ketamina, MDMA) pronte per essere commercializzate nel Dark Web, oltre a **163 pasticche di ecstasy** e **78 francobolli impregnati di LSD,** nonché un'attività commerciale di **Exchange di Bitcoin**, utilizzata per la monetizzazione e il riciclaggio delle somme percepite in valuta virtuale dalle attività criminali poste in essere Le indagini sono proseguite con l'analisi, secondo le più moderne tecniche della "*Digital Forensics*", dei personal computer e apparati telefonici sequestrati che hanno portato a riconoscere in capo agli amministratori del Black Market l'associazione per delinquere finalizzata alla commissione di molteplici reati in concorso con i *vendor* mediante la concessione di uno spazio web (vetrina) sul proprio *store* (negozio) virtuale, unitamente alla gestione dei pagamenti (in criptovalute), al fine di conseguire un profitto per tale attività illegale.
I proventi illeciti accertati ammontano a circa 41 bitcoin, pari a circa 400.000,00 euro a fronte di un volume complessivo di transazioni annue pari a circa **2 milioni di euro**.
Gli elementi raccolti grazie alle minuziose attività investigative svolte dal personale specializzato del Nucleo Speciale Tutela Privacy e Frodi Tecnologiche, con il coordinamento della Procura della Repubblica di Brescia, hanno portato all'emissione di misure cautelari personali della **custodia in carcere** a carico di **3 soggetti** gestori di Berlusconi Market.
Il brillante risultato conseguito costituisce il quarto esempio al mondo di un Black Market del Dark Web reso non più operativo, dopo le operazioni dell'FBI statunitense e della polizia olandese condotte nei confronti dei Black Market "Silk Road", "Alfa Bay" e "Hansa Market".

Attività e segnalazioni del CERT Nazionale

Le attività svolte nel 2019 confermano un contesto di grande variabilità degli agenti di minaccia che ha richiesto interventi mirati nella mitigazione e prevenzione degli incidenti.
Nel corso dell'anno passato l'attività del CERT Nazionale si è caratterizzata per una sempre maggiore integrazione delle modalità operative con quanto previsto dalla partecipazione alla rete dei CSIRT istituita dalla Direttiva NIS, che ha richiesto di focalizzarsi su molteplici canali di "information sharing." e di avviare l'utilizzo di diversi strumenti collaborativi messi a disposizione dalla "Core Service Platform", la piattaforma di cooperazione realizzata per supportare i CSIRT della rete.
A fine novembre, fra l'altro, il CERT Nazionale si è sottoposto ad una "peer review" da parte dei rappresentanti della rete dei CSIRT volta alla certificazione del proprio livello di maturità operativa.
Queste attività agevoleranno l'inserimento del costituito CSIRT Italiano all'interno del circuito europeo e mondiale dei CSIRT.
Come noto, infatti, con il DPCM dello scorso 8 agosto 2019 (GU n.262 del 8-11-2019) è stata definita l'organizzazione e il funzionamento del CSIRT Italiano, istituito presso il Dipartimento delle informazioni per la sicurezza della Presidenza del Consiglio dei ministri, dando seguito a quanto previsto dal DLgs. del 18 maggio 2018, n.65 di recepimento della Direttiva NIS, che trasferisce le competenze del CERT Nazionale e del CERT-PA al CSIRT italiano.

Le attività

Il numero di segnalazioni ricevute nel corso del 2019, circa 8.000, ha confermato il CERT Nazionale quale punto di riferimento, a livello nazionale e internazionale, per lo scambio di informazioni utili per la prevenzione e la mitigazione di incidenti informatici e delle minacce, vulnerabilità e compromissioni che vengono riscontrate nel cyber spazio.

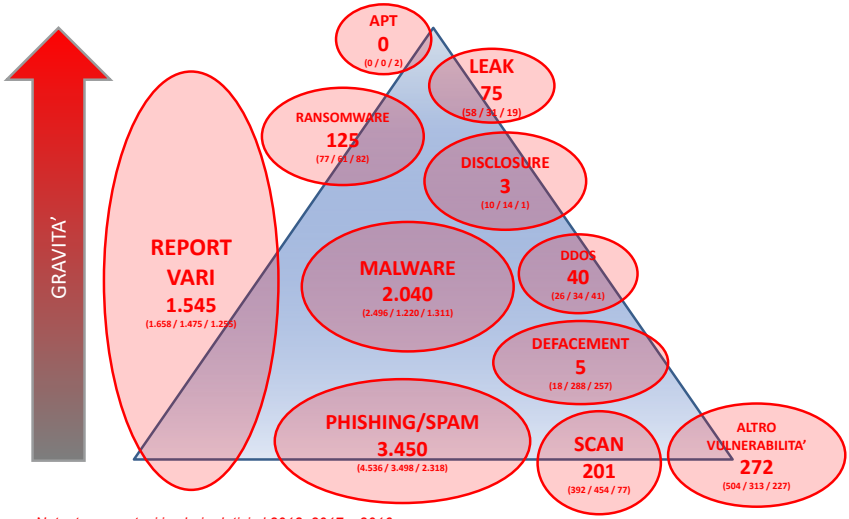


Il numero di Operatori e *Internet Service Provider* nazionali con i quali il CERT si è interfacciato nel corso del tempo è in costante crescita. Sono oltre 675 gli Operatori con i quali sono state scambiate o condivise informazioni relative alle rispettive reti volte a mitigare o a prevenire incidenti e attacchi informatici.
Il CERT Nazionale si pone come facilitatore per la risoluzione e, soprattutto, la prevenzione di incidenti informatici, e per questo un'importanza primaria viene attribuita nelle attività giornaliere nell'assicurare un efficiente processo *infosharing* rendendo estremamente proficuo il rapporto, basato sula reciproca fiducia, instaurato con i propri interlocutori .
L'attività di *infosharing* è proseguita anche a livello internazionale, grazie, come già detto, all'appartenenza del CERT Nazionale alla *CSIRT Network* a livello europeo, che consente uno scambio informativo efficace ed efficiente con gli Stati Membri, e all'accreditamento a reti internazionali fidate, quale, ad esempio, *Trusted Introducer*, che consente di raggiungere ed essere raggiunti dagli omologhi CERT internazionali per segnalazioni transnazionali.
Il numero di omologhi CERT a livello internazionale con i quali il CERT Nazionale italiano è entrato in contatto ha superato i 60 soggetti di altrettanti Paesi europei ed extra-europei.

Segnalazioni, minacce e incidenti

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 numero di segnalazioni ricevute nel 2019, poco meno di 8.000, pur se in calo rispetto a quelle del 2018, sono in linea con la media registrata negli ultimi anni.
Il 2019 ha continuato a registrare un notevole peso delle segnalazioni relative ad attacchi di *phishing*, che, da sole, rappresentano circa il 40% del totale, con una componente sempre crescente di *spear phishing*, ovvero di attacchi mirati, talvolta preceduti da attività di *social engineering*.
Pur rappresentando un vettore di attacco ben conosciuto, il *phishing* riesce ancora a colpire diverse vittime attraverso tecniche sempre diverse come, ad esempio, l'utilizzo di account PEC (Posta Elettronica Certificata) compromessi, utilizzati in diverse massive campagne di *phishing* o di diffusione di *malware* nel corso dell'anno. Nel 2019 si sono registrate, infatti, diverse campagne più o meno mirate di *phishing* e *malspam* che hanno sfruttato credenziali PEC compromesse. La maggiore fiducia riposta dagli utilizzatori nello strumento PEC, soprattutto da chi non ha particolari conoscenze tecniche, ha reso tali campagne particolarmente pericolose.
Sulla falsariga dell'anno precedente sono proseguite periodiche campagne di diffusione di *malware* (*malspam*) volte alla compromissione delle credenziali di posta elettronica o di accesso a servizi bancari. Non sono mancate segnalazioni relative ad ondate di attacchi, tentati o a andati a buon fine, volti alla diffusione di *malware* estorsivo (*ransomware*) che, pur non avendo registrato fenomeni mediatici comparabili a quelli del 2017 (*WannaCry*, *notPetya*), resta una delle principali minacce per gli utilizzatori della rete.
Anche i fenomeni di *data breach* con furto, pubblicazione ed eventuale rivendita di dati

compromessi, continuano a crescere. Per stimare la dimensione del fenomeno il solo sito *haveibeenpwned*, sito tra i più noti, che consente di verificare se il proprio account risulti tra quelli appartenenti ai principali *data breach* conosciuti, contiene al momento circa 9,5 miliardi (!) di record, contro i circa 6 dell'anno precedente. Questi valori oltre a dare un'idea della dimensione forniscono anche una indicazione della crescita del fenomeno (almeno della parte emersa). Il rischio maggiore legato alla pubblicazione (o alla rivendita) di credenziali e dati compromessi provenienti da siti apparentemente "innocui" in termini di contenuti di dati personali resta quello della *password-reuse*, quando le stesse credenziali di accesso, oltre a consentire una facile individuazione del soggetto fisico coinvolto (si pensi ad esempio a e-mail nel formato nome.cognome@azienda.it) vengono utilizzate per l'accesso a servizi aziendali, personali o comunque contenenti dati sensibili.
Nella figura seguente sono riassunte le segnalazioni giunte al CERT Nazionale nel corso del 2019



Nota: tra parentesi i valori relativi al 2018, 2017 e 2016

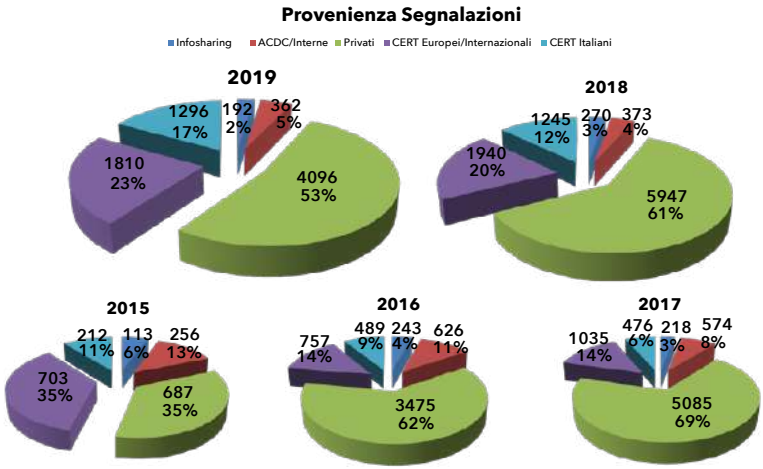
La rappresentazione riportata è chiaramente una esemplificazione di quanto pervenuto al CERT: gran parte delle segnalazioni sono riconducibili a vulnerabilità, spesso note o non sfruttate, a *scan* di rete volti alla loro individuazione, o a compromissioni con rischio intrinseco "limitato", come ad esempio quelle legate all'invio di spam e a siti web compromessi o predisposti *ad-hoc* e utilizzati per attacchi di *phishing*.
Queste compromissioni, per quanto intrinsecamente ancora poco pericolose, possono spesso rappresentare una base per lanciare attacchi avanzati ed estremamente mirati da parte dei criminali informatici, attraverso, per esempio, la compromissione delle credenziali di

accesso a sistemi informatici ottenute attraverso un attacco di *phishing* andato a buon fine. Tra gli attacchi sicuramente più pericolosi e dall'effetto immediato si può annoverare la distribuzione di *malware* o lo sfruttamento di configurazioni scorrette che tipicamente lasciano "aperti" in rete protocolli o servizi sfruttabili per attacchi a terze parti, come il lancio di attacchi DDoS. Da questo punto di vista, già dalla fine del 2016, l'avvento dell'IoT (*Internet of Things*) aveva iniziato a far nascere alcune problematiche significative per il grande numero di apparati vulnerabili e/o compromessi in rete, spesso progettati senza particolare attenzione ai problemi di sicurezza, potenzialmente utilizzabili come piattaforme di lancio di attacchi a terze parti. Tuttavia anche il 2019, come già gli anni precedenti, pur continuando a registrare una notevole diffusione di *botnet* basate su IoT (e non solo) e il proliferare di C&C che le possono sfruttare, non sembra aver registrato, almeno sulla base delle segnalazioni ricevute dal CERT Nazionale, eventi di grandissimo impatto, come temuto successivamente all'attacco della *botnet* "Mirai" di fine 2016.

Ciononostante non sono mancati, nel corso dell'anno, importanti attacchi DDoS basati sui classici meccanismi di "*Reflection and Amplification*" utilizzando anche protocolli già sfruttati in passato come il CLDAP che assicura un elevato fattore di amplificazione pari all'incirca a 70.

Di una certa rilevanza sono stati alcuni importanti attacchi nei confronti di diverse società di scommesse on-line registrati a partire da ottobre. Gli attacchi diretti di tipo DDoS sono stati accompagnati da massicci attacchi secondari ad entità terze con *spoofing* di indirizzo e utilizzo di blocchi delle vittime con lo scopo di forzare le terze parti a chiudere il traffico, anche legittimo, proveniente dai soggetti colpiti. Numerose segnalazioni sono giunte al proposito da parte di soggetti internazionali sparsi in tutto il mondo. In un caso si è avuta evidenza di un tweet di *extorsion* relativo al particolare vettore di attacco (DDoS diretto congiunto allo *spoofing* dei blocchi), pur non avendo avuto alcuna evidenza della sua effettiva origine e attendibilità.

Anche nel 2019 si sono registrati diversi casi che hanno visto il ricorso al CERT Nazionale, da parte di diversi soggetti, privati cittadini o, più frequentemente, ricercatori di sicurezza, per segnalazioni di vulnerabilità di varia gravità in modalità "responsabile". Le segnalazioni giunte nel corso dell'anno, talvolta relative a problematiche estremamente serie per 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.



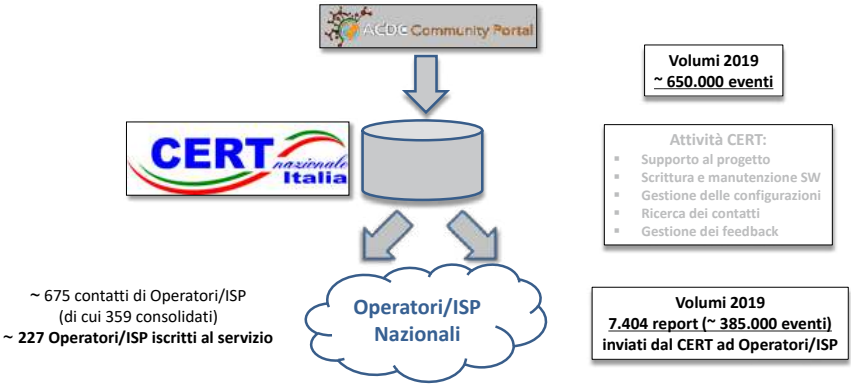
La provenienza delle segnalazioni conferma una quota importante da soggetti privati (53%) legata alla diffusione della conoscenza dell'esistenza del CERT Nazionale nel corso degli anni grazie anche all'accreditamento presso organismi riconosciuti a livello internazionale, quali *Carnegie Mellon* e *Trusted Introducer*, già a partire dal 2016. D'altra parte il consolidamento dei rapporti all'interno della rete dei CERT europei attraverso la *CSIRT Network* e con gli omologhi CERT internazionali si riflette in un incremento dei contatti, delle segnalazioni e degli scambi informativi a livello transnazionale.

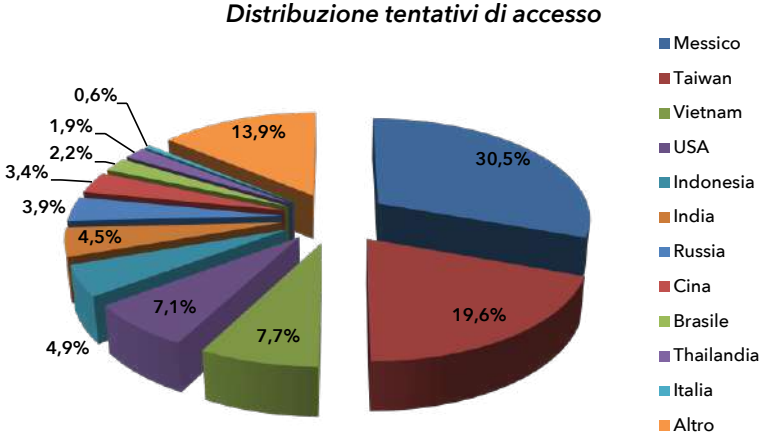
Le honeypot

Il CERT Nazionale può contare su una fonte informativa interna estremamente interessante costituita dalle *honeypot* predisposte nell'ambito del progetto europeo ACDC (*Advanced Cyber Defence Center*).

Si tratta di vere e proprie "esche" che consentono a macchine opportunamente predisposte di "intercettare" i tentativi di attacco e il relativo traffico malevolo proveniente da tutto il mondo. Parallelamente alle *honeypot* ereditate del progetto ACDC (ormai concluso già dal 2015), che sono di tipo "passivo", ovvero si limitano ad intercettare i tentativi malevoli provenienti dalla rete, sono in fase di sperimentazione, con buoni risultati, altre *honeypot* "ad alta interazione" che, di fatto, cercano di interagire con il *malware* o l'entità che cerca di attaccarle, al fine di ottenere maggiori informazioni sulla metodologia di attacco attraverso la predisposizione di opportune *sandbox* dinamiche all'interno delle quali il *malware* viene indotto a portare a termine la sua azione malevola.

Anche nel corso del 2019 è proseguita l'attività di diffusione agli Operatori coinvolti delle segnalazioni fornite dalla rete *anti-botnet* (composta delle reti di *honeypot* del progetto europeo ACDC). L'informatizzazione della procedura di ricezione e invio delle segnalazioni ha consentito di inviare circa 7.400 report nel corso dell'anno agli oltre 225 Operatori iscritti al servizio.





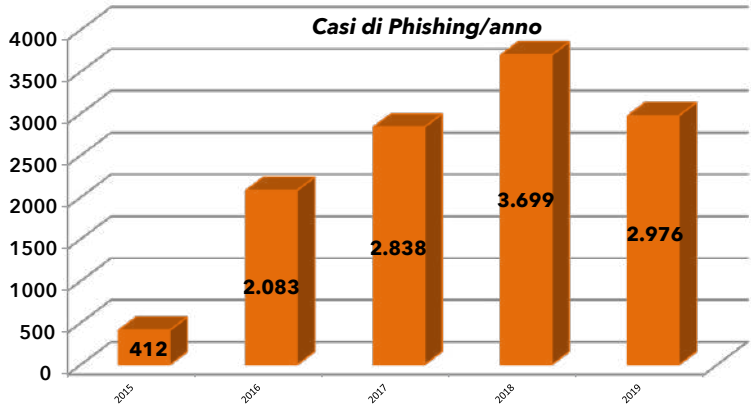
La rete di *honeypot* predisposta nell'ambito del progetto raccoglie un notevole numero di eventi (diverse centinaia di milioni all'anno), tra tentativi di connessioni malevole e tentativi di scaricamento di *malware*, consentendo anche di avere una ricca base dati sulla provenienza, a livello mondiale, di determinati tipi di attacco oltre che una estesa lista di indirizzi potenzialmente malevoli.

Il phishing

Nel corso del 2019 si sono registrate numerose campagne di *malspam*, *phishing* e *spear-phishing*, che restano i principali vettori di diffusione di *malware* oltre ad essere i classici strumenti per la compromissione di credenziali, confermando quando rilevato negli anni precedenti.

Oltre ai tipici attacchi "generici" di *phishing* (in leggero calo rispetto all'anno precedente), si sono rilevate perniciose e continuate campagne di compromissione di account (principalmente di entità afferenti alla Pubblica Amministrazione) che utilizzano account precedentemente compromessi per comprometterne altri, sfruttando l'invio di messaggi leciti da un punto di vista sistemistico, in quanto provenienti da account riconosciuti e che quindi possono evadere agevolmente i sistemi *antispam*.

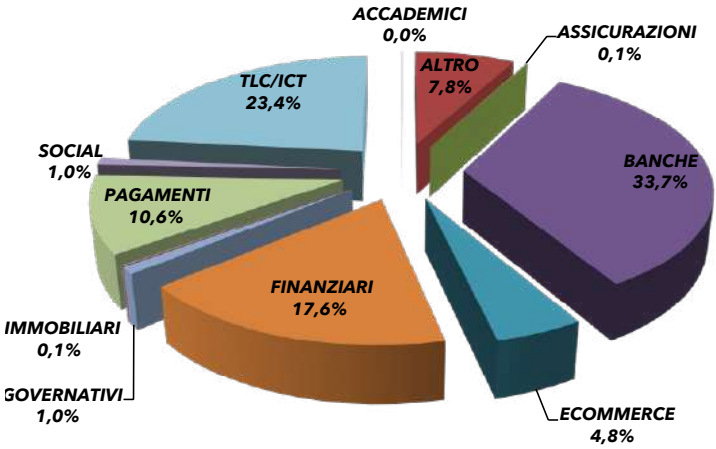
Anche la tendenza degli attacchi di *spear phishing* è in crescita, con sempre più segnalazioni di tentativi di attacco nei confronti di strutture apicali di enti pubblici o privati.



Le segnalazioni di pagine di *phishing* ospitate su server italiani compromessi e pervenute al CERT Nazionale si sono attestate attorno alle 3.000, in riduzione rispetto all'anno precedente, ma in linea con il 2017.

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*) non aggiornati.

Generalmente le segnalazioni arrivano al CERT Nazionale solo dopo tentativi preventivi di contattare gli amministratori o di risolvere in altra maniera l'incidente e il numero di segnalazioni ricevute rappresentano pertanto una quota verosimilmente ridotta del fenomeno, seppure probabilmente quelle più complicate da risolvere.



In particolare, nel corso dell'anno 2019, sono state ricevute e gestite complessivamente 2.976 segnalazioni riguardanti pagine di *phishing*:

un terzo circa ha riguardato siti di *phishing* ai danni di clienti di banche, spesso con presenza multinazionale: circa 80 le banche coinvolte;

poco meno di un quarto ha riguardato tentativi di cattura di credenziali relativi a servizi TLC/ICT, tipicamente credenziali di grandi Operatori "*Over The Top*", o credenziali e-mail, il più delle volte veicolati da e-mail malevole contenenti link fraudolenti;

in crescita il numero di segnalazioni (quasi il 18%) relative a servizi finanziari;

in crescita anche il numero di segnalazioni relative al settore dei pagamenti online, mentre il settore e-commerce rappresenta circa il 5% del totale; residuale il resto delle segnalazioni, tra le quali quelle riferibili a servizi governativi (principalmente esteri) che non raggiungono l'1% del totale.

Riguardo alle reti coinvolte, sono stati circa 70 gli Operatori/ISP italiani che il CERT Nazionale ha informato nel corso dell'anno riguardo alla presenza di pagine di *phishing* ospitate sulle rispettive reti, con ovvia concentrazione su quelli che offrono servizi di hosting o free-hosting di utenza residenziale o micro affari.

Le policy di intervento dei vari Operatori/ISP si sono rilevate molto differenti, passando da interventi estremamente tempestivi a casi in cui i tempi di reazione si sono rivelati più lunghi, ma nella totalità dei casi si è giunti alla risoluzione del problema in tempi decisamente contenuti a seguito della segnalazione del CERT Nazionale.

Il sito web

Il sito web del CERT Nazionale (**https://www.certnazionale.it**) si rivolge a cittadini e imprese con notizie di interesse generale legate alla sicurezza informatica, bollettini tecnici e linee guida di comportamento con l'obiettivo di trattare argomenti tecnici con la necessaria

precisione, ma cercando al contempo di renderne i contenuti utili e comprensibili anche a chi non necessariamente ha conoscenze tecniche professionali.
Le statistiche di accesso al sito web confermano una crescita (+3% rispetto all'anno precedente) del numero di visite.

Nel corso del 2019, in particolare, sono state pubblicate oltre 240 notizie a valenza informativa di vasto interesse a copertura degli eventi di sicurezza rilevati, dalla diffusione di *malware* all'utilizzo di nuove tecniche di attacco, dalla pubblicazione di aggiornamenti di sicurezza da parte dei *vendor* alla scoperta di nuove vulnerabilità. Le notizie, pubblicate con cadenza giornaliera, rappresentano un giusto compromesso tra una trattazione tecnica specialistica e una informativa generale relativa alle problematiche di sicurezza del momento e contengono informazioni utili per tutti gli utilizzatori di sistemi informatici, indipendentemente dal loro livello di conoscenza tecnica.

Il punto di vista del CERT-PA

Il CERT-PA, che cesserà formalmente di esistere entro il primo semestre del 2020 per via dell'attuazione delle previsioni contenute nella legge di recepimento della Direttiva NIS, ha operato sin dal 2013 all'interno dell'Agenzia per l'Italia Digitale (AgID), alla quale la normativa vigente[1] affida il mandato di attuare iniziative tecniche ed organizzative volte sia a migliorare la consapevolezza della Pubblica Amministrazione nei riguardi della minaccia cibernetica, sia ad aumentarne le capacità di prevenzione, protezione e risposta agli incidenti. Pur se la sua *constituency* di riferimento era formata solamente da Pubblica Amministrazione Centrale, Regioni e Città metropolitane, il CERT-PA ha da sempre supportato, pur se in modalità *best-effort*, tutte le altre PA che necessitassero di assistenza.
In accordo al proprio mandato, in questi anni il CERT-PA ha fornito alle Amministrazioni richiedenti:

- *servizi di analisi e di indirizzo*, finalizzati a supportare la definizione dei processi di gestione della sicurezza, lo sviluppo di metodologie, il disegno di processi e di metriche valutative per il governo della sicurezza cibernetica;
- *servizi proattivi*, aventi come scopo la raccolta e l'elaborazione di dati significativi ai fini della sicurezza cibernetica, l'emanazione di bollettini e segnalazioni di sicurezza, l'implementazione e la gestione di basi dati informative, lo sviluppo della *readiness* e della *preparedness*;
- *servizi reattivi*, aventi come scopo la gestione degli allarmi di sicurezza, il supporto ai processi di gestione e risoluzione degli incidenti di sicurezza all'interno del dominio delle PA;
- *servizi di formazione e comunicazione* per promuovere la cultura della sicurezza cibernetica, favorendo il grado di consapevolezza e competenza all'interno delle PA, attraverso la condivisione di informazioni relative a specifici eventi in corso, nuovi scenari di rischio o specifiche tematiche di sicurezza delle informazioni.

A queste attività si sono affiancate quelle, riservate, connesse alla partecipazione del CERT-PA al sistema nazionale di protezione dello spazio cibernetico del nostro Paese, in particolare per quanto riguarda la partecipazione al Nucleo di Sicurezza Cibernetica istituito presso la Presidenza del Consiglio.
Infine il CERT-PA ha svolto anche un'intensa e sempre più crescente attività informativa e di divulgazione indirizzata al pubblico generale. Questa è consistita principalmente nella sistematica e tempestiva diffusione di bollettini, notizie ed approfondimenti riguardanti eventi rilevanti in ambito sicurezza cibernetica, preparate dagli analisti del CERT-PA. Tali informazioni sono state rese disponibili sia sul sito del CERT-PA (https://www.cert-pa.it/) che mediante i canali ufficiali del CERT-PA attivi su Twitter (@CertPa) e su Telegram (@certpaitalia) ai quali chiunque può iscriversi senza alcuna formalità.

1 In particolare: il Quadro Strategico Nazionale per la sicurezza dello spazio cibernetico, il collegato Piano Nazionale per la protezione cibernetica e la sicurezza informatica, nonché la Direttiva 1 agosto 2015 del Presidente del Consiglio.

Principali iniziative del 2019

Nel corso del 2019 il CERT-PA ha provveduto innanzitutto a sviluppare ulteriormente la propria struttura operativa, dotandosi di nuove risorse e di strumenti tecnici aggiornati a supporto delle proprie attività, e sviluppando ulteriormente i servizi messi a disposizione della comunità.

In particolare, a seguito del completamento avvenuto nel 2018 della sperimentazione svolta sin dal 2017 per mettere a punto strumenti e protocolli di *infosharing*, con l'obiettivo di costituire una rete nazionale di scambio automatico di IoC (indicatori di compromissione) validati e *actionable* mediante l'uso dei protocolli STIX e TAXII, è stata costituita una piattaforma aperta per la distribuzione di IoC qualificati, alle quali tutte le PA potranno attingere gratuitamente.

Il CERT-PA è inoltre stato coinvolto nell'attuazione di molteplici iniziative in ambito cybersecurity previste nel Piano Triennale dell'AgID e rivolte alla Pubblica Amministrazione, in particolare nei programmi di accompagnamento per le Regioni e nello sviluppo di strumenti e metodologie per la diffusione delle *best practices* di cybersecurity presso le Amministrazioni.

La cybersecurity nel Piano Triennale dell'AgID 2019-2021

Sotto il profilo strategico, l'attività più impegnativa dell'Agenzia per l'Italia Digitale (AgID) è la redazione annuale del Piano Triennale per l'informatica nella Pubblica Amministrazione, che il Presidente del Consiglio dei ministri deve adottare ogni anno entro ottobre. Tale adempimento definisce il percorso evolutivo dell'impiego delle tecnologie informatiche all'interno della Pubblica Amministrazione e quindi, in definitiva, traccia il solco entro cui questa nel suo complesso si evolve.

Nel Piano Triennale 2019-2021 la cybersecurity gioca un ruolo fondamentale. In effetti già nel piano precedente essa veniva esplicitamente indicata quale componente trasversale rispetto ai tre strati orizzontali delle "Infrastrutture materiali", "Infrastrutture immateriali" ed "Ecosistemi", declinando per ciascuno di essi le relative esigenze specifiche di sicurezza. Nel Piano triennale tuttavia la cybersecurity assurge a vero e proprio componente cruciale dell'intero sistema in quanto, come si vede dalla mappa schematica del modello, abbraccia e racchiude tutti i macro ambiti che aggregano gli elementi omogenei oggetto del Piano.

Fra le iniziative più significative che AgID attraverso il CERT-PA ha realizzato tra quelle previste dal Piano per il 2019 spiccano:

- il rilascio al pubblico generale della piattaforma Infosec, la quale fornisce un supporto ricco ed altamente qualificato agli analisti di sicurezza;
- il rilascio in via sperimentale, per le Pubbliche amministrazioni, della piattaforma nazionale di trasmissione automatizzata di IoC qualificati, realizzata a seguito della sperimentazione svolta nel corso del 2018 da parte di due Gruppi di lavoro coordinati da AgID e dal CERT-PA;
- la pubblicazione del modello organizzativo standard per la realizzazione di quelli che sono stati definiti "CERT di prossimità", ossia CERT di secondo livello ("orizzontali" o territoriali, e "verticali" o tematici), che costituiscano un punto di snodo fra il CERT-PA centrale e le realtà più distribuite della PA quali gli enti locali e territoriali o determinate comunità specifiche, in particolare i CERT Regionali;
- molteplici attività finalizzate ad incrementare la cybersecurity della Pubblica Amministrazione, in particolare accompagnando le Regioni e supportando l'azione dei Responsabili della transizione digitale che, a norma del CAD, hanno anche responsabilità in termini di sicurezza. Fra queste vanno almeno annoverate l'emanazione delle Linee Guida per la sicurezza nel procurement e lo sviluppo di un tool on-line per il risk assessment delle Amministrazioni.

Tale attività verrà incrementata nel corso del 2020, così come previsto dal Piano Triennale.

Riepilogo dell'attività svolta nel 2019

Le statistiche di andamento delle attività erogate dal CERT-PA sono rese disponibili a chiunque desideri consultarle, grazie alla costante pubblicazione di un insieme puntuale di indicatori (KPI), i quali fanno parte del sistema di monitoraggio nazionale denominato "Avanzamento trasformazione digitale" (https://avanzamentodigitale.italia.it/it) e concorrono altresì a formare l'indice europeo DESI (The Digital Economy & Society Index).
Qui di seguito riportiamo un breve riepilogo dei dati riferiti all'anno 2019.

Segnalazioni

Le segnalazioni pervengono al CERT-PA da varie fonti: dalle Pubbliche Amministrazioni stesse, da altri CERT o strutture di monitoraggio quali il CNAIPIC, o ancora dallo stesso CERT-PA mediante la propria costante attività di monitoraggio automatico e semiautomatico delle fonti pubbliche.
Nel corso del 2019 il CERT-PA ha gestito un totale di 1.234 segnalazioni rilevanti, un numero sostanzialmente costante rispetto alle 1.297 del 2018. In **Figura 1** è riportato il relativo andamento mensile.

Figura 1 : L'andamento mensile delle segnalazioni pervenute al CERT PA nel 2019

CVE importati in Infosec

La piattaforma Infosec importa automaticamente tutti i CVE pubblicati dal MITRE non appena si rendono disponibili, per consentirne le analisi e correlazioni con tutti gli altri indicatori di cui dispone. Nel corso del 2019 Infosec ha importato 18.131 CVE, un numero sostanzialmente costante rispetto ai 18.453 del 2018. In **Figura 2** è riportato il relativo andamento mensile.

Figura 2 : L'andamento mensile dei CVE importati in Infosec nel 2019

IoC lavorati da Infosec

Nella piattaforma Infosec vengono altresì inseriti, per esservi analizzati, molteplici Indicatori di Compromissione (IoC) ottenuti da fonti prevalentemente OSINT. Nel corso del 2019 sono stati lavorati da Infosec 1.024.301 IoC, circa il 38% in meno rispetto ai 1.657.623 del 2018. In **Figura 3** è riportato il relativo andamento mensile.

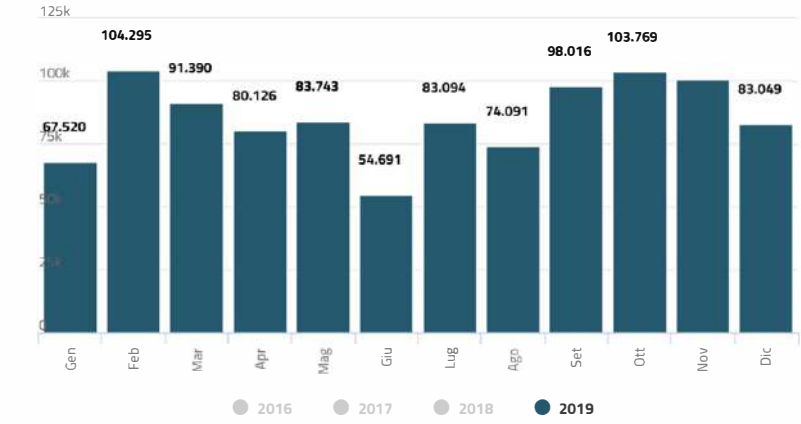


Figura 3: L'andamento mensile degli IoC lavorati da Infosec nel 2019

Malware analizzati da Infosec

Questo indicatore riguarda il numero dei file di malware scaricati ed analizzati da Infosec. Nel corso del 2019 sono stati analizzati da Infosec 16.613 malware, circa il 30% in più rispetto ai 12.775 del 2018. In **Figura 4** è riportato il relativo andamento mensile.

Figura 4: *L'andamento mensile dei malware analizzatii da Infosec nel 2019.*

FQDN/IP segnalati

Questo indicatore riguarda il numero degli IoC qualificati come domini o IP, prodotti e condivisi da Infosec. Nel corso del 2019 sono stati segnalati da Infosec 13.036 IoC, circa il 176% in più rispetto ai 4.714 del 2018. In **Figura 5** è riportato il relativo andamento mensile.

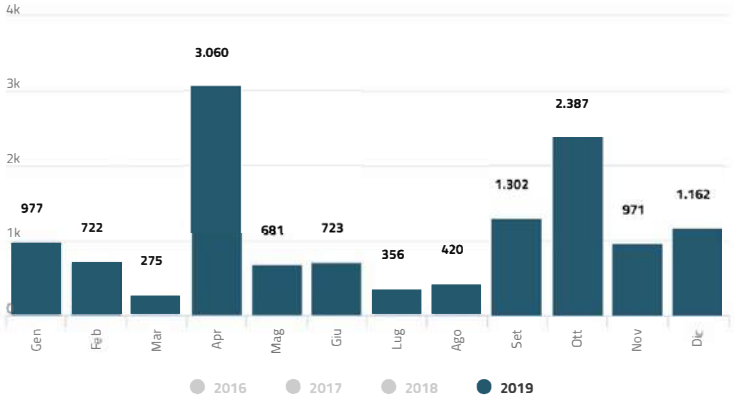


Figura 5: *L'andamento mensile degli IoC qualificati come domini o IP prodotti Infosec nel 2018 e 2019 (primo quadrimestre).*

URL segnalate

Questo indicatore riguarda il numero degli IoC qualificati come URL, prodotti e condivisi da Infosec. Nel corso del 2019 sono stati segnalati da Infosec 32.135 IoC, circa il 104% in più rispetto ai 15.740 del 2018. In **Figura 6** è riportato il relativo andamento mensile.

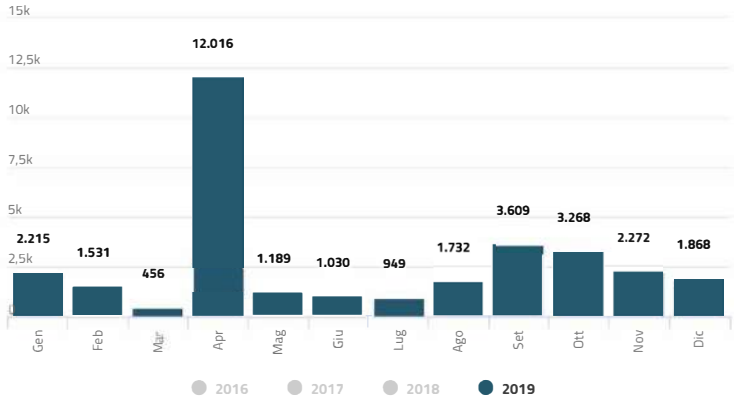


Figura 6: *L'andamento mensile degli IoC qualificati come URL prodotti Infosec nel 2018 e 2019 (primo quadrimestre).*

Dal CERT-PA allo CSIRT e oltre

La norma di recepimento della Direttiva NIS (D.Lgs. 18 maggio 2018 n. 65) prevedeva come noto la costituzione di uno CSIRT Italiano unico, che unificasse le funzioni del CERT Nazionale e del CERT-PA. Le modalità di creazione e organizzazione dello CSIRT sono affidate ad un DPCM emanato a novembre 2019 (DPCM 8 agosto 2019, "Disposizioni sull'organizzazione e il funzionamento del Computer security incident response team - CSIRT italiano", pubblicato in GU Serie Generale n.262 del 08-11-2019). Pertanto nel corso del 2019 il CERT-PA ha proseguito la collaborazione con il CERT Nazionale, avviata come gestione provvisoria sin dal 2018, finalizzata a presentare ai soggetti interessati dalla norma (Operatori di servizi essenziali e Fornitori di servizi digitali) un'unica interfaccia di servizio.
Il DPCM attuativo ha definitivamente stabilito che lo CSIRT italiano è costituito presso il DIS, e ad esso vengono trasferite le funzioni del Ministero dello sviluppo economico, in qualità di CERT nazionale, e dell'AgID, in qualità di CERT-PA: i tempi di attuazione prevedono che tale trasferimento debba essere completato entro il 6 maggio 2020, data in cui lo CSIRT entrerà pienamente in funzione e contestualmente cesseranno di esistere come soggetti autonomi il CERT Nazionale ed il CERT-PA. Per lo svolgimento dei propri compiti lo CSIRT italiano potrà tuttavia continuare ad avvalersi dell'AgID, come previsto dal D.Lgs 65/2018, secondo modalità stabilite da un accordo da stipularsi tra le parti entro il 22 marzo.

Il CERT-PA dunque concluderà il suo mandato istituzionale entro i primi mesi del 2020; rimarrà tuttavia in funzione come centro di competenza di eccellenza all'interno di AgID, proseguendo la sua attività di indirizzo e supporto verso l'Agenzia e, tramite essa, verso tutte le Amministrazioni. Il CAD infatti attribuisce ad AgID i compiti di:

- definire linee guida (tra l'altro) nel settore della sicurezza (art. 14-bis, comma 2 lett. a)
- vigilanza sui servizi fiduciari ai sensi del regolamento UE eIDAS in qualità di organismo a tal fine designato, sui gestori di posta elettronica certificata, sui conservatori di documenti informatici accreditati, nonché sui soggetti, pubblici e privati, che partecipano a SPID; (art. 14-bis, comma 2 lett i)) [gli obblighi comunitari di vigilanza fanno particolarmente riferimento alle problematiche di sicurezza]
- emanare regole per individuare le soluzioni tecniche idonee a garantire la protezione, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati e la continuità operativa dei sistemi e delle infrastrutture. (Art. 51, comma 1)
- attuare, per quanto di competenza e in raccordo con le altre autorità competenti in materia, il Quadro strategico nazionale per la sicurezza dello spazio cibernetico e il Piano nazionale per la sicurezza cibernetica e la sicurezza informatica. (art. 51, comma 1-bis)

Inoltre le PA e i gestori di servizi pubblici, aderiscono ogni anno ai programmi di sicurezza preventiva coordinati e promossi da AgID secondo le procedure dettate dalla medesima AgID con le Linee guida. (art. 51 comma 2-ter).

Elementi sul Cyber-crime nel settore finanziario in Europa

[A cura di Pier Luigi Rotondo, IBM]

Il cybercrime finanziario ha subito una ulteriore evoluzione nel corso del 2019, sia nel modus operandi dei gruppi cyber criminali che nei malware usati. Questa porzione rilevante di tutto il cybercrime è dominata da gruppi internazionali, ben strutturati e organizzati.

L'anno è stato caratterizzato anche da importanti normative europee del settore dei pagamenti, entrate a pieno regime, anche se con alcune proroghe a livello nazionale. Queste promettono buoni risultati il cui impatto però sarà misurabile solo nei prossimi mesi.

Nell'analisi che segue, presento e commento i risultati delle rilevazioni sul cybercrime nel settore finanziario in Europa nel corso del 2019. Questo lavoro è stato possibile anche grazie ai contributi del team di ricerca IBM Security, IBM X-Force, i dati forniti da IBM Trusteer, e al lavoro quotidiano di molti colleghi IBM che l'autore desidera ringraziare.

Tutte le fonti consultate sono elencate nella bibliografia al termine del capitolo

Un anno di cybercrime finanziario

Le analisi delle principali campagne di attacco del 2019 ha mostrato che il fenomeno delle frodi finanziarie su Internet ha coinvolto un numero ampio di malware, ma si è anche avvalso in maniera rilevante dello sfruttamento malevolo degli strumenti di sistema operativo. Molti i malware usati. TrickBot, Gozi/Ursnif, Bugat/Dridex, Necurs e GootKit sono stati i principali, seguiti da una nutrita lista di altri malware con un impatto minore sul mercato EMEA (Europa, Medio Oriente e Africa), preso in considerazione. Per la prima volta riportiamo nel diagramma anche la rilevante porzione di compromissioni del browser, molte e diverse che coinvolgono tutte le componenti (plug-in, estensioni, altro).

Nel diagramma di **Figura 1**, e in tutto lo studio che segue, analizziamo il solo malware per frodi finanziarie e bancarie, sottoinsieme di tutto il malware. La prima analisi è relativa alla distribuzione dei malware sui dispositivi infetti.

Cumulativamente, i 3 malware più diffusi nel corso dell'anno (TrickBox, Gozi/Ursnif e Bugat/Dridex) assommano a solo il 41% di tutte le infezioni, e quindi la maggior parte delle infezioni derivano dalla pletora di altri malware che mai come quest'anno sono riusciti a farsi spazio e guadagnare una cerca popolarità.

Oltre che le infezioni su dispositivi, abbiamo misurato e analizzato la quantità di traffico riconducibile a ciascun malware. Qui rientra non solo il traffico generato dai dispositivi infetti verso i siti da attaccare (prevalentemente banche e istituzioni finanziarie nel nostro caso), ma anche il traffico legato alla esfiltrazione di credenziali dai dispositivi infetti, e quello da e verso le reti di Command-and-Control dai quali i malware scaricano moduli, aggiornamenti, target list e configuration files.

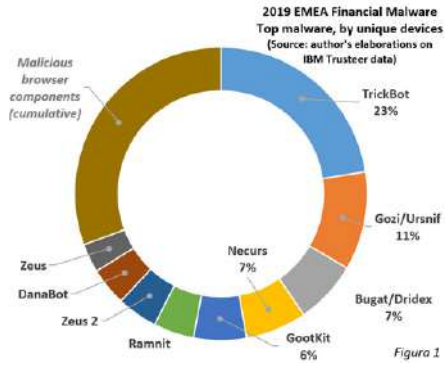


Figura 1

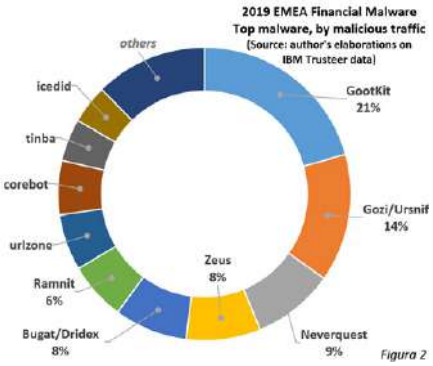


Figura 2

Questo tipo di rilevazione (**Figura 2**) è di particolare importanza per chi fornisce servizi su Internet, in quando permette al gestore di classificare una connessione, e le transazioni in essa condotte, come malevola, e agire per prevenire potenziali frodi. Il diagramma delle rilevazioni in EMEA (Europa, Medio Oriente e Africa) relativamente alle connessioni da dispositivi infetti da malware rivela uno spaccato leggermente diverso.

Le campagne che generano maggiore traffico sono costruite attorno ai malware GootKit, Gozi/Ursnif, Neverquest, seguiti dalla famiglia dei malware derivati dal codice di Zeus, Bougat/Dridex, e poi una lunga lista di altri malware.

Nel raffrontare i due diagrammi occorre tenere in giusta considerazione il differente comportamento di ciascun malware, e soprattutto come vengono rilevati i dati.

Mentre il diagramma di **Figura 1** misura la capacità del malware di evadere le protezioni di rete e di sistema, e infettare il dispositivo, la **Figura 2** invece misura la quantità di traffico che i dispositivi infetti hanno generato.

Una soluzione di sicurezza deve assolutamente tenere in considerazione entrambi i fenomeni, combinandoli per proteggere ciascuna transazione.

TrickBot

TrickBot è un malware per sistemi Windows, complesso e articolato e specializzato nel furto di credenziali per l'accesso a siti bancari. È stato individuato per la prima volta nell'agosto 2016, e attribuito ad un gruppo cyber criminale Russo.

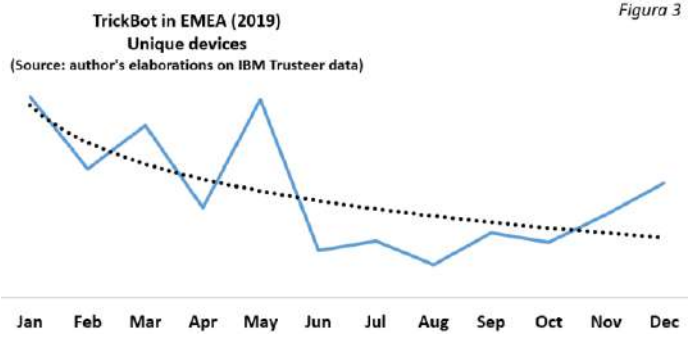
TrickBot è solitamente scaricato e installato su un computer tramite altri malware, il più famoso dei quali è Emotet. Quest'ultimo è distribuito tramite e-mail di spam con allegati documenti Office, e ha spiccate capacità di offuscamento, evasione dai prodotti anti-malware, e se individua computer non aggiornati, anche capacità di propagazione da computer a computer. Emotet era originariamente nato come malware bancario, ma da qualche tempo si è specializzato nel veicolare altri malware, tra cui TrickBot.

Nelle versioni usate a partire dall'inizio 2019 TrickBot disabilita il Windows Defender (che

comunque segnalerà all'utente che il computer non è protetto) e Sophos [1], e si guadagna la persistenza creando uno scheduled task per controllare periodicamente il funzionamento di tutte le componenti, e rieseguirsi.

TrickBot è composto da una serie di moduli, tra questi il pwgrab è specializzato nella cattura di credenziali all'interno del sistema per poi inviarle all'esterno in forma criptata attraverso la infrastruttura di Command-and-Control. Il modulo pwgrab di TrickBot era già in grado di catturare le credenziali dal browser durante la navigazione sui siti bancari, anche con l'uso di webinject per indurre l'utente a digitare altri fattori di autenticazione, o altri dati sensibili come ad esempio tutti i dati della carta di credito. Questo è il compito principale di TrickBot, e ha dimostrato di farlo particolarmente bene. Successivamente a TrickBot sono state aggiunte funzionalità per impossessarsi delle credenziali di accesso a Outlook, WinSCP, Filezilla. Nel corso del 2019 pwgrab è stato aggiornato per la cattura di credenziali delle applicazioni di accesso remoto, come Windows RDP (Remote Desktop Protocol), VNC, PuTTY e le chiavi private di OpenSSH memorizzate in %USERPROFILE%\.ssh, spesso usate per l'amministrazione di sistema con le credenziali amministrative, e poi le userid e password usate in TeamViewer, le credenziali OpenVPN salvate nella registry, le credenziali Git memorizzate localmente, l'intero database locale del KeePass Password Manager, i certificati di SSL memorizzati localmente, e i file dei wallet Bitcoin [2].
Presumibilmente a partire da fine 2019 il nuovo modulo ADll di TrickBot viene usato per accedere anche al database di Active Directory di Windows [3] e al file ntds.dit che contiene utenti, password sotto forma di hash, gruppi, condivisioni, e altre preziose informazioni.
TrickBot è stato uno dei malware più aggressivi del 2018 e così si è confermato nel 2019.
In passato gli operatori di TrickBot si erano concentrati con attacchi mirati verso la clientela business e clienti con grossi asset, ma a partire dal 2018 hanno diversificato i loro attacchi includendo siti di commercio elettronico e piattaforme di gestione di cripto valuta. [4]

Figura 3



Nel corso degli anni TrickBot ha preso di mira obiettivi in tutto il mondo, con una prevalenza di siti anglofoni, come Regno Unito e Stati Uniti. Pochi malware sono riusciti a mantenersi efficaci così a lungo, indicando che i suoi operatori hanno competenze, risorse

e connessioni a sufficienza per continuare a fare evolvere e gestire questo malware.
Ciascuna campagna è caratterizzata da una articolata lista di obiettivi colpiti tutti assieme, prima che l'efficacia della campagna si attenui, fino a scomparire nel giro di qualche giorno, a causa dell'identificazione da parte delle soluzioni antifrode e antimalware.
Nella prima parte dell'anno numerose campagne di spamming veicolano TrickBot all'interno di e-mail contenenti allegati Office, verso utenti in Europa [5]. La tecnica è piuttosto semplice e consiste in un messaggio all'interno del documento che invita l'utente ad abilitare le macro, e successivamente a cliccare su un link dal quale viene poi scaricato il codice del malware. Molti utenti si fidano e infettano le loro macchine.
Alla fine di luglio inizia un'importante campagna di spamming in Italia che veicola malware TrickBot, ai danni di dipendenti della Pubblica Amministrazione [6]. In questo caso la mail in lingua italiana fa riferimento a moduli da compilare relativi alla normativa GDPR. I link all'interno della e-mail, se cliccati, scaricano localmente un file zip che una volta aperto contengono un file VBScript offuscato. Cliccando sul file .vbs il contenuto viene decodificato, e il codice così ottenuto si occupa di scaricare ed eseguire il malware vero e proprio. Una seconda campagna, più evoluta della prima, dopo aver scaricato e lanciato il file in memoria, si occuperà di cancellarlo da disco per renderne più difficile l'individuazione da parte dei prodotti antimalware.
Qualche mese più tardi [7] una nuova versione di TrickBot ottimizza questo meccanismo sui sistemi Windows 10, in veloce diffusione a causa del fine supporto di Windows 7 e la conseguente migrazione. La componente loader controlla i dettagli. Se la versione è precedente alla 10, i file vengono salvati localmente. Invece, se TrickBot è in esecuzione su Windows 10, i moduli TrickBot e i file di configurazione rimangono solo in memoria senza essere salvati localmente, il che significa che il malware scaricare moduli e configurazioni ad ogni reboot, ma a vantaggio di un migliore offuscamento.
Tra settembre e dicembre 2019 compaiono anche alcune campagne di phishing the veicolano TrickBot attraverso link a documenti Google Docs, contenenti il malware. Il documento Google Docs in realtà è una pagina che simula un problema nell'apertura del file, e invita l'utente a scaricare il documento manualmente ed aprirlo sul proprio computer. Il file che si scarica, è un eseguibile .exe camuffato da PDF, e sfrutta alcune limitazioni di Windows nella visualizzazione delle estensioni dei file, assieme ad una icona di Acrobat Reader abilmente associata al file exe. Il doppio click sull'icona del reader esegue il file, installando TrickBot sulla macchina della vittima.
A gennaio 2020 una nuova campagna diffonde Trickbot in messaggi e-mail che sostengono di contenere documenti doganali da riempire a seguito di spedizioni non andate a buon fine, e generati da mittenti reali le cui caselle postali sono state presumibilmente compromesse.

GootKit

GootKit è stato il primo malware a fare uso della tecnica dei redirection attack in Italia, con una campagna contro sei banche italiane [8] nel 2017. La tecnica dei redirection attack, cresciuta enormemente del corso del 2017 e di cui avevamo parlato nel rapporto CLUSIT 2018 [9], se da un lato era molto difficile da individuare e bloccare, fortunatamente si è rivelata anche molto difficile da gestire, e ha segnato un rallentamento con un conseguente ritorno ai webinject già dal 2018. Anche GootKit torna ai webinject in tutte le campagne in Europa del 2018 (Italia, Regno Unito, Francia, Olanda e Belgio).

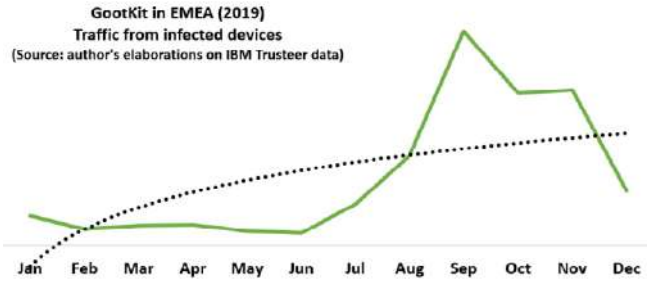


Figura 4

Il 2019 si è aperto per l'Italia sulla coda di una campagna di spamming Gootkit [10] che incrementava la dimensione su disco dell'eseguibile fino a superare 450MB, dimensione scelta per rendere difficile se non impossibile l'analisi automatica in sandbox. Questa release di GootKit implementava numerosi controlli per verificare l'esecuzione in modalità debug o dentro macchine virtuali, segno di un'analisi dell'eseguibile, automatizzata oppure assistita dall'operatore.

A febbraio una campagna di malspam coinvolge utenti in Italia. È veicolata da caselle PEC precedentemente compromesse, con messaggi che sembrano risposte a conversazioni già avvenute. Il file .zip allegato contiene al suo interno un .pdf (innocuo) assieme ad un file .jse contenente codice javascript. Il file .jse, se eseguito, lancia uno script powershell che a sua volta scarica un altro file contenente il malware GootKit, e lo esegue. L'incapsulamento di un file che ne contiene altri è evidentemente una tattica di offuscamento del malware. Questa particolare campagna cerca di catturare le credenziali di accesso a decine di siti web Italiani, molti dei quali però risultano inattivi o di scarso interesse. Evidentemente solo un test per future campagne.

A marzo 2019 un'altra campagna di spamming su PEC prende di mira vittime in Italia [11]. Questa campagna è veicolata attraverso mail che contengono due allegati javascript malevoli, configurati per impossessarsi delle credenziali di accesso alla macchina e inviarle verso l'esterno. Ad aprile una nuova campagna, ancora veicolata via messaggi PEC contenenti una fantomatica comunicazione importante, ancora con 2 allegati, dei quali il primo è innocuo e contiene solo informazioni volte a carpire la fiducia della vittima, mentre il secondo è

una VBScript che scarica il malware GootKit e lo esegue sul computer della vittima.
A luglio ed agosto due distinte campagne [12] [13] usano una tattica molto simile. Una mail contiene un archivio zip, con all'interno un documento Office che contiene una PowerShell, questa scarica il malware JasperLoader che alla fine scarica GootKit. Ancora una volta la complessità della catena e degli incapsulamenti è mirata a offuscare il malware finale e filtrare attraverso le protezioni aziendali.
JasperLoader [14] è un loader, componente specializzata nell'infiltrare la macchina della vittima, evadendo i controlli antimalware e rimanendo offuscata per poi scaricare il payload, un altro malware. Nel 2019 molte campagne in Europa hanno visto la combinazione del JasperLoader che ha scaricato e installato il malware Gootkit, in particolare in Germania e Italia.

Evoluzione del malware per frodi finanziare e bancarie

Tutti i principali malware per frodi finanziarie si sono evoluti verso *piattaforme di attacco*, configurabili di volta in volta per prendere di mira obiettivi anche eterogenei. I malware sono solitamente usati all'interno di campagne caratterizzate da uno stesso ceppo linguistico. In questo modo gli sviluppatori traggono il massimo vantaggio dagli sforzi di localizzazione del malware.
Le piattaforme sono impiegate, a seconda dell'obiettivo, dal semplice furto di credenziali, al furto dei dati della carta di credito, alla sostituzione delle coordinate di pagamento (IBAN o del wallet elettronico), fino ai criptowallet.
L'obiettivo principale dei malware per frodi finanziarie, era e rimane, l'impossessarsi delle credenziali di accesso ai sistemi di pagamento, oppure dei dati delle nostre carte di pagamento, oppure ancora di cambiare di nascosto le coordinate di pagamento. Sempre più spesso però notiamo che i malware operano la cattura di credenziali di accesso ad altri sistemi, tra cui la posta elettronica, oppure le credenziali amministrative di singoli sistemi.
La cattura delle credenziali per accedere alla posta elettronica è un attività apparentemente anomala per un financial malware. I gruppi cyber criminali fanno questo per avere una base dalla quale lanciare successivamente attacchi di tipo BEC, diffondendo malware da caselle elettroniche reali e spesso note alla vittima con una efficacia nettamente maggiore rispetto a quanto non si riesca a fare con il tradizionale phishing. I numerosi esempi ti campagne veicolate tramite PEC ne sono un esempio.
Il caso di TrickBot è eclatante. Nelle ultime versioni cattura le credenziali memorizzate nei browser, quelle di Outlook (sistema di posta elettronica), degli strumenti di amministrazione remota come WinSCP, Filezilla, Windows RDP, VNC, PuTTY, le chiavi private di OpenSSH, OpenVPN, Git, i certificati SSL memorizzati localmente, i cookies e infine i wallet Bitcoin [2] e tutto quanto troviamo in Active Directory [3].
È chiaro che tutto può essere utile per costruire un attacco, oppure per dare maggiore credito ad una e-mail ricevuta, e questo non può che farci pensare che mentre noi analizziamo quanto accaduto, i gruppi cyber criminali stanno già pensando un imprevedibile schema di attacco futuro.

Un panorama di malware sempre più diversificato

Cresce e si diversifica il panorama dei malware usati nelle frodi finanziarie e bancarie.

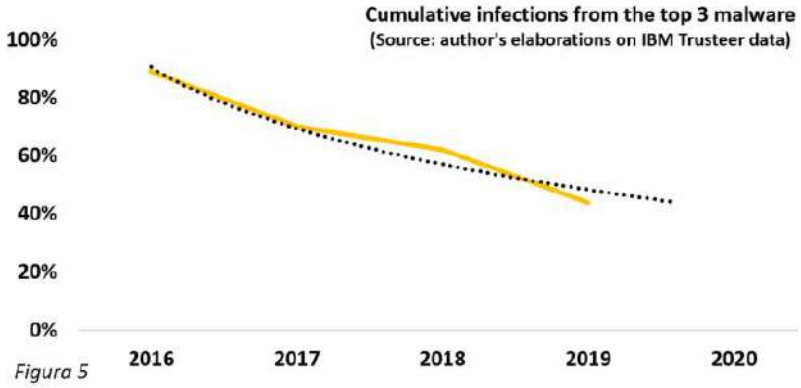


Figura 5

Mettendo assieme i 3 malware più diffusi, TrickBox, Gozi/Ursnif e Bugat/Dridex nella nostra rilevazione sugli endpoint infetti, questi raggiungono il 41% di tutte le infezioni. Nel 2018 [15] i 3 malware più attivi (TrickBot, Gozi/Ursnif e Zeus) raggiungevano assieme il 62% delle infezioni. Tornando a ritroso nel tempo il panorama diventa sempre più concentrato attorno a pochi contendenti. Nel 2017 [9] Dridex, Ramnit e Zeus rappresentavano il 70% delle infezioni, mentre nel 2016 [16] i top 3 (Neverquest, Bugat/Dridex e Gozi) rappresentavano quasi il 90% delle infezioni.

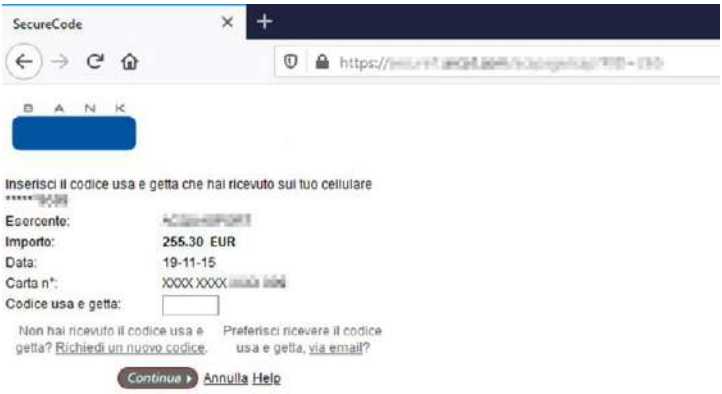
Questo significa che cresce l'influenza dei malware considerati minori, in quanto poco diffusi, e per questo a volte poco studiati. Gli operatori del FinTech devono prepararsi a fronteggiare una varierà sempre maggiore di gruppi cyber criminali, con una conseguente diversificazione delle tattiche, tecniche e procedure operative.

Inoltre, confrontando **Figura 1** e **Figura 2**, si nota come non esista sempre una corrispondenza diretta tra *diffusione* e *attività di rete* di un malware. A causa del diverso meccanismo di azione del malware, e delle tattiche orchestrate dai gruppi cyber criminali, una soluzione anti-malware deve essere in grado di rilevare entrambi le dimensioni del problema, e correlare rilevazioni sulle macchine dell'utente, con le analisi del traffico di rete, e le rilevazioni sul server web che eroga il servizio online e che di fatto riceve i potenziali attacchi.

L'anno dell'Autenticazione Forte del Cliente

Tra le novità introdotte dalla direttiva Europea PSD2 (2015/2366/UE), entrata a pieno regime a Settembre 2019 (seppur con alcune proroghe fino a dicembre 2020), una delle più rilevanti per il contrasto alle frodi è sicuramente l'autenticazione forte del cliente, o **Strong Customer Authentication** (SCA).

L'autenticazione forte del cliente impone che tutte le operazioni con un potenziale rischio di frode, come i pagamenti elettronici a distanza e altre operazioni sui conti online, siano autorizzate usando due o più fattori di autenticazione, scelti combinando qualcosa che solo chi effettua l'operazione conosce (ad esempio un PIN o una password), qualcosa che solo chi effettua l'operazione possiede (ad esempio un'app su un dispositivo mobile), o una caratteristica biometrica dell'utente (impronta digitale, volto, o un'altra caratteristica biometrica). I fattori usati devono essere indipendenti, in modo che la violazione di uno dei fattori non comprometta l'affidabilità degli altri.



Ogni volta che usiamo una carta di pagamento via Internet all'interno dell'area SEPA, il negoziante invia al gestore della carta di pagamento, o ad altri intermediari specializzati, un gran numero di elementi caratteristici della transazione, analizzati all'istante per valutare il livello di rischio della transazione. La valutazione del rischio comporta l'analisi dei dati contestuali inviati dal commerciante, della cronologia delle transazioni del titolare della carta, e numerose altre caratteristiche della transazione come importo, identificativo univoco del dispositivo e la sua posizione. Ciascuna transazione è analizzata singolarmente, e alla fine la maggior parte delle operazioni sono autorizzate all'istante senza eccessive formalità. Nei casi incerti, il gestore della carta introduce elementi aggiuntivi di verifica dell'operazione, ad esempio inviando una OTP (One Time Password) via SMS al nostro cellulare, oppure una richiesta di conferma attraverso l'app bancaria. Un meccanismo analogo avviene quando effettuiamo un bonifico dal nostro conto online.
La Strong Customer Authentication agisce nel contrasto di molte frodi che analizziamo in questo capitolo.

Dal punto di vista pratico, scompariranno le transazioni effettuate solo con una username e una password o un pin statici, facili da catturare e riusare in un secondo tempo. Inol-

tre, nella richiesta del secondo fattore di autenticazione per autorizzare una transazione, deve comparire a schermo un identificativo univoco della transazione, con il beneficiario e l'importo. Avevamo già visto in passato [15] una nuova tattica emersa nella seconda parte del 2018. In almeno due campagne studiate da IBM Security, i malware erano stati usati per seguire e osservare le attività online della vittima senza alcun intervento, lasciandogli effettuare il login e la navigazione all interno di un sito, intervenendo però con webinject solo al momento dell'effettiva operazione dispositiva, sostituendo le coordinate bancarie del beneficiario e l'importo. Questo attacco di fatto non aveva bisogno delle credenziali di accesso dell'utente al sito. La Strong Customer Authentication renderà questa forma di attacco in molti casi più difficili, proprio per le indicazioni che compaiono a schermo al momento dell'autorizzazione della transazione e che sono generate spesso da una piattaforma di pagamento diversa da quella su cui si sta operando. Non impossibile, solo più difficile.
All'interno della Strong Customer Authentication, si cela inoltre una pratica che più di altre potrebbe imprimere una spinta virtuosa al mercato. Un importante scenario di esenzione dalla Strong Customer Authentication è rappresentato dai pagamenti elettronici gestiti da fornitori che riescono a dimostrare un tasso di frode particolarmente basso. In questo caso l'esperienza per il cliente è nettamente migliore in quanto non gli viene chiesto alcun fattore aggiuntivo di autenticazione, con un acquisto completato all'instante e con poche operazioni, ma ancora entro criteri di alta sicurezza. L'importo della transazione esente dipende direttamente dal tasso di frode del fornitore dei servizi di pagamento, e raggiunge fino a 500 nel caso di pagamenti elettronici il cui fornitore mantenga un tasso di frode inferiore allo 0,01%, un obiettivo ambizioso e inferiore all'attuale tasso di frode medio nell'area unica dei pagamenti in euro (SEPA, o Single Euro Payments Area). Questo spingerà l intero sistema dei pagamenti a ridurre costantemente il proprio tasso di frode, per attrarre sempre più clienti con una esperienza di acquisto migliore.

La dimensione del fenomeno delle frodi sulle carte di pagamento

Una parte rilevante delle frodi che analizziamo in questo capitolo si realizzano attraverso un passo finale che prende di mira le transazioni con le carte di pagamento, intese come la vasta categoria che raccoglie le quasi 100 milioni di carte di debito, carte di credito e carte prepagate attualmente attive in Italia [17]. Nel corso del 2018 le famiglie italiane le hanno usate per saldare il 37% di tutti i pagamenti [20], con una crescita del +9% rispetto all'anno precedente.
Secondo i più recenti dati europei [21] il 73% in valore delle frodi sulle carte di pagamento è avvenuto nei pagamenti da remoto su Internet (i cosiddetti pagamenti *Card-Not-Present* o CNP), il 19% nei pagamenti ai terminali POS all'interno di un negozio, e il rimanente 8% nelle operazioni ATM come ad esempio il prelievo di contante. Il contesto italiano ha riportato il 69% di transazioni fraudolente di tipo CNP, 22% su POS e 8% su ATM. Il totale delle transazioni fraudolente sulle carte di pagamento emesse nei 36 paesi dell'area SEPA ha ammontato a 1,8 MLD nel 2016.
Solo il 35% delle transazioni fraudolente è avvenuto all'interno del paese di emissione della

carta. Il 43% delle transazioni fraudolente ha invece avuto luogo in altri paesi SEPA, diversi da quello di emissione. Le transazioni al di fuori dell'area SEPA sono state solo il 2% del totale, ma hanno rappresentato il 22% del valore totale.
I paesi emettitori di carte di pagamento che hanno riportato tassi di frode più alti sono stati Danimarca, Regno Unito, Francia e Irlanda. L'Italia si è posizionata virtuosamente ben al di sotto della media SEPA.
Relativamente all'Italia, sono stati 4930 i casi di frode finanziaria riportati alla Polizia Postale e delle Comunicazioni nel corso 2019. [22]

SIM swap e l'addio agli SMS PIN

La crescita degli attacchi basati sulla cattura delle One Time Password (OTP) inviate via SMS (SMS PIN), assieme ai nuovi tool e librerie sviluppate appositamente per questa attività [23], stanno portando il mercato ad allontanarsi da questo meccanismo [24], in favore di altri strumenti e in particolare delle app che ciascuna banca e operatore finanziario mette a disposizione [25]. Gli SMS sono suscettibili sia di attacchi Man-in-the-Middle (MitM) da parte di malware specializzato, che attacchi di tipo SIM swap. Quest'ultimo attacco si basa su una nuova SIM, emessa ad insaputa della vittima usando un suo documento contraffatto o rubato, e che consente di ricevere gli SMS PIN inviati dalla banca. La vittima di un attacco SIM swap solitamente vede il suo cellulare disconnettersi dalla rete di telefonia cellulare. Contattando il gestore telefonico questo ci dice che avevamo richiesto la sostituzione della SIM in nostro possesso con una nuova. Nel frattempo, i cyber criminali usano la nuova SIM per catturare gli SMS PIN e con questi autorizzano operazioni dal nostro conto.
Le app bancarie, a seconda dell'implementazione, hanno meccanismi alternativi di autorizzazione delle operazioni, che vanno dalle *push notifications*, codici di conferma mostrati a schermo attraverso l'app stessa, all'autorizzazione con l'impronta digitale, e che contribuiscono in maniera robusta all'autenticazione del reale intestatario del conto, essendo più difficili da catturare rispetto agli SMS. È quindi buona pratica installare e usare le app bancarie, allontanandosi velocemente dagli SMS. [25]
Nel corso dell'anno Metro Bank (Regno Unito) è stata vittima di un attacco [26] che ha sfruttato una vulnerabilità nel protocollo SS7, usato dagli operatori telefonici per gestire le chiamate e per veicolare SMS, e che ha permesso di intercettare messaggi di testo attraverso la rete, senza alterare il telefono della vittima. Gli *attacchi SS7*, malgrado rari e tecnicamente articolati, sono stati una realtà almeno negli ultimi 10 anni, e hanno permesso di rompere ripetutamente il meccanismo di autenticazione e conferma delle operazioni basato su SMS.

Continua l'ascesa degli attacchi Business E-mail Compromise (BEC)

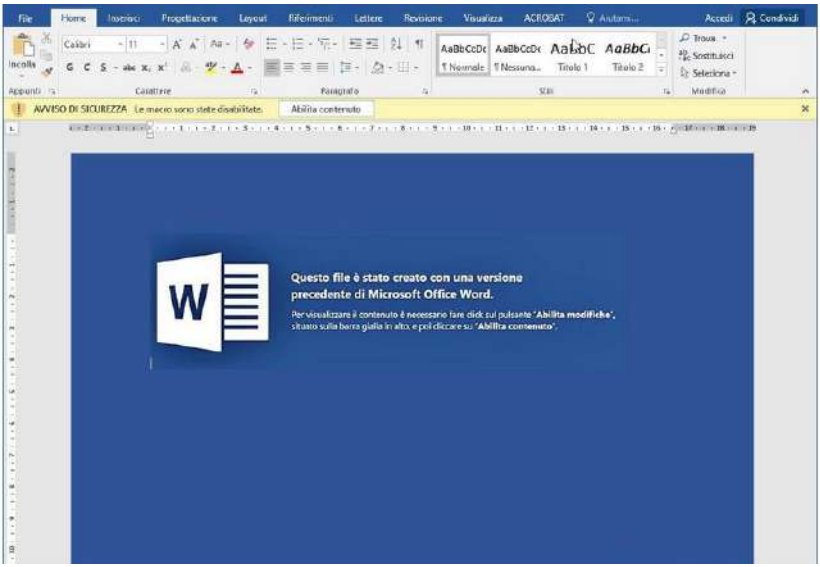
La pubblicazione a Gennaio 2019 di #Collection1, una raccolta con oltre 700 milioni di indirizzi e-mail e decine di milioni di password, ha spianato la strada a ondate di *attacchi BEC*, o Business E-mail Compromise. Gli attacchi Business E-mail Compromise prendono il nome dalla compromissione, o la creazione, di account aziendali (Business) strumentali

per la riuscita dell'attacco. Siamo alle prese con l'ultima evoluzione del phishing, che negli anni continuamente si reinventa in maniera sempre nuova.
Gli attacchi di tipo BEC mirano a trarre in inganno le vittime (solitamente i dipendenti di un'azienda, o gli utenti di un servizio) inducendoli ad autorizzare o effettuare pagamenti fraudolenti per beni o servizi verso conti riconducibili a gruppi di cyber criminali [28]. Esistono molte varianti di BEC. In tutte il social engineering viene portato all'estremo, anche compromettendo le caselle di posta elettronica di dipendenti che ricoprono posizioni chiave. Le versioni più recenti di questi attacchi combinano, a sofisticate tecniche di social engineering e spear phishing, anche l'utilizzo di malware specializzato per frodi finanziarie inserito come allegato all'interno di conversazioni già in corso tra la vittima e un interlocutore noto.
Combinando diverse fonti, l'FBI ha valutato in oltre 12 miliardi di dollari il danno economico complessivo negli ultimi cinque anni [29], con circa 80000 incidenti analizzati in oltre 150 nazioni. Il gruppo di ricerca IBM X-Force riporta che il 29% di tutti gli attacchi osservati durante il 2018 ha avuto origine con e-mail di phishing [30], e il 45% di queste ha contribuito a schemi Business E-mail Compromise. La maggior parte delle transazioni fluisce, attraverso una rete di prestanome, verso conti in Cina e Hong-Kong [22] [30], quindi per bloccare e provare a recuperare le somme frodate è necessaria un'azione tempestiva. Nel corso del 2019 la Polizia Postale e delle Comunicazioni è riuscita a bloccare e recuperare circa 13,5 milioni di euro su una movimentazione fraudolenta individuata in circa 18,8 milioni [22]. Questo è avvenuto grazie alla piattaforma OF2CEN (On line Fraud Cyber Centre and Expert Network) per l'analisi e il contrasto delle frodi, frutto di convenzioni con gran parte del mondo bancario, e che ha consentito di intervenire in tempo quasi reale sulla segnalazione, bloccando la somma prima che ne sia stata persa traccia.

Complici degli attacchi verso noi stessi

Se nel 2019 il principale veicolo di propagazione sono stati documenti Office contenenti script che fanno download del malware, veicolate come attachment, link, documenti caricati su Google Drive e altri canali, il metodo di infezione prevalente è stato l'utente che ha aperto i documenti, spesso togliendo le protezioni che il software ci fornisce. In altri termini, l'elemento che ha contribuito al successo delle principali campagne di malware dell'anno è stata la compartecipazione della vittima.
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. Alcune campagne hanno simulato messaggi legittimi emessi da Windows, come ad esempio incompatibilità tra diverse versioni di prodotto, per indurre l'utente ad abilitare le macro, cioè programmi nascosti all'interno del documento.
Tutte le versioni di Office, a partire da Office 2010 e fino al più recente Office 365 hanno una configurazione di default con macro disabilitate e la visualizzazione protetta abilitata. Questo è sufficiente a garantirci in adeguato livello di protezione. Sono davvero poche le situazioni in cui questo meccanismo ha necessità di essere disabilitato, e comunque mai

su documenti ricevuti da controparti sconosciute o non affidabili. Se la visualizzazione protetta viene disabilitata e le macro abilitate, anche azioni semplici come la preview di un documento malevolo dall'interno del client di posta elettronica possono infettare il nostro computer.



Sfruttamento degli strumenti di sistema operativo

La generale consapevolezza del rischio cyber e il conseguente aumento delle misure di sicurezza spingono i cyber criminali a adattare costantemente le loro tattiche per un migliore ritorno degli investimenti. IBM X-Force continua a notare una decrescente dipendenza dai malware per gli attacchi, mentre più della metà degli attacchi (57%) sfruttano strumenti di amministrazione come la PowerShell, la PsExec e i VBScript [30].

Per gli amministratori di sistema la PowerShell è uno strumento incredibilmente versatile per gestire i sistemi Windows. Lo stesso è per i cyber criminali. La PowerShell è usata per eseguire i VBScript inseriti all'interno di file Office, allegati a mail di phishing. I ricercatori di IRIS (IBM X-Force Incident Response and Intelligence Services) evidenziano l'ascesa nell'uso fraudolento della PowerShell [31], sulla scorta dei successi nell'iniettare il malware in processi Windows in esecuzione, senza la necessità di scaricare file in locale, evadendo di conseguenza molti degli antivirus. Inoltre, le tecniche di encoding native della PowerShell, come la *base64-encoded*, permettono un buon offuscamento del malware con uno sforzo davvero minimo. Non da ultimo, essendo la PowerShell uno strumento di largo e frequente utilizzo in molte attività amministrative Windows, bloccarla porterebbe a conseguenze avverse.

Ascesa del cyptojacking

2017 e 2018 sono stati caratterizzati da notizie di attacchi ransomware di larga scala, WannaCry e NotPetya solo per citarne alcuni. Diverse fonti [30] [32], tra le quali anche Europol [33], evidenziano un declino in termini numerici del fenomeno ransomware nel corso del 2019, con una concentrazione di attacchi mirati a specifiche organizzazioni (ospedali, aziende, pubblica amministrazione) piuttosto che come attacchi generalizzati, verso la grande massa. Il ransomware nella sua forma originaria non si è dimostrato redditizio come originariamente ipotizzato e i cyber criminali cercano forme più remunerative di attacco.
Il declino del ransomware è stato accompagnato da una crescita del cryptojacking, cioè l'installazione di malware per il mining di criptomoneta, che sfrutta potenza di calcolo e energia elettrica della vittima, senza che quest'ultima se ne accorga.

L'IBM X-Force Threat Intelligence Index 2019 [30] parla di una crescita del cryptojacking del 450% nel corso di tutto il 2018, e questo fenomeno è continuato nel 2019.
Cambia il modello di business dell'attacco. Con il ransonware, il gruppo cyber criminale infiltra la macchina della vittima una volta, e si mette in attesa, sperando che la vittima paghi il riscatto (ransom) per riaccedere ai propri dati. Pagamento che fortunatamente accade raramente. Nel criptojacking invece la macchina della vittima lavora per il gruppo cyber criminale, 24h su 24h, producendo un flusso continuo di cripto valuta.

L'anno della sicurezza collaborativa

La velocità con cui gli attacchi prendono di mira le organizzazioni, la loro crescente complessità e automazione, le tecniche di offuscamento e la moltitudine di sistemi e applicazioni, lasciano pochissimo tempo per analizzare il singolo evento, valutarlo e prendere una decisione ponderata.

In questo contesto le piattaforme di Threat Intelligence collaborativa sono un potente ausilio per l'investigazione degli eventi di sicurezza, consentendo di verificare e confrontare allarmi, log, file binari, con una fonte autorevole, e con lo scopo di confermare o escludere una potenziale minaccia. La piattaforma di Threat Intelligence diventa collaborativa quando consente di creare dinamicamente team di lavoro, e condividere in maniera protetta le informazioni sull'investigazione in corso.
Le tre dimensioni di una buona piattaforma di Threat Intelligence collaborativa partono dalla ricerca, per investigare gli incidenti di sicurezza con contenuti curati. La collaborazio-

ne, per validare le minacce e mettere appunto piani di risposta coinvolgendo tutte le parti in causa. E infine l'integrazione della threat intelligence con le altre soluzioni di sicurezza attraverso standard aperti, come le REST API oppure gli standard STIX/TAXII.

Continua l'adozione dell'intelligenza artificiale

Sono molte le aziende che stanno adottando l'intelligenza artificiale (AI) e i sistemi cognitivi. Lo stesso stanno facendo i gruppi cyber criminali.
L'uso dell'intelligenza artificiale nelle soluzioni di sicurezza offerte sul mercato si sta orientando su più linee principali. Anzitutto nella ricerca di pattern su una grossa mole di flussi informativi, per identificare autonomamente nuove frodi. C'è 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, discussioni durante le conferenze, webinar, notizie di agenzia, tweet, advisories e altre fonti che altrimenti rischierebbero di finire ignorate in quanto non fruibili dalle soluzioni di sicurezza finora usate. Qui una parte rilevante è la produzione in linguaggio naturale e non trascritta. 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 una tecnologia che sostituisce il security analyst, ma piuttosto una tecnologia a supporto del security analyst, di cui incrementa sensibilmente la produttività.
I sistemi di AI sono però potenzialmente aperti a nuove forme di attacco che non esistono nei sistemi tradizionali. L'adversarial attack è una forma di attacco che inietta, nei sistemi di Machine Learning, input appositamente creati per innescare errori. Variazioni di dati, impercettibili per un umano, possono portare fuori strada gli algoritmi ML. Indubbiamente un nuovo asset da proteggere, a mano a mano che i sistemi di Intelligenza Artificiale entrano a far parte delle soluzioni di sicurezza di un'organizzazione.

Conclusioni

Il terreno delle frodi finanziarie è dominato da gruppi cyber criminali tecnicamente competenti e ben organizzati, pronti a cambiare rapidamente tattica se necessario a portare un riscontro economico. I professionisti della sicurezza sono chiamati a adottare lo stesso approccio. Ma c'è una differenza. Mentre gli attaccanti possono abbandonare soluzioni rivelatesi non remunerative, le aziende devono tenere sotto controllo la complessità, difendendo tutto il perimetro aziendale. Per questo, servono strumenti in grado di integrare tutte le soluzioni di protezione.
Il rischio di cyber attacchi cresce, anno dopo anno. A livello globale, il 76% delle organizzazioni prevede di pianificare aumenti del budget per la sicurezza nel 2020 [34].
Affinché una frode produca un ritorno economico serve una concomitanza di elementi. La capacità tecnologica di costruire e mantenere un malware, l'infrastruttura di Command-and-Control e le componenti di anonimizzazione ed encryption del traffico di rete. Gli attacchi richiedono poi una conoscenza accurata dell'interfaccia del sito di banking, con

una localizzazione dei messaggi che compaiono durante l'attacco nella lingua della vittima. Infine, per ogni attacco che ha successo, occorre una rete di spalloni digitali o *money mule* che fanno fluire la somma frodata di conto in conto, fino a renderne difficoltoso il recupero.
Le soluzioni di **fraud protection** combinano numerosi indicatori di rischio per identificare la sessione sospetta, prima che la transazione venga finalizzata. Ogni volta che effettuiamo un pagamento con la nostra carta di credito su Internet, il negoziante invia al gestore della carta di credito oltre 100 elementi caratteristici della transazione (data point), analizzati all'istante per valutare il livello di rischio della transazione. La valutazione del rischio comporta l'analisi dei dati contestuali inviati dal commerciante, della cronologia delle transazioni del titolare della carta, il suo rapporto con il sito internet, se è un utente abituale, l'analisi delle altre transazioni, oppure se ha effettuato l'acquisto come guest. Fattori di autenticazione apparentemente non visibili, come il device fingerprinting, la geolocalizzazione, l'IP reputation, i dati degli operatori di telefonia mobile (MNOs), possono contribuire in maniera sostanziale a verificare l'identità dell'utente per una valutazione del rischio di ciascuna transazione, e decidere come agire per prevenire una frode senza impattare le operazioni legittime.

La password, come le abbiamo conosciute finora, sono ormai destinate a un veloce e inesorabile declino. Il *Future of Identity Study 2018* [27] 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 è quella della **Multi-Factor Authentication (MFA)** [35], o autenticazione a più fattori, nella quale si combinano più elementi di autenticazione, appositamente scelti e combinati per rendere la compromissione del sistema più complessa. I malware che nel corso del 2019 hanno implementato la cattura degli SMS come fattore di autenticazione (2FA) basato sull'SMS, assieme ai tool e librerie sviluppate appositamente per questa attività [23], ci invitano ad abbandonare quanto prima anche gli SMS come fattore di autenticazione. Fortunatamente sull'MFA è possibile costruire scenari di autenticazione decisamente più robusti [35] e difficili da raggirare. Tra questi il **password-less login** basato sulla scansione di un QR Code con un dispositivo precedentemente associato a noi, oppure l'uso delle numerose **app authenticator**, con PIN di autenticazione che cambia continuamente, 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 sé l'ulteriore vantaggio di mantenere le credenziali biometriche confinate all'interno del nostro dispositivo.
La **User Behavior Analytics (UBA)** [36] 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 anomale dei cyber criminali che cercano di impersonificare la vittima, autenticandosi con le sue credenziali. Lo fa analizzando una grande quantità di elementi sul comportamento online dell'utente, finora ignorati. La User Behavior Analytics dovrebbe essere la naturale evoluzione di ciascun sistema **SIEM**.

Queste soluzioni, già disponibili, aggiungono contesto all'utente e al dispositivo usato, e contribuiscono a misurare in maniera accurata il livello di rischio di ciascuna transazione. Si apre la strada verso il **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 [37]. 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 come ad esempio l'uso di un ulteriore fattore di autenticazione.
In un contesto mutevole come quello descritto, qualsiasi sia la soluzione scelta, questa deve potersi evolvere per adattarsi rapidamente alle nuove tattiche di attacco. Ad esempio, un SIEM adesso deve individuare utilizzi malevoli della PowerShell, e deve integrarsi con i **feed di Threat Intelligence** per avere in tempo reale l'indice di rischio di un indirizzo IP, di una URL, di un attachment, o capire se la nostra rete sta comunicando con un una botnet.

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'intelligenza artificiale ci sta aprendo a fonti di informazione che in passato non erano mai state integrate nei processi aziendali.
Se da un lato possiamo vedere nell'intelligenza artificiale un potente ausilio a supporto del lavoro delle figure coinvolte nella cyber security, dall'altro i possibili vettori di attacco ai sistemi intelligenti sono ancora poco chiari. Indubbiamente aumenta la superficie di attacco e quindi una delle aree chiave sulla quali la security aziendale deve concentrarsi è la protezione dei sistemi basati su intelligenza artificiale. Protezioni adeguate per esseri umani potrebbero improvvisamente cadere di fronte a sistemi appositamente addestrati. L'area della sicurezza biometrica, in particolare quella del riconoscimento della voce e del volto, e più in generale quella dell'autenticazione, è quella più a rischio.

Fondamentale il ruolo dei **Security Operation Center (SOC)** e di tutte le figure che in essi operano. 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. Una **piattaforma di Threat Intelligence** è lo strumento fondamentale per l'investigazione degli eventi di sicurezza, consentendo di verificare velocemente alert, log, file binari, con gli IOC (Indicator of compromise - indicatori di compromissione) su una fonte autorevole e aggiornata, per confermare o escludere una potenziale minaccia. La piattaforma di Threat Intelligence deve essere collaborativa, e consentire di creare dinamicamente team di lavoro per condividere in maniera protetta le informazioni sull'investigazione in corso. La piattaforma deve essere inoltre interrogabile attraverso standard aperti, per poterla integrare con le altre soluzioni e applicazioni di sicurezza.

I malware e le Tattiche, Tecniche e Procedure (TTPs) dei gruppi cyber criminali si evolvono continuamente. Qualsiasi informazione può essere utile per costruire un attacco, oppure contribuire a dare maggiore credito a e-mail di phishing o BEC. Mentre noi analizziamo gli attacchi appena accaduti, i gruppi cyber criminali stanno già pensando al prossimo schema di attacco.
Il panorama è articolato e mutevole, ma non mancano le buone notizie. L'Italia si è dimostrata virtuosa nell'ambito del contesto europeo delle frodi sulle carte di pagamento. L'entrata a pieno regime della direttiva PSD2, in particolare della **Strong Customer Authentication**, renderà più difficili alcune tecniche di attacco delineatesi nel recente passato, con risultati il cui impatto sarà misurabile solo nei prossimi mesi.

Bibliografia

[1] M. Praszmo *Detricking TrickBot Loader* CERT Polska, Febbraio 2019
[2] *Trickbot's Updated Password-Grabbing Module Targets More Apps and Services* TrendMicro, December 2019
[3] L. Abrams *TrickBot Now Steals Windows Active Directory Credentials* BleepingComputer, January 2020
[4] O. Harpaz *TrickBot's Cryptocurrency Hunger: Tricking the Bitcoin Out of* Wallets SecurityIntelligence, February 2018
[5] *Threat Alert: MalSpam* Threat Advisories and Attack Reports Radware, Gennaio 2019
[7] O. Ozer *The Curious Case of a Fileless TrickBot Infection* SecurityIntelligence, August 2019
[6] *Campagne di malspam con varianti di Trickbot ai danni della PA* CERT-PA, Luglio 2019
[8] Limor Kessem *GootKit Malvertising Brings Redirection Attacks to Italian Banks* SecurityIntelligence, Maggio 2017
[9] Pier Luigi Rotondo, Domenico Raguseo *Alcuni elementi sul cybercrime nel settore finanziario in Europa* Rapporto CLUSIT 2018 sulla sicurezza ICT in Italia, Marzo 2018
[10] *Malspam Gootkit con dropper da 450+ MB* d3Lab, Dicembre 2018
[11] *Campagna di malspam Gootkit indirizzata verso PEC italiane* AGID CERT-PA, Marzo 2019
[12] *Campagna Gootkit tramite JasperLoader verso Pubbliche Amministrazioni* CERT-PA, Luglio 2019
[13] *Nuova campagna Gootkit (tramite JasperLoader) verso le PP.AA.* CERT-PA, Agosto 2019
[14] N. Biasini, E. Brumaghin, A. Williams *JasperLoader Emerges, Targets Italy with Gootkit Banking Trojan* Cisco Talos, April 2019
[15] Pier Luigi Rotondo, Domenico Raguseo *Elementi sul cybercrime nel settore finanziario in Europa* Rapporto CLUSIT 2019 sulla sicurezza ICT in Italia, Marzo 2019
[16] Pier Luigi Rotondo, Domenico Raguseo *Alcuni elementi sul cybercrime nel settore finanziario in Europa* Rapporto CLUSIT 2017 sulla sicurezza ICT in Italia, Marzo 2017
[17] *Osservatorio Carte di Credito e Digital Payments* Assofin, Nomisma, Ipsos e Crif, Settembre 2019
[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] *Mobile Payment in Italia: continua la crescita dei pagamenti innovativi* Osservatori Digital Innovation del Politecnico di Milano, Marzo 2019
[21] *Fifth report on card fraud* European Central Bank – Eurosystem, September 2018
[22] *Il resoconto dell'attività della Polizia Postale e delle Comunicazioni nel 2019* Dicembre 2019
[23] *New Reverse Proxy Tool Can Bypass Two-Factor Authentication and Automate Phishing Attacks* SecurityIntelligence.com, Gennaio 2019
[24] Limor Kessem IBM X-Force Security Predictions for 2020 SecurityIntelligence.com, December 2019
[25] Pier Luigi Rotondo *Shopping e saldi invernali più sicuri con i pagamenti elettronici* IBM thinkMagazine, Dicembre 2019 https://ibm.biz/acquistisicuri
[26] J. Cox *Criminals Are Tapping into the Phone Network Backbone to Empty Bank Accounts* Motherboard, January 2019
[27] Limor Kessem *Future of Identity Study 2018* IBM Security, January 2018
[28] Pier Luigi Rotondo *Sai cosa sono gli attacchi BEC?* IBM thinkMagazine, June 2019 https://ibm.biz/attacchibec
[29] *Business E-mail Compromise The 12 Billion Dollar* Scam FBI, July 2018
[30] *2019 IBM X-Force Threat Intelligence Index* February 2019
[31] Camille Singleton *An Increase in PowerShell Attacks: Observations From IBM X-Force IRIS* SecurityIntelligence.com, October 2018
[32] John Zorabedian *Cryptojacking Rises 450 Percent as Cybercriminals Pivot From Ransomware to Stealthier Attacks* SecurityIntelligence, February 2019
[33] Internet Organised Crime Threat Assessment (IOCTA) 2019 Europol, October 2019
[34] *FireEye Cyber Trendscape Report* FireEye, November 2019
[35] Pier Luigi Rotondo *Multifactor Authentication Delivers the Convenience and Security Online Shoppers Demand* SecurityIntelligence, January 2019 https://securityintelligence.com/multifactor-authentication-delivers-the-convenience-and-security-online-shoppers-demand/
[36] T. Obremski *Take a Dive: Deep Network Insights for Deeper Analytics* SecurityIntelligence, December 2017
[37] *Deloitte Christmas Survey 2019* Deloitte, November 2019
[38] Directive (EU) 2015/2366 of the European Parliament and of the Council Official Journal of the European Union, November 2015
[39] Pier Luigi Rotondo *How Will Strong Customer Authentication Impact the Security of Electronic Payments?* SecurityIntelligence, September 2019 https://securityintelligence.com/posts/how-will-strong-customer-authentication-impact-the-security-of-electronic-payments/
[40] Pier Luigi Rotondo *Come proteggersi dagli attacchi Business Email Compromise* INTESA, May 2019 https://www.intesa.it/come-proteggersi-dagli-attacchi-business-email-compromise/

[41] Pier Luigi Rotondo *Acquisti online? Ecco come farli in modo sempre più sicuro* IBM thinkMagazine, Dicembre 2018 https://ibm.biz/ibmblackfriday
[42] Pier Luigi Rotondo *IBM X-Force: un passo avanti nella difesa dagli attacchi finanziari più evoluti* IBM thinkMagazine, Febbraio 2018 https://ibm.biz/pierluigirotondo
[43] Pier Luigi Rotondo *Proteggere le risorse informative con la sicurezza cognitiva e con soluzioni in grado di adattarsi alle minacce future* ICT Security Magazine n.140/2016, October 2016
[44] M. Schieppati *I 5 tech-trend del 2020 in banca* Bancaforte, Gennaio 2020

Profilazione delle minacce e scambio di informazioni nelle attività di cyber intelligence

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

La dimensione *cyber* caratterizza, in modo diretto o indiretto, gran parte delle minacce contemporanee.
La minaccia cibernetica costituisce sempre più il vettore o il terminale di un vasto coacervo di fenomeni di natura diversa spesso inseriti in un quadro di operazioni statuali e di guerra ibrida.
L'evoluzione dello scenario internazionale, caratterizzato da minacce sempre più complesse e interconnesse, richiede l'approntamento di nuovi strumenti.
L'impiego di tecniche di *intelligence* rappresenta un complemento essenziale ai classici presìdi di *cybersecurity*. La *cyber intelligence* si basa su acquisizione informativa e capacità di analisi: a queste attività afferiscono l'*information sharing* e il *threat modeling*.
Per ogni organizzazione risulta di primaria importanza individuare i fenomeni che possono avere impatti su patrimonio compiti e reputazione, nonché reperire e condividere informazioni. Tale condivisione mira ad accrescere il grado di conoscenza collettiva della minaccia e ad aumentare la capacità sistemica di prevenzione e contrasto.

Aspetti definitori

Il *threat model* mira all'individuazione di potenziali minacce e alla definizione del relativo grado di pericolosità in relazione agli *assets* da proteggere.
Partendo dal possibile punto di vista di un attaccante o di un agente di minaccia, tale modello definisce il profilo delle potenziali minacce e le caratteristiche degli stessi agenti di minaccia (persone fisiche, altre organizzazioni, entità governative, eventi naturali ed esogeni, etc.).
Considerando i rapidi cambiamenti dello scenario globale e la complessità intrinseca di molte organizzazioni che operano in settori strategici, la modellizzazione delle minacce è da intendersi come attività costante e in continua evoluzione.
Stante il quadro sopra delineato in materia di interconnessione di minacce, ad un approccio classico incentrato sulla gestione del rischio, appare più efficace un modello basato sulla gestione preventiva delle minacce.
Nella definizione del modello, sono state tenute in considerazione le principali correnti metodologiche e gli strumenti esistenti per il *threat modeling*, specie in campo IT (ad esempio, DFD - *data flow diagrams*, PFD – *process flow diagrams*, ATM – *application threat model*, OTM – *operational threat models*, DMM – *detection maturity model*, OCTAVE, VAST, STRIDE, *attack trees*, P.A.S.T.A., Trike).
Preliminarmente, è opportuno introdurre alcuni concetti e definizioni di base afferenti alla

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

semantica di un *threat model*. Il vocabolo "*threat*"[2] (minaccia) è attualmente inteso come un possibile e imminente pericolo; il concetto è anche interrelato al potenziale sfruttamento di vulnerabilità e alla violazione del perimetro di sicurezza.
Il termine inglese "*model*" (dal latino "*modĭlus*", modello) indica un riferimento teorico da poter riprodurre e aggiornare costantemente sulla base dell'esperienza (e si aggiunge - in conformità al metodo scientifico – sulla base dell'esperimento); in questo ambito, l'aggiornamento è anche legato alla conoscenza riveniente dallo sviluppo di indagini sul campo.
Il presente modello, autonomo e sinottico, mira primariamente a: descrivere un insieme teorico di strumenti di livello superiore (*layer* 1) per l'identificazione di ontologie; introdurre strumenti concreti di implementazione (*layer* 2), in particolare la *threat matrix* (questa matrice non viene sviluppata qui, ma vengono esposti i criteri per la sua valorizzazione).[3]
Il *cyber threat model*[4] è da intendere come sotto-insieme del *threat model* in relazione ad una specificità di dominio: il cyberspazio.
Sia per il *threat model*, sia per il *cyber threat model* vi sono peculiarità di classificazione. Considerando la trasversalità del dominio *cyber*, si devono vagliare non solo quelle che hanno diretta attinenza al mondo ICT o che riguardano specificatamente funzioni informatiche, ma anche altri tipi di minacce. Un evento di altra natura potrebbe comportare conseguenze su operazioni e processi informatici e pertanto deve essere ricompreso nel novero delle minacce afferenti al dominio *cyber*.
Il *threat model* presuppone una tassonomia delle minacce e una categorizzazione dei possibili effetti. Le minacce sono generalmente raggruppate secondo diverse ontologie. Se ne propone qui una suddivisione per natura: minaccia intenzionale (esogena - ad esempio attacchi informatici, spionaggio informatico e attacchi fisici; endogena - ad esempio minaccia interna), involontaria e/o accidentale (ad esempio, avaria), ambientale (ad esempio, evento naturale, pandemico), sociale (disoccupazione, rivolte, crolli finanziari, migrazioni, carestie etc.), causata da negligenza (ad esempio, incuria o disattenzione), fisiologica (es. obsolescenza tecnologica).
Quanto ai possibili effetti della minaccia, occorre distinguere tra effetti diretti e indiretti. Tra quelli diretti, si evidenziano: effetti fisici (incendio, calamità naturale, terremoto, pandemia etc.), interruzione di servizi (guasto dell'infrastruttura, interruzione di servizio, guasto tecnico temporaneo...), perdita materiale (furto, danneggiamento di beni, violazione di dati con effetti materiali diretti...), perdita immateriale (danno alla reputazione, danno all'imma-

[2] Derivato dall'inglese antico "*threat*" (per oppressione), di origine germanica, legato all'olandese "*verdrieten*" (addolorarsi) e al tedesco "*verdriessen*" (irritare).

[3] La matrice della minaccia rappresenta in dettaglio l'incrocio tra vulnerabilità, obiettivi, capacità dell'attaccante, TTP e dinamiche dei vettori di attacco per ogni macro-categoria. In questa fase, ciascuna organizzazione focalizza la profilazione sui propri *asset* e sulle proprie vulnerabilità, in base a una determinata minaccia. Per ogni macro-categoria (es. *cyber crime*), vi possono essere sotto-categorie, con minacce e agenti di minaccia specifici (es. galassie *cyber* criminali comparto finanziario).

[4] La parola "*cyber*" deriva dall'inglese "*cybernetics*", che a sua volta ha origine dalla antica radice greca **κυβερ**- (da cui anche il latino *guber*- e *gubernator*, timoniere). Oggi il termine si riferisce, in linea generale, al mondo dell'informatica, di Internet e dei computer.

gine, violazione di dati ..). L'interconnessione delle minacce e i fenomeni di minaccia ibrida possono comportare anche effetti indiretti (es. una minaccia che produce primariamente effetti fisici, può avere ripercussioni indirette su perdite materiali e immateriali).
I concetti di *threat model* e *cyber threat model* sono collegati a quelli di "vulnerabilità", "*target"* e "agente di minaccia".
Una "vulnerabilità" (dall'antico latino "*vulnus*", ferita, danno o dolore) è intesa come una debolezza che può essere sfruttata da un attore della minaccia, ad esempio un attaccante, per eseguire azioni non autorizzate all'interno di un sistema informatico o anche come un difetto intrinseco nei sistemi e nell'organizzazione, a fronte di eventi naturali ed esogeni.
La parola "*target*" (dal francese "*targuete*", piccolo scudo) indica un obiettivo. In questo frangente, si riferisce a una persona o a un'organizzazione oggetto di un attacco o influenzata da un'azione; o più specificamente a un *asset* (materiale/immateriale) di una persona o di un'organizzazione.
I due concetti - obiettivi e vulnerabilità - ancorché distinti e speculari, sono quindi qui trattati congiuntamente. A ben vedere, i *target* e le vulnerabilità possono essere trattati come due facce della stessa medaglia: in effetti, al di là del concetto di "obiettivo" di alto livello (scopo), l'obiettivo concreto a cui mira un avversario e in cui una minaccia potrebbe andare a segno, risiede proprio nelle vulnerabilità.
La locuzione "agente di minaccia" indica sia un evento naturale e/o esogeno sia un individuo o un gruppo di individui (attaccanti) che possono causare una minaccia.
L'*information sharing*[5] indica una condivisione, uno scambio di informazioni. È a volte indicato – con il medesimo significato, ma con espressione diversa – come *information exchange*.
Per quanto concerne le relazioni tra attività di *threat modeling*, *information sharing* e *cyber intelligence*, vi sono diversi collegamenti, che riguardano sia l'attività di acquisizione informativa sia quella di analisi.
Da un lato il *threat model* orienta la politica di acquisizione informativa alimentando i *priority intelligence requirements* (PIR),[6] dall'altro la conoscenza riveniente dall'acquisizione informativa alimenta e aggiorna il *threat model*.
Ovviamente, profilazione delle minacce e scambio di informazioni non esauriscono l'arco di attività che sottendono alla *cyber intelligence*: ragionando per macro-aree, ci si limita qui a rilevare da una parte l'*all-source intelligence* per quanto riguarda l'*information acquisition* e dall'altra l'analisi strategica, operativa e tecnico-tattica per quanto attiene all'analisi.
Il presente modello è disegnato per organizzazioni complesse, ovvero caratterizzate da una grande quantità e varietà di interdipendenze non lineari (complessità); esse si trovano immerse in un fitto reticolo iper-connesso, che interseca a più livelli diversi gangli sociali.
Il *focus* è qui posto su organizzazioni di dimensioni medio-grandi, con una proiezione su

[5] "*Information*" dal latino "*informare*" (dar forma), passando per il francese antico; "*sharing*" dall'antico inglese "*scieran*" (tagliare), di derivazione proto-germanica.

[6] Requisiti informativi che orientano le priorità nella pianificazione delle attività di *intelligence*.

scala transnazionale, che operano in settori strategici quali finanza, sanità, energia, telecomunicazioni, difesa e *intelligence*.
Tali settori e organizzazioni hanno caratteristiche che li possono far ascrivere alla categoria dei sistemi adattativi complessi (CAS).[7]

Profilazione delle minacce

Un'adeguata profilazione delle minacce non può prescindere dall'analisi dello scenario geopolitico e internazionale, specie per un'organizzazione complessa. Questo tipo di analisi, unitamente ad una attività di *all-source intelligence*, costituisce il complemento necessario all'analisi e all'investigazione tecnica degli eventi (che riguarda "il cosa" e in parte "il come" di un evento cibernetico), per indagare - e possibilmente comprendere - chi può sferrare un attacco (il chi) e per quali motivazioni (il perché). Lo stesso vale per eventi esogeni e naturali, con riguardo all'esame delle cause a monte.
L'analisi può essere condotta anche *ex post*, per capire chi e perché ha plausibilmente attaccato. Un sistema compiuto di *cyber intelligence* prevede l'impiego di analisi strategica unitamente ad analisi tecnico-tattica e operativa[8]. L'analisi strategica di *cyber intelligence* potenzia una reazione di tipo sistemico e aumenta la capacità di prevenzione.
Il *threat model* e il *cyber threat model* sono strumenti essenziali per lo svolgimento di attività di *cyber intelligence*. Tali modelli e le loro evoluzioni costituiscono, infatti, la stella polare da seguire nelle attività di prevenzione e contrasto delle minacce.
Il *threat model* rappresenta uno strumento indispensabile per l'identificazione e la definizione delle potenziali minacce e per la loro prioritizzazione; il suo aggiornamento deve tuttavia ancorarsi al concreto lavoro di indagine. L'assunto teorico che sottende alla profilazione trova validazione nella sperimentazione quotidiana sul campo, fatta di analisi e investigazione su casi concreti.
Lo sviluppo di un *threat model* deve tener conto del complesso dei *trend* in atto e della specificità della minaccia cibernetica, anche per fornire una base adeguata per la definizione di un *cyber threat model*. Entrambi questi modelli vanno continuamente aggiornati, seguendo un approccio di tipo evolutivo e adattativo verso il contesto esterno.
Il *cyber threat model* ha la funzione primaria di offrire un *benchmark* sempre aggiornato sull'evoluzione delle minacce *cyber* rilevanti per l'organizzazione: esso consente lo svolgimento di adeguate attività di *cyber intelligence*.

---

[7] La componente adattativa dei *complex adaptive systems* (CAS) risiede principalmente nella loro capacità intrinseca di mutare e auto-organizzarsi nei confronti dell'ambiente esterno. Si ipotizza che tali caratteristiche intrinseche, mutazione e auto-organizzazione, possano essere stimolate, aumentando gli effetti positivi per l'organizzazione considerata. In particolare, con mutazione ci si riferisce alla capacità di generare variazioni strutturali e modifiche funzionali; l'auto-organizzazione è da intendersi come capacità di auto-regolazione da parte degli elementi del sistema (secondo un concetto "ristretto" di neghentropia). L'obiettivo è il potenziamento della capacità di adattamento ed evoluzione per mezzo di un comportamento emergente, un'intelligenza collettiva (o *swarm intelligence*).

[8] Questo approccio mima la combinazione tra risposta immunitaria adattativa o acquisita e risposta immunitaria innata o aspecifica in ambito biologico.

Un'efficace attività di *cyber intelligence* è supportata da un continuo processo di modellizzazione delle minacce, che dipende dalla costante evoluzione di un *threat model* "aperto".
Il punto di partenza del *threat modeling* è rappresentato da una fase di immedesimazione dei potenziali aggressori e agenti di minaccia, per identificare minacce principali in base a obiettivi preferenziali e vulnerabilità dell'organizzazione di riferimento.
Come anticipato in precedenza, il modello disegnato tiene conto dei classici modelli IT di *threat modeling*, ma viene sviluppato in modo autonomo.[9]
Per quanto riguarda gli *standard* internazionali in tale ambito, si sottolinea qui la necessità di approfondire le specificità e le peculiarità di ciascuna singola organizzazione/Istituzione considerata: ancorché lo *standard* può aiutare a modellare *framework* ad ampio spettro, lo sviluppo di un modello *ad hoc* è fondamentale, se si tiene presente l'attuale scenario, caratterizzato da minacce sempre più polimorfiche, metamorfiche e soprattutto mirate.
La modellazione delle minacce può influire su diversi livelli, dal livello fisico a quello applicativo. Particolare interesse in questo campo rivestono i sistemi cyber-fisici e l'interdipendenza di presìdi di sicurezza, fisici e logici.[10]
Inoltre, la trasversalità intrinseca del dominio cibernetico e la complessità/interconnessione delle minacce rendono necessario adottare un approccio sinottico al *threat modeling*.
Conseguentemente, l'analisi si concentra su una rappresentazione di alto livello (*layer 1*) delle ontologie di minacce che possono avere impatti su attività, compiti e reputazione di un'organizzazione complessa.
La **Figura 1** mostra alcune macro-categorie, che sintetizzano una gamma molto più articolata e granulare di minacce. I fenomeni rappresentati sono direttamente o indirettamente interconnessi (collegamenti volutamente non evidenziati).
Il grafo è una raffigurazione ideale delle categorie di potenziali minacce, sottoposta a continua revisione e integrazione. L'approccio sinottico al *threat modeling* è accompagnato da un criterio evolutivo.
Senza entrare nella descrizione dettagliata della tassonomia e dei suoi sviluppi, è opportuno sottolineare la rilevanza nello scenario internazionale della minaccia ibrida: tale fenomeno – centrale nelle attuali dinamiche globali, ma con profonde radici storiche – consiste nella deliberata volontà di colpire diversi *target* (e/o perseguire fini molteplici), attraverso mezzi variegati, con l'adozione sinergica di tecniche convenzionali e non convenzionali.
Tale volontà - che può avere alla base agenti di minaccia statuali e non - determina una strategia basata su plurimi *target* (e/o scopi) e diversi mezzi di attacco.[11]

---

[9] Anche se di seguito sono rappresentati grafi e mappe mentali, questo lavoro non include *attack trees* e diagrammi di flusso utilizzati nel *threat modeling* IT.

[10] Lo sfruttamento di vulnerabilità del perimetro fisico possono rendere inefficaci i presìdi logici (e viceversa). Un evento nel dominio fisico può generare impatti sulla sicurezza del dominio logico. Inoltre, l'utilizzo di sistemi informativi è sempre più diffuso nelle attività volte a garantire la sicurezza fisica.

[11] La deliberata volontà di perseguire fini molteplici con mezzi diversi, si accompagna alla complessità e alla interdipendenza delle minacce globali; un fenomeno può avere repentine ripercussioni su altri comparti e domini, al netto della eventuale deliberata volontà

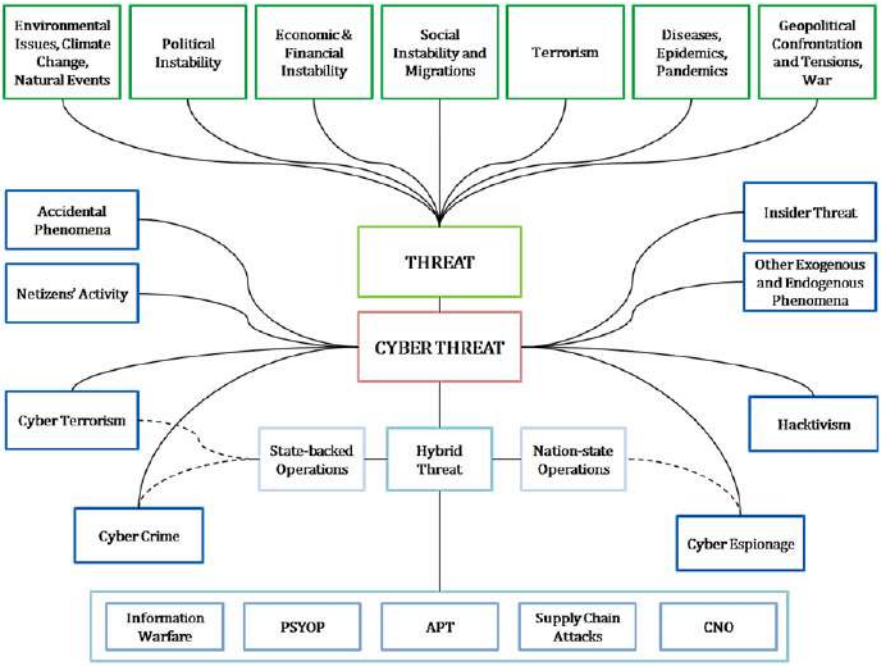


Figura 1. *Grafo sinottico - Ontologie di minacce per un'organizzazione complessa*

Nello scenario corrente, quella ibrida è da considerare tra le minacce più insidiose, poiché si basa su azioni ad ampio spettro e opera in modo spesso surrettizio. Di conseguenza, il fenomeno è difficile da rilevare, definire, attribuire e persino perseguire.
Il problema dell'attribuzione del resto domina le operazioni di uno dei vettori principali della minaccia ibrida, ovvero il dominio *cyber*: uscire dal campo della plausibilità è spesso difficile, se non si è in possesso di prove certe ("*smoking guns*"), peraltro raramente reperibili.
Nella congiuntura attuale - e ci si attende un potenziamento di questo *trend* per il futuro - la vera sfida consiste non tanto nella capacità di profilazione delle minacce, ma nella capacità di rilevazione, a fronte di sofisticate tecniche di offuscamento e anonimizzazione.
Molti attacchi e tentativi di attacco possono rimanere non rilevati o al meglio non precisamente identificati. Questo potrebbe anche falsare la quantificazione numerica dei fenomeni, evidenziando la preponderanza dei soli fenomeni con eventi rilevati (al netto di quelli rilevati e non associati ad alcuna minaccia specifica).

– statuale e non – alla base dell'evento.

Nelle pieghe di tale indeterminatezza, lo strumento *cyber* - in luogo della guerra cinetica - è uno dei mezzi di attacco privilegiato per supportare strategie ibride e il sistema economico-finanziario è uno degli ambiti di maggiore confronto. Le cosiddette operazioni sotto-soglia, unitamente a tattiche di deterrenza, sono preferite a confronti diretti e aperti, riducendo episodi di *escalation*.
Attacchi informatici contro infrastrutture critiche, APT (qui intesa come minaccia/fenomeno e non come agente), CNO, PSYOP, *information warfare*, *supply chain attacks* (sia nella forma *seeding*, sia in quella *interdiction*), costituiscono le manifestazioni superficiali di un confronto talvolta sotterraneo. La guerra economica asimmetrica è spesso parte di una più ampia campagna di guerra ibrida, combattuta simultaneamente e con una vasta gamma di strumenti, a volte molto diversi tra loro.

Al di là della causa che li ha scatenati (intenzionale o non), l'utilizzo congiunto di fenomeni - come l'instabilità sociale, le fluttuazioni finanziarie, il vettore *cyber*, l'informazione,[12] le pandemie, gli eventi naturali, le risorse energetiche, le migrazioni e altri fenomeni - per scopi di predominio geopolitico, non appartiene più soltanto alla narrativa propagandistica di alcuni Stati o alla letteratura di qualche analista di *intelligence*.
Quanto agli agenti di minaccia sottesi alle macro-categorie rappresentate, si opera di seguito una semplificazione tassonomica (e come tale, non esaustiva e perfettibile). Una dicotomia a monte può partire dalla separazione tra possibili aggressori ed eventi naturali/esogeni.

La granularità può seguire ulteriori ramificazioni per ogni categoria, ma le principali classi rilevate sono: Stati (Stati nazionali, *intelligence*, forze armate e altri apparati governativi; APT intese qui anche come entità attaccanti); *netizen* (persone, macchine e BOT che attraverso la rete compromettono sistemi informatici); *cyber* criminali (persone affiliate a organizzazioni criminali, che utilizzano il dominio *cyber* perpetrando reati); *hacktivisti* (persone che attaccano siti web o entrano illegalmente in sistemi e infrastrutture informatici di terzi, a fini politici e di protesta, azioni dimostrative etc.); *cyber* terroristi (persone che organizzano e/o commettono azioni con conseguenze violente ed eventuali feriti/vittime, per scopi ideologici, religiosi, politici, mediante sistemi e infrastrutture informatiche[13]); dipendenti e talpe[14] (persone che lavorano per l'organizzazione o che entrano in contatto con l'organizzazione per esfiltrare informazioni); eventi naturali ed esogeni (disastri naturali, incendi, malattie, pandemie, etc.).
L'implementazione del modello e lo sviluppo del *layer 2* - la fase che attiene alla definizione di *priority intelligence requirements* (PIR), al *reverse targeting* e alla individuazione dei reali

[12] La guerra nel campo dell'informazione e della comunicazione è uno strumento ortogonale rispetto a tutte le altre leve: riveste centralità, su più livelli, nel confronto nazionale e internazionale.

[13] Non esiste una definizione ampiamente condivisa e codificata di ciò che si intende per *cyber* terrorista, a causa del concetto asimmetrico e talvolta ibrido del fenomeno.

[14] Questi agenti possono coincidere, ma una talpa può essere anche un lavoratore esterno, un consulente o un visitatore.

agenti di minaccia – avviene attraverso la valorizzazione di una *threat matrix*, da sviluppare in base alle caratteristiche dell'organizzazione considerata.
Prima di procedere alla valorizzazione di una *threat matrix*, occorre però fare una analisi preliminare per ognuna delle macro-categorie di minaccia individuate (quelle rappresentate in **Figura 1**).
Per un'Istituzione finanziaria, ad esempio, prima di individuare le minacce specifiche, in base ai propri *asset* e alle proprie vulnerabilità, si identificheranno gli APT più attivi a livello globale e le principali galassie criminali attive nel settore finanziario (**Figure 2** e **3**).

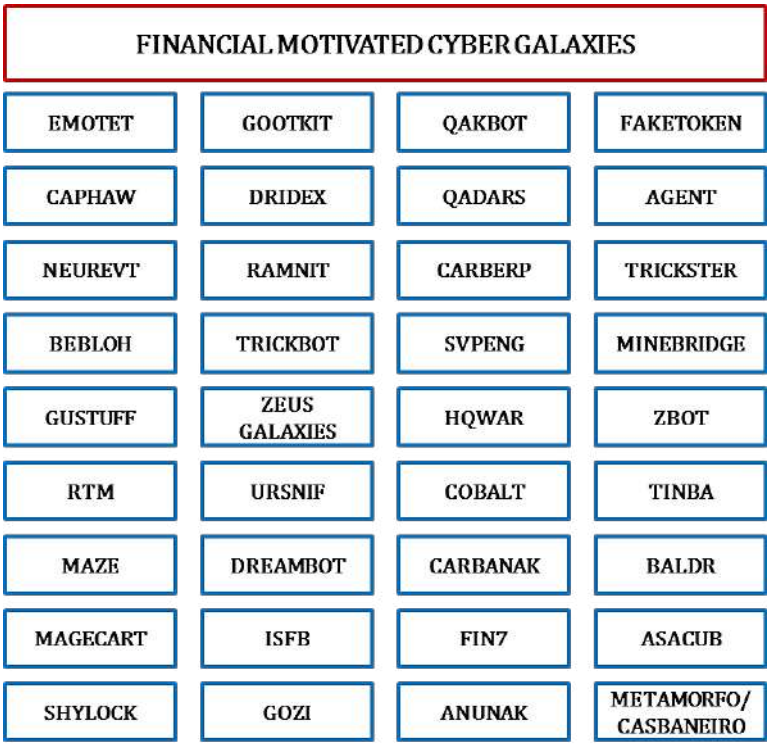
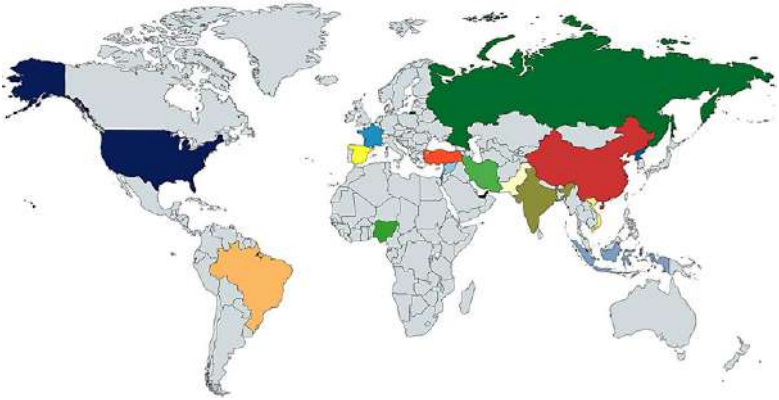


Figura 2. *Analisi propedeutica alla valorizzazione della threat matrix per macro-categoria minaccia Cyber Crime – Financial Motivated Cyber Galaxies*



CHINA: APT 1 (SEA SALT, COMMENT CREW), APT 3, APT 10 (Stone Panda, MenuPass, Red Apollo), APT 12, APT 15 (Vixen Panda, Ke3Chang, GREF, Playful Dragon), APT 16, APT 17 (Deputy Dog, Axiom, BARIUM, Winnti, ShadowHammer, ShadowPad, Wicked Panda), APT 18 (Wekby), APT 19 (Codoso Team), APT 22, APT 27 (EMISSARY PANDA, LUCKY MOUSE), APT 30, APT31 (Zirconium), APT 40 (Leviathan), APT 41, Stalker Panda, Mofang, Iron Tiger, TA428, Thrip (Billbug, Lotus Blossom), Mustang Panda. PKPLUG, TURBINE PANDA, BRONZE PRESIDENT

BRAZIL: GHOST DNS, POSEIDON, TEAMXRAT (CORPORACAOXRAT), Metamorfo (Casbaneiro)

FRANCE: SNOWGLOBE (ANIMAL FARM)

INDIA: SIDEWINDER, DROPPING ELEPHANT (PATCHWORK, DONOT, APT-C-35), Bitter

IRAN: APT 33 (Elfin, Holmium, MAGNIALLIUM), APT 34 (OilRig, Crambus), APT 35 (Newscaster, NewsBeef, Charming Kitten, Imperial Kitten), Leafminer, Greenbug, Muddywater (Seedworm, Static Kitten), ROCKET KITTEN, INFY, APT39 (Chafer), Bahamut (WINDSHIFT)

INDONESIA: DevilScreaM (Indonesian Cyber Army)

ISRAEL: DUQU, DUQU 2.0

LEBANON: DARK CARACAL

NIGERIA: SILVER TERRIER (Sweed)

NORTH KOREA: HIDDEN COBRA, LAZARUS, APT 37, APT 38, Konni Group, CARROTTBALL, KIMSUKY, ScarCruft, HOPLIGHT

PAKISTAN: OPERATION C-MAJOR, MYTHIC LEOPARD, BARMANOU

PALESTINIAN TERRITORIES: Gaza Cybergang, Molerats

RUSSIA: GRIZZLY STEPPE, APT 28 (SOFACY, FANCY BEAR, TSAR TEAM, PAWN STORM, SEDNIT, THREAT GROUP-4127, IRON TWILIGHT, STRONTIUM), APT 29 (Cozy Bear), SANDWORM, BLACK ENERGY, GREY ENERGY, ENERGETIC BEAR, CROUCHING YETI, RED OCTOBER, WebCobra, Silence, MoneyTaker, TURLA GROUP (Waterbug), SNAKE, Gamaredon

SPAIN: Careto/Mask

SOUTH KOREA: Higaisa

SYRIA: APT – C – 27, Deadeye Jackal, SEA

TURKEY: Ayyildiz Tim, Aslan Neferler Tim (Lion Soldiers Team)

UNITED ARAB EMIRATES: STEALTH FALCON

USA: EQUATION GROUP

VIETNAM: APT 32 (Ocean Lotus)

Figura 3. *Analisi propedeutica alla valorizzazione della threat matrix per macro-categoria minaccia Hybrid Threat – APT globali (attribuzioni ritenute maggiormente plausibili)*

L'information sharing

L'*information sharing* (anche *infosharing* o *info-sharing*) o *information exchange* indica scambio/condivisione di informazioni. Con riguardo alle attività di *cyber intelligence*, tale condivisione – che avviene solitamente tra CERT o CSIRT[15] – consiste nello scambiare dati grezzi, informazioni e analisi riguardanti le minacce cibernetiche.

L'*infosharing* può avvenire in base a diversi *pattern*, quali *one-to-one*, *one-to-many* (*hub-spoke*), *many-to-one*, *many-to-many*.

Al fine di regolare in modo omogeneo il grado di diffusione delle informazioni scambiate, è bene attenersi a specifico protocollo (stabilito da parte terza), che delimiti il perimetro entro il quale è possibile condividere. Questo approccio garantisce un *level playing field* tra le parti contraenti.

In tale ambito, si fa generalmente ricorso al TLP (*traffic light protocol*), che definisce il grado di possibile diffusione (*red*, *amber*, *green*, *white*) stabilito dalla controparte inviante.

Ciò non si sostituisce alle *policy* riguardanti il grado di riservatezza da attribuire alle informazioni, definite sia a livello di singola organizzazione, sia a livello nazionale.

La gestione delle fonti (intese qui come controparti) e delle informazioni sono attività continuative che supportano il processo di *infosharing*.

In particolare, il *source management* per l'*infosharing* contribuisce a fornire gli strumenti necessari per individuare e prioritizzare il novero delle controparti in grado scambiare informazioni rilevanti e utili per l'organizzazione.

A tal proposito, anche realtà con un bacino informativo più limitato, potrebbero avere, in un preciso momento, un dato o una informazione che può rivelarsi vitale per la propria organizzazione. Questo fa preferire in generale un approccio tendente alla simmetria regolatoria (con accordi *peer-to peer* e protocolli di terza parte, fatta salva la normativa nazionale e transnazionale rilevante).

Anche l'appartenenza al medesimo settore non è un vincolo per l'*infosharing*: considerato il complesso quadro di minacce suesposto, uno scambio di informazioni inter-settoriale appare non soltanto utile, ma necessario.

Quanto all'oggetto dello scambio informativo, i CERT o i CSIRT condividono IOC, CVE, artefatti, indirizzi IP, TTPs, informazioni su attori e attribuzioni di attacchi.

Lo scambio può avvenire attraverso piattaforme tecnologiche,[16] siano esse *open source* o proprietarie, per mezzo di *threat intelligence platform*, email crittografate, riunioni di presenza, *conference call* etc.[17] Con riguardo ai mezzi impiegati, occorre prediligere un approccio tecnologicamente neutrale, tenendo sempre presente che il fine ultimo è l'acquisizione di informazioni utili alla produzione di *actionable intelligence*. Occorre insomma non con-

[15] I CERT o CSIRT possono essere accreditati nell'ambito di consessi e circuiti sovranazionali come FIRST e *Trusted Introducer*.

[16] In Italia, si segnala l'iniziativa di CERT-PA, sotto la supervisione del Nucleo per la Sicurezza Cibernetica, di fornire una piattaforma di *information sharing* in materia di CTI.

[17] Tra i protocolli attualmente più utilizzati figurano STIX, TAXXI. Per la descrizione delle famiglie dei *malware* si utilizzano correntemente le cosiddette *Yara Rules*, che consistono in stringhe ed espressioni booleane.

fondere il mezzo col fine.
Il valore delle attività di *infosharing* è strettamente legato alla qualità di ciò che viene condiviso: le informazioni scambiate possono risultare incomplete e/o eterogenee. L'eterogeneità può riguardare sia la forma sia il contenuto. Nel primo caso, vi è la necessità di una sistematica attività di normalizzazione delle informazioni, nel secondo occorre applicare un attento processo di validazione.
Il filtraggio e la validazione delle informazioni in ingresso sono tanto più importanti, quanto più ci si muove dall'ambito tecnico-tattico verso quello strategico.
A fronte di un'ingente mole di dati e indicatori e nell'oggettiva impossibilità di rinvenire prove certe, l'analista può essere spesso indotto ad avallare in modo meccanico un'errata attribuzione di terza parte considerata autorevole[18] e trasfonderla in piattaforme, che automatizzano e amplificano esponenzialmente l'errore a monte, con effetto a catena. Dovrebbe essere evitato il rimbalzo di analisi di terze parti, senza valutazione e verifica. È sempre da preferire un'analisi strategica interna (corredata da analisi di contesto e SAT) sulle informazioni ricevute: in questo modo, si possono disinnescare eventuali *bias* cognitivi e interferenze geopolitiche dell'analisi a monte. Anche l'analisi di tipo tecnico-tattica dovrebbe prevedere una fase di *intelligence* sugli indicatori: la valorizzazione del contenuto informativo, attraverso correlazione e contestualizzazione, riduce il rischio di uno scambio sterile.
Nell'*infosharing*, si possono presentare fenomeni di non completa condivisione. La scarsa propensione a condividere informazioni, sia nel comparto pubblico sia in quello privato, trae origine da motivazioni di varia natura, siano esse legate alla strategia dell'organizzazione, alla riservatezza e segretezza, alla volontà di non pubblicizzare proprie vulnerabilità o mancanze. A questo, si può aggiungere la difformità o disomogeneità nei mezzi, protocolli e infrastrutture per lo scambio informativo tra le controparti.
Specie per lo scambio di informazioni particolarmente riservate - con agenzie di *intelligence*, *law enforcement*, altre Istituzioni o aziende private - è preferibile la stipula di convenzioni operative, del tipo *peer-to-peer* tra CERT e omologhi (unità tecniche); tali convenzioni potrebbero prevedere eventuali adeguamenti infrastrutturali (es. reti separate, criptate etc.) su richiesta delle controparti.

[18] Posta l'autorevolezza della terza parte, non si dovrebbe dare automaticamente per scontata l'attendibilità dell'attribuzione.

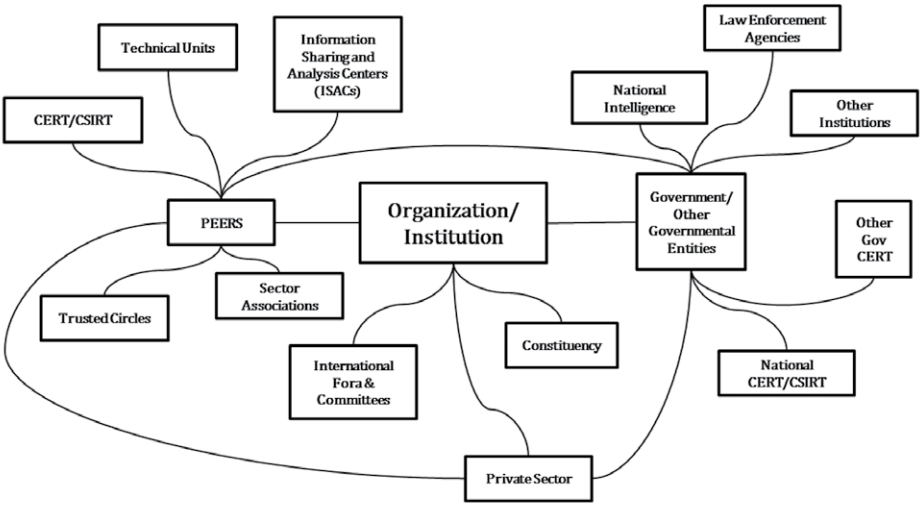


Figura 4. *Controparti supra system per un'organizzazione complessa*

In questo ambito, l'obiettivo principale per una organizzazione complessa è la creazione di una rete di reti informative, un "sovra-sistema"[19] per lo scambio di informazioni (**Figura 4**). L'importanza della cooperazione nell'*infosharing*, per l'intero Sistema-Paese, risiede nella maggiore capacità di prevenzione e contrasto derivante da una accresciuta conoscenza collettiva. Il richiamato sovra-sistema mira a potenziare una stretta collaborazione tra agenzie di *law enforcement*, *intelligence*, istituzioni pubbliche e comparto privato. Il fine principale è evitare sistemi sconnessi e compartimenti stagni promuovendo un'impostazione *win-win*, pur tenendo presente che nello scambio è sovente invalso l'approccio del *do ut des*.

Conclusioni

La profilazione delle minacce e lo scambio di informazioni sono azioni essenziali per l'efficace svolgimento di attività di *cyber intelligence*.
È fondamentale potenziare strumenti idonei per individuare le minacce che possono avere impatti su patrimonio, compiti e reputazione di un'organizzazione complessa. In questo frangente, la fase di profilazione è supportata da analisi strategica, geopolitica e di contesto, per comprendere i reali agenti di minaccia e le reali motivazioni alla base dei fenomeni.

[19] Su questi concetti, si veda "*Development of a cyber threat intelligence apparatus in a central bank*" di Pasquale Digregorio e Boris Giannetto – Banca d'Italia – 2019.

La modellazione delle minacce deve seguire un approccio adattativo ed evolutivo, stimolando *driver* quali mutazione e auto-organizzazione.
Elemento basilare nelle attività di *cyber intelligence* è anche l'*information sharing*: occorre promuovere uno scambio informativo allargato, per accrescere il grado di conoscenza collettiva della minaccia e per aumentare la capacità sistemica di prevenzione e contrasto.

Bibliografia

- ARTIFICIAL SWARM INTELLIGENCE IN THE CONTEXT OF SINGULARITY - Thomas Caldwell – 2020
- THE GLOBAL RISKS REPORT 2020 - World Economic Forum – 2020
- RELAZIONE SULLA POLITICA DELL'INFORMAZIONE PER LA SICUREZZA relativa ad anni 2018 e 2019 – Dipartimento delle Informazioni per la Sicurezza (DIS) – 2019 e 2020
- UNCOVERING THE SOCIAL INTERACTION IN SWARM INTELLIGENCE WITH NETWORK SCIENCE - M. Oliveira, D. Pinheiro, M. Macedo, C. Bastos-Filho, R. Menezes - 2019
- A THREAT-DRIVEN APPROACH TO CYBER SECURITY - Michael Muckin, Scott C. Fitch - Lockheed Martin Corporation - 2019
- DEVELOPMENT OF A CYBER THREAT INTELLIGENCE APPARATUS IN A CENTRAL BANK - Pasquale Digregorio, Boris Giannetto – Banca d'Italia – 2019
- INFORMATION SHARING IN CYBERSECURITY: A REVIEW - Ali Pala, Jun Zhuang - University at Buffalo, Buffalo, New York – 2019
- ADDRESSING HYBRID THREATS - Gregory F. Treverton, Andrew Thvedt, Alicia R. Chen, Kathy Lee, and Madeline McCue – SDU, CATS, CoE - 2018
- GOING BEYOND RESILIENCE, A REVITALIZED APPROACH TO COUNTERING HYBRID THREATS - Heine Sørensen, Dorthe Bach Nyemann – Hybrid CoE – 2018
- POST-EVENT ANALYSIS OF THE HYBRID THREAT SECURITY ENVIRONMENT: ASSESSMENT OF INFLUENCE COMMUNICATION OPERATIONS - Rubén Arcos – Hybrid CoE – 2018
- THREAT MODELING: A SUMMARY OF AVAILABLE METHODS - Nataliya Shevchenko, Timothy A. Chick, Paige O'Riordan, Thomas Patrick Scanlon - PhD, & Carol Woody, PhD - 2018
- A HYBRID THREAT MODELING METHOD - Nancy R. Mead, Forrest Shull, Krishnamurthy Vemuru, Ole Villadsen - Carnegie Mellon University - 2018
- CYBER THREAT INTELLIGENCE MODEL: AN EVALUATION OF TAXONOMIES, SHARING STANDARDS, AND ONTOLOGIES WITHIN CYBER THREAT INTELLIGENCE - Vasileios Mavroeidi, Siri Bromander, University of Oslo - 2018

- CYBER THREAT MODELING: SURVEY, ASSESSMENT, AND REPRESENTATIVE FRAMEWORK - Deborah J. Bodeau, Catherine D. McCollum, David B. Fox – 2018
- CYBER THREAT INTELLIGENCE INFORMATION SHARING - Edilson Arenas - Central Queensland University - 2017
- BUILDING A NATIONAL CYBER INFORMATION-SHARING ECOSYSTEM - Bruce J. Bakis, Edward D. Wang – MITRE - 2017
- STRATEGIC ASPECTS OF CYBERATTACK, ATTRIBUTION, AND BLAME - Benjamin Edwards, Alexander Furnas, Stephanie Forrest, and Robert Axelrod - 2017
- CYBER DEFENSE AS A COMPLEX ADAPTIVE SYSTEM: A MODEL-BASED APPROACH TO STRATEGIC POLICY DESIGN - Michael D. Norman, Matthew T. K. Koehler – 2017
- ATTRIBUTING CYBER ATTACKS - Prof. Thomas Rid & PhD. Ben Buchanan - 2015
- QUANTUM MIND AND SOCIAL SCIENCE, UNIFYING PHYSICAL AND SOCIAL ONTOLOGY – Alexander Wendt – Cambridge - 2015
- ADVANCES IN THREAT AND RISK MODELING - Gerald Beuchelt, Vijay Mehra - #ISC2Congress. Strengthening Cybersecurity Defenders – 2014
- CYBERSPACE: THE ULTIMATE COMPLEX ADAPTIVE SYSTEM – Ph.D. Paul W. Phister Jr. – C2 Journal – 2010
- EFFECTIVE LEADERSHIP AND DECISION-MAKING IN ANIMAL GROUPS ON THE MOVE - Iain D. Couzin, Jens Krause, Nigel R. Franks & Simon A. Levin - 2005
- STUDYING COMPLEX ADAPTIVE SYSTEMS – Prof. John H. Holland - 2005
- ANT COLONY OPTIMIZATION THEORY: A SURVEY - in Theoretical Computer Science - Prof. Marco Dorigo, Christian Blum – 2005
- FROM SWARM INTELLIGENCE TO SWARM ROBOTICS – in Lecture Notes in Computer Science – Prof. Gerardo Beni - 2004
- COMPLEXITY AND EMERGENT BEHAVIOUR IN ICT SYSTEMS - Seth Bullock, Dave Cliff – HP – 2004
- COMPLEX ADAPTIVE SYSTEMS AND COMPLEXITY THEORY: INTER-RELATED KNOWLEDGE DOMAINS - Rebecca Dodder, Robert Dare – MIT - 2000
- EVOLUTIONARY COMPUTATION: AN OVERVIEW – Melanie Mitchell, Charles E. Taylor, Santa Fe Institute - 1999

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

A livello globale le imprese stanno cambiando. Qualsiasi impresa è ormai impegnata in percorsi di trasformazione digitale e in progetti innovativi che stanno impattando in maniera rilevante le strategie di business, i processi e i sistemi interni, le competenze, i prodotti e i servizi. Ormai da anni le reti e le infrastrutture aziendali si confrontano con nuove tecnologie e innovazioni esogene ed eterogenee di qualsiasi tipo, dai dispositivi mobili agli oggetti connessi, dai servizi cloud ai dati e alle tecnologie di terze parti. Ai sistemi aziendali accedono risorse e tecnologie sia dall'interno che dall'esterno del perimetro aziendale, in misura così pervasiva e sistematica che è corretto riconoscere l'IT come una infrastruttura sempre più organica e senza soluzione di continuità tra qualsiasi organizzazione e il suo ambiente circostante. Queste dinamiche contribuiscono a rafforzare il ruolo della Sicurezza IT in cima alle priorità strategiche delle imprese, che sono chiamate a proteggere e valorizzare un patrimonio di dati e informazioni sempre più ingovernabile.

L'approccio alla Sicurezza IT richiede un atteggiamento proattivo e una grande consapevolezza da parte delle aziende, con strategie di investimento capaci di mirare con consapevolezza a una ragionevole mitigazione del rischio IT nella relazione con dipendenti, clienti e partner. Come le imprese, allo stesso modo i governi stanno aumentando l'attenzione alla tematica, soprattutto nella consapevolezza che la tutela della sicurezza sta diventando un rischio sistemico che richiede interventi e regolamentazioni a livello di sistemi paese per tutelare la fiducia del mercato, la privacy dei cittadini, gli interessi e la sovranità nazionale. In considerazione di queste tendenze di fondo, a livello internazionale IDC osserva alcune dinamiche che nei prossimi anni avranno un considerevole impatto sulle imprese e sui cittadini, che dovranno confrontarsi con strategie e tecnologie sempre più sofisticate.

Lo "skill shortage" continuerà a rimanere una tematica critica, soprattutto in un contesto in cui le competenze degli specialisti della Sicurezza vanno ulteriormente approfondendosi: sarà sempre più importante disporre di analisti con competenze anche nelle aree del machine learning, in considerazione del peso sempre maggiore che l'Intelligenza Artificiale giocherà nel monitoraggio, nella detection e nella gestione di eventuali incidenti. La varietà e i volumi degli alert cresceranno in maniera esponenziale e soltanto questi strumenti potranno aiutare le aziende a gestire situazioni anomale, ricorrendo a molteplici fonti per disegnare regole e profili di rischio basati su comportamenti complessi.

La progressiva digitalizzazione delle aziende e la continua integrazione dell'IT con le tecnologie della produzione rappresenteranno per molti anni una opportunità di crescita per la Sicurezza IT. Come è ben noto, le minacce verso la produzione, soprattutto negli scenari IoT, sono numerose e in continua crescita. Secondo IDC, entro il 2024 – con nuovi stru-

menti per la visibilità sulle Operational Technologies, il 60% delle aziende manifatturiere globali opterà per un approccio integrato OT/ IT per la gestione della Sicurezza. Oltre a beni e servizi materiali, le Smart Factories produrranno una quantità sempre maggiore di dati gestiti nei sistemi Edge: la gestione dei rischi IT connessi alle operazioni diventerà un fattore essenziale per garantire la continuità delle operazioni aziendali e mantenere la capacità competitiva dei settori nel nuovo millennio.

Un'altra tendenza caratterizzante nei prossimi anni è il rinnovamento della Sicurezza come strumento per gestire e alimentare il Digital Trust. Sempre più spesso le imprese si impegneranno nella definizione di programmi e di framework capaci di costruire un rapporto nuovo con clienti e partner basato su affidabilità sia organizzativa che tecnologica nella gestione delle transazioni B2B e B2C e in questa sfida si aprirà uno spazio per l'affermazione di un ruolo sempre più importante della Sicurezza IT come infrastruttura essenziale per la Digital Economy. Secondo IDC, entro il 2025 il 25% della spesa in servizi di sicurezza sarà destinata allo sviluppo, all'implementazione e al mantenimento di un "trust framework". Non si tratterà soltanto di una sfida tecnologica: oltre alla Sicurezza IT, sarà necessario adottare una strategia che prevede interventi organizzativi in grado di trasformare processi e gestire il cambiamento, in un contesto dominato da una elevata interdipendenza tra funzioni e organizzazioni, sia interne che esterne.

Nei prossimi anni le imprese saranno sempre più impegnate a trovare un equilibrio virtuoso tra la qualità dell'esperienza digitale e i requisiti sempre più stringenti di controllo e sicurezza. L'obiettivo di garantire elevati livelli di fluidità dell'esperienza digitale, da un lato, e la necessità di provvedere opzioni di autenticazioni sempre più veloci, semplici e naturali, dall'altro, comporterà l'investimento in soluzioni e tecnologie innovative per la gestione dell'identità digitale. IDC prevede che entro il 2022 il 35% delle transazioni a livello globale avverrà attraverso sistemi di autenticazione che salvaguarderanno la qualità della "digital experience" ricorrendo a tecnologie di autenticazione che spazieranno ampiamente su tecnologie biometriche.

Si conclude questa breve introduzione con un'ultima tendenza che nel medio termine guiderà gli investimenti nella Sicurezza IT: la proliferazione di sistemi distribuiti di Edge Computing in qualsiasi ambito, dal commercio alla finanza fino al settore industriale. Secondo IDC, entro il 2025, per gestire l'esplosione del volume di dati sensibili derivanti dal "digital footprint" degli utenti, il 25% dei dati delle imprese risiederà in sistemi distribuiti per garantire una maggiore tutela e protezione dei dati personali, dei contatti commerciali e dei segreti industriali. L'analisi e la gestione dei dati all'estrema periferia delle reti attraverso sistemi di Edge Computing sarà una strategia efficace per proteggere le informazioni aziendali, per proteggere i dati sensibili da accessi indesiderati e garantire una corretta gestione delle informazioni anche in termini di data lineage, attestando l'origine e l'integrità dei dati su cui prendono vita le strategie aziendali.

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 derivano 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 oltre 400 milioni di euro nel 2019 (**Fig. 1**). Con un $CAGR_{2019\text{-}2022}$ di sette punti percentuali, le prospettive di crescita a breve rimangono sostanzialmente inalterate rispetto allo scorso anno, alcuni segmenti (come Security & Vulnerability Management e Network Security) continuano a trainare la crescita del comparto, in alcuni casi con tassi di crescita fino al dieci percento. L'integrazione del Machine Learning per la gestione delle vulnerabilità aziendali consentirà di sostenere in modo strutturale la crescita di questo comparto nel medio-lungo termine (in modo particolare, si pensa a modalità di integrazione sempre più evoluta tra applicazioni e processi che andranno a realizzare concretamente modalità di Augmented Security nelle imprese).

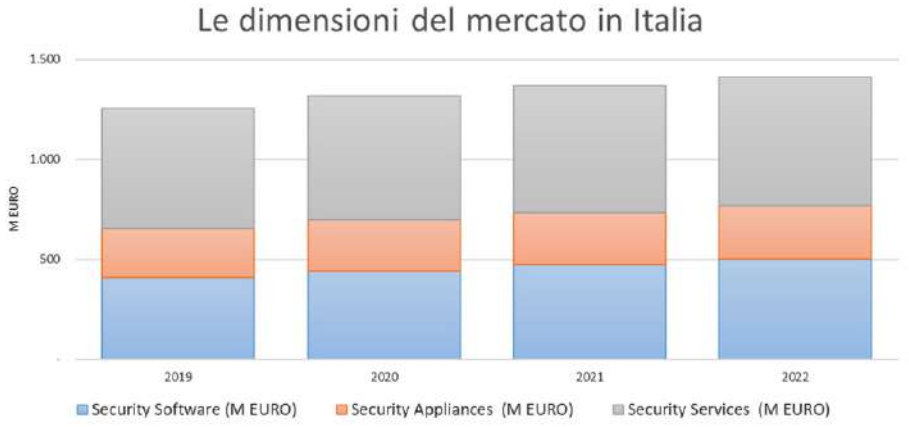


Figura 1 - *La Sicurezza IT, i principali segmenti del mercato italiano (Software, Appliance e Servizi). Fonte: IDC Italia, 2019*

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 240 milioni di euro (**Fig. 1**). Con un $CAGR_{2019\text{-}2022}$ stimato in circa tre punti percentuali, IDC continua a ridimensionare le sue stime di medio termine: la maggiore intensità di crescita nell'orizzonte previsionale considerato è riconducibile all'area UTM, nell'ambito della quale si prevede un tasso di crescita di medio termine ancora positivo.
I Servizi per la Sicurezza IT rappresentano il segmento caratterizzato dalla maggiore dinamicità degli operatori, con un grande impulso verso lo sviluppo di servizi innovativi per soddisfare le esigenze sempre più complesse del mercato. Proponendo una tassonomia neutrale rispetto al mercato, IDC stima la dimensione del comparto in base alla ripartizione generale tra servizi riconducibili all'area dell'IT Consulting e servizi riconducibili nell'ambito della System Integration/ Implementation. Con un $CAGR_{2019\text{-}2022}$ attorno ai due punti percentuali, in sostanziale continuità rispetto alle previsioni dello scorso anno, i servizi hanno un valore che si attesta attorno a 600 milioni di euro nel 2019.

Opportunità e sfide per le imprese italiane

Nella sezione seguente verranno evidenziati i risultati provenienti da alcune indagini condotte da IDC nel mercato italiano che hanno coinvolto centinaia di Medie e Grandi Imprese con una ampia rappresentazione della struttura industriale del Paese (dal manifatturiero ai servizi, dal commercio alla pubblica amministrazione, dalle utilities fino ai trasporti e alle comunicazioni). Gli studi hanno 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 modelli tecnologico-organizzativi (dalla Trasformazione Digitale all'IoT/ Edge all'Intelligenza Artificiale).

Le indagini hanno coinvolto sia le figure apicali dell'IT aziendale (CIO/ Directors/ etc.), sia figure più specializzate che danno centralità alla Sicurezza IT in azienda (Chief Information Security Officer/ IT Security Manager/ etc.), sia figure di middle management più generaliste rispetto alle quali la Sicurezza IT rappresenta un compito collaterale comunque imprescindibile (IT Manager/ Responsabili IT/ etc.). Laddove possibile, il dato campionario è stato estrapolato all'universo delle Medie e Grandi Imprese in base a modello territoriale IDC basato su dati ISTAT così da portare una rappresentazione integrale del fenomeno della Sicurezza IT rispetto alle dimensioni effettive del mercato italiano.

Il ruolo della Sicurezza IT e le esigenze emergenti

La sicurezza si conferma tra le principali priorità tecnologiche delle aziende italiane, soprattutto per le organizzazioni di maggiori dimensioni che anche nel 2020 saranno impegnate su progetti di miglioramento della sicurezza dei sistemi e delle infrastrutture IT. La cybersecurity è centrale nei programmi di investimento delle imprese italiane, in particolar modo per il settore manifatturiero, che a differenze di altri comparti ad alta intensità di informazione,

come il Finance o la Pubblica Amministrazione, soltanto in questi ultimi anni hanno cominciato a comprendere il potenziale valore strategico degli investimenti nella Sicurezza IT per affrontare le nuove sfide dell'Industria 4.0 e dell'Intelligenza Artificiale.

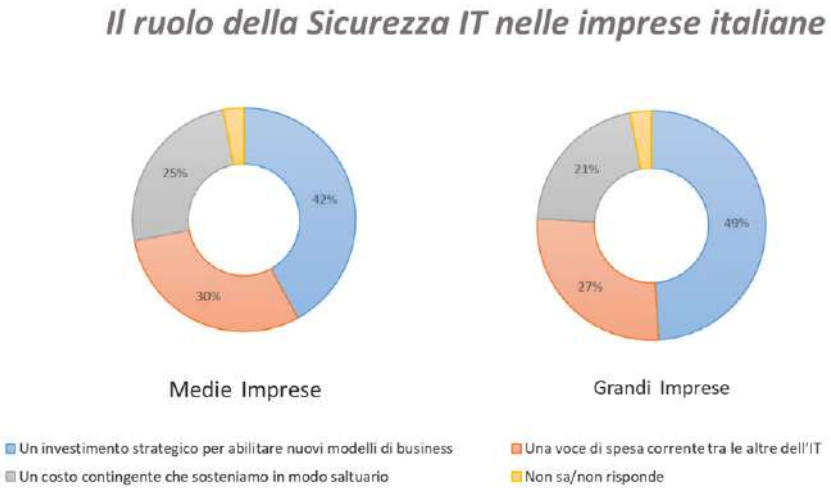


Figura 2 - *Il ruolo della Sicurezza nel Budget IT. Fonte: Survey IDC Italia, 2019 (n=400 – imprese con oltre 50 addetti).*

Le imprese di maggiori dimensioni molto spesso hanno definito una chiara strategia nell'ambito della Sicurezza IT, mentre le medie imprese, anche quelle che prestano grande attenzione al tema del rischio IT, di solito riconoscono la necessità di colmare alcune lacune. La Sicurezza IT rappresenta un investimento strategico per abilitare nuovi modelli di business per il 42% delle Medie Imprese e per circa il 50% delle Grandi imprese (**Fig. 2**), con declinazioni differenti a seconda del settore di riferimento e della specifica vocazione del core business alla gestione del dato. Nonostante queste dinamiche, risulta ancora allarmante il divario con una parte importante del mercato italiano: circa il 25% delle Medie Imprese e il 21% delle Grandi considera la spesa in Sicurezza IT un costo contingente del tutto saltuario, evidenziando una distanza abissale rispetto ai temi del cyberwarfare, della concorrenza sleale attraverso gli strumenti digitali e del rischio IT come rischio sistemico generale.

Sebbene l'ottimizzazione e la sicurezza delle infrastrutture IT rimangano tra le principali priorità dell'IT aziendale, persiste tuttavia ancora un certo "effetto dimensionale" che comporta l'espressione di una declinazione piuttosto articolata di questa sensibilità a seconda del grado di strutturazione organizzativa. Nelle aziende di minori dimensioni prevale un fattore culturale che sottovaluta l'importanza della Sicurezza come abilitatore di nuovi modelli di business nel digitale: questo è un fattore che incide in misura sostanziale su qualsiasi po-

tenziale intervento organizzativo per mitigare il rischio IT, ancor più della carenza di risorse da investire nello stato dell'arte della tecnologia.

Il ruolo sempre più pervasivo che l'IT sta assumendo, non soltanto nella gestione dei servizi e nelle modalità di relazione con il mercato, ma nella stessa organizzazione delle operazioni aziendali, sta rapidamente riducendo il divario di sensibilità tra Medie e Grandi Imprese: la progressiva convergenza tra OT/ IT all'interno delle aziende di qualsiasi settore e dimensione sta rifocalizzando l'attenzione delle imprese verso la necessità di proteggere apparecchiature e macchinari ben al di là della tradizionale sicurezza fisica, salvaguardando la produzione aziendale da rischi esogeni del tutto imprevedibili.

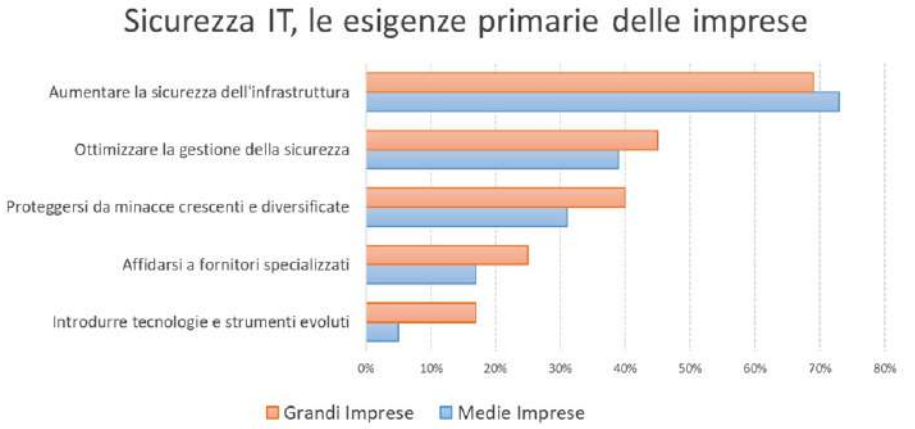


Figura 3 - *Sicurezza IT, le esigenze primarie delle aziende italiane.*
Fonte: Survey IDC Italia, 2019 (dato campionario, n=400 – imprese con oltre 50 addetti).

Con la progressiva connessione in rete di macchinari e strumenti di produzione, il rischio IT assume una valenza sistemica, con potenziali ripercussioni che si estendono dalla sicurezza fisica dei dipendenti alle attività produttive, alla qualità dei beni prodotti e ai livelli di servizio erogati. Diventa prioritario proteggere i dati della produzione perché esprimono una parte della proprietà intellettuale e degli onerosi investimenti in ricerca e sviluppo, soprattutto quando la supply chain diventa sempre più frammentata a livello internazionale. In uno scenario di connessione sempre più capillare e pervasiva, con oggetti intelligenti che partecipano in vario modo alle diverse fasi della produzione, gli "entry point" di potenziali minacce esterne si moltiplicano in misura esponenziale.
L'attenzione rispetto alle molteplici e multiformi manifestazioni del rischio IT (**Fig. 4**) trova una sua focalizzazione primaria nella privacy e nella gestione dei dati personali e nella possibile diffusione non autorizzata di informazioni commerciali. Il vigoroso impulso normativo degli ultimi anni ha ravvivato il timore dei data breach in azienda, con la compromissione

della riservatezza, dell'integrità e della disponibilità dei dati di clienti, dipendenti, partner, oppure la possibile diffusione di informazioni commerciali sensibili che potrebbero compromettere la competitività dell'azienda. Un ulteriore rischio che allarma le imprese italiane è l'interruzione dell'operatività aziendale: le imprese temono attacchi devastanti capaci di interrompere il flusso normale della produzione, con impatti negativi non soltanto sui risultati economici immediati, ma sulla reputazione aziendale e sulle relazioni consolidate con clienti e stakeholder di qualsiasi tipo. La capacità di reagire con la massima prontezza ad attacchi DDoS richiede la predisposizione di una strategia chiara e ben definita per non rischiare di aggravare la situazione con risposte irresolute e tardive.

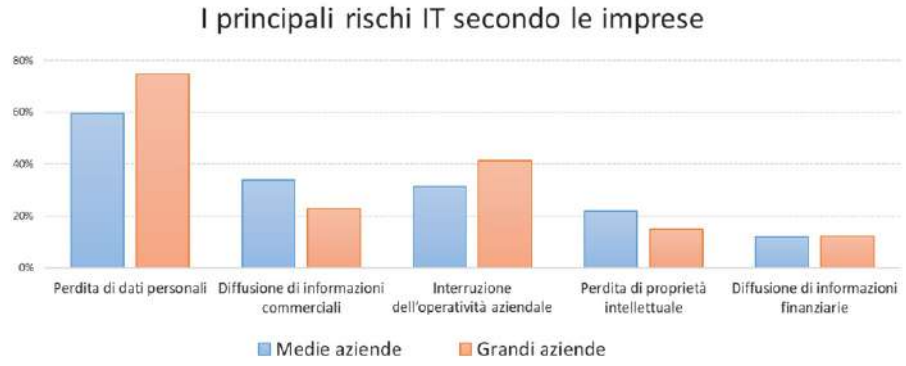


Figura 4 - *I principali rischi in caso di attacco informatico.*
Fonte: Survey IDC Italia, 2019 (n = 400, imprese con oltre 50 addetti).

Gli imprenditori avvertono ancora numerose sfide aperte per rafforzare i profili di rischio delle imprese italiane nei mercati digitali, soprattutto quando il tema è la capacità di affrontare le minacce del cybercrime e del cyber-warfare. Circa il 30% delle imprese mette in evidenza la carenza di risorse finanziare da destinare a investimenti in tecnologia e formazione. La moltiplicazione dei vettori di attacco e la costante rincorsa tecnologica tra black-hat e white-hat richiedono budget sempre più impegnativi per migliorare la cultura aziendale della sicurezza, per incrementare l'awareness dei dipendenti e rafforzare la resilienza digitale dell'organizzazione rispetto al rischio IT.
Una ulteriore difficoltà, ormai endemica: la carenza di competenze adeguate alla gestione della Sicurezza IT in azienda. Se la formazione interna del personale è un aspetto fondamentale, un aspetto forse ancora più importante è l'accesso a opportune competenze per sviluppare e operare con tecnologie sempre più complesse basate su intelligence, advanced analytics e machine learning e competenze specialistiche dell'ambito forense e legale.

E per concludere, l'esigenza imprescindibile di garantire la Sicurezza IT ventiquattrore su ventiquattro, sette giorni su sette: un'altra sfida importante per qualsiasi azienda, anche e

soprattutto per le organizzazioni di maggiore dimensione, che nel 40% dei casi evidenziano questo aspetto come una delle sfide più complesse e problematiche: in questo caso, diventa prioritario disporre di risorse interne o di partner capaci di garantire un monitoraggio costante e "always on" dei sistemi, degli apparati e degli accessi, per una rapida diagnosi e risoluzione di eventuali incidenti, gettando le fondamenta per sviluppare la capacità di affrontare il rischio IT in modo proattivo e non soltanto reattivo.

Il ruolo della Sicurezza IT nei modelli Edge e IoT

Nelle scorse edizioni è già stato evidenziato in diverse occasioni il ruolo della Sicurezza IT come abilitatore di nuovi modelli tecnico-organizzativi legati ai processi di Trasformazione Digitale delle imprese. Come illustrato nelle previsioni di IDC a medio termine, i modelli di sviluppo legati alle architetture Edge e IoT va profilandosi come una delle maggiori opportunità per lo sviluppo del settore della Sicurezza IT, con tante sfide, sia tecniche che tecnologiche, ancora da superare, per realizzare integralmente i principi di una progettazione dove la Security-by-Design sia effettivamente un principio pienamente affermato.

Se si esamina un perimetro composto da circa 7 mila imprese italiane che stanno sviluppando una specifica progettualità Edge/ IoT, è possibile comprendere quali opportunità si stanno effettivamente aprendo nel mercato italiano. È possibile classificare queste imprese in due raggruppamenti distinti in base al focus prevalente sul monitoraggio dei processi di business oppure sulla gestione delle infrastrutture aziendali (**Fig. 5**).

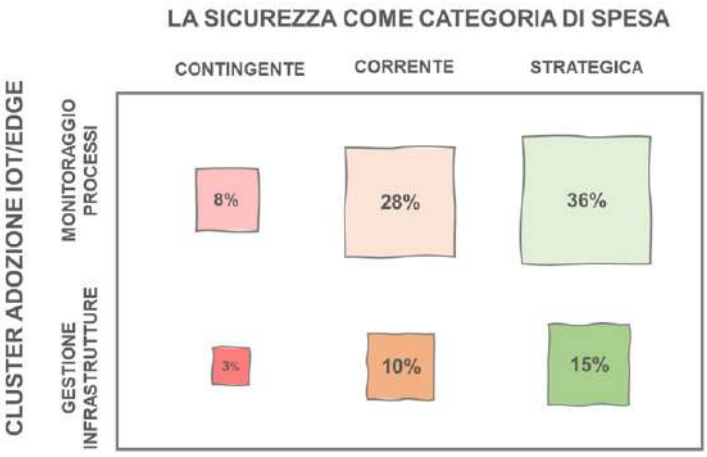


Figura 5 - *Il ruolo della Sicurezza IT tra le imprese con progetti IoT/ Edge.*
Fonte: IDC Italia, 2019 (imprese con oltre 50 addetti; estrapolazione a N = 6.700)

Le imprese che stanno concretamente lavorando su progetti in field e POC cominciano ad apprezzare un ruolo maggiore della Sicurezza IT tra i capitoli di spesa della propria azienda: oltre la metà delle imprese riconoscono la necessità di includere le tecnologie per la sicurezza in una progettualità di medio-lungo termine se si intende portare avanti l'integrazione tra IT e OT. Invece, ancora una impresa su dieci, pur affrontando progetti complessi, non riesce a cogliere il valore abilitante delle Sicurezza IT per progredire nella roadmap di sviluppo tecnologico.

Le differenze tra i raggruppamenti affondano radici profonde nelle distinte modalità di rischio che le imprese saranno chiamate ad affrontare quando le piattaforme Edge/ IoT diventeranno operative. Esaminando la percezione del rischio IT tra i due distinti raggruppamenti si osservano sensibilità distinte che lasciano intravedere l'opportunità di procedere con una segmentazione del mercato, aprendo spazi ulteriori di differenziazione per quegli operatori che sapranno cogliere l'opportunità di specializzare la propria offerta di tecnologie.

È possibile formulare una prima discriminazione di base esaminando la percezione dei rischi che gravano sui dati personali e sull'operatività aziendale. La privacy è un tema ampiamente sentito da tutte le imprese italiane, in modo particolare dopo l'impulso normativo degli ultimi anni, però rappresenta un obiettivo cruciale soprattutto per le imprese dove l'Edge e l'IoT partecipano alla gestione delle infrastrutture (90%). La discontinuità delle operazioni aziendali viene evidenziata all'interno dello stesso raggruppamento da quasi quattro aziende su dieci mentre ricorre in meno di un caso su dieci nel raggruppamento alternativo. Invece, le imprese orientate al monitoraggio dei processi mettono in evidenza altri aspetti critici nella gestione del rischio IT, che riguardano in misura prevalente le nuove forme di concorrenza sleale che possono diventare sempre più comuni in una economia ancora più digitalizzata nel prossimo futuro: il furto della proprietà intellettuale e dei contatti commerciali, rispettivamente il 37 e il 29% (**Fig. 6**).

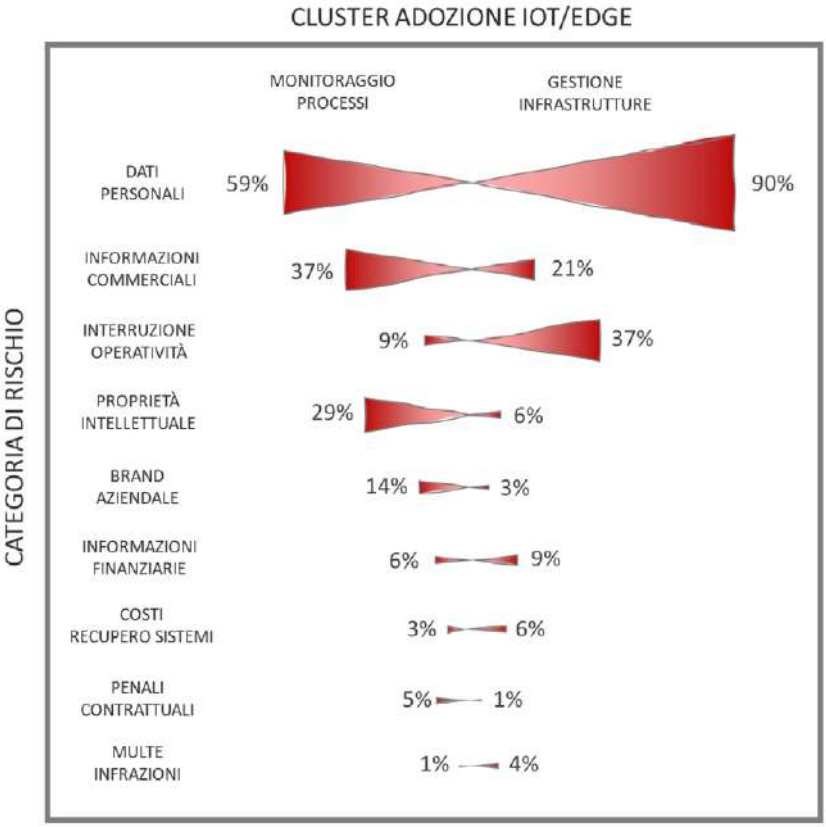


Figura 6 - *La percezione del rischio IT nei cluster di adozione IoT/ Edge.*
Fonte: IDC Italia, 2019 (imprese con oltre 50 addetti; estrapolazione a N = 6.700, basi differenti nei sottogruppi)

Gli operatori della Sicurezza avranno l'opportunità di cogliere e valorizzare al meglio i diversi segmenti del mercato italiano soltanto nel momento in cui le tecnologie si specializzeranno ulteriormente nella comprensione delle variegate forme che può assumere il rischio IT, tenendo sempre più spesso in considerazione la specifica "semantica" dei dati coinvolti nei diversi scenari di confronto con il cybercrime, il cyberwarfare e lo spionaggio digitale. In questa direzione e con questo obiettivo di fondo, la convergenza tra tecnologie della Sicurezza e algoritmi di Machine Learning consentirà di sviluppare piattaforme e soluzioni che consentiranno non soltanto di aumentare la capacità di analisi degli specialisti, ma permetteranno di mitigare i comportamenti a rischio degli utenti più ingenui.

È legittimo chiedersi se esiste una convergenza tra le roadmap di investimento nella Sicurezza IT e nel Machine Learning, oppure le tecnologie siano alternative rispetto ai budget disponibili. Quanto emerge dalle ultime indagini condotte tra le imprese italiane non mette ancora in evidenza una chiara convergenza nei programmi di investimento, quantomeno nel breve termine: le imprese che investono in Sicurezza IT di solito non investono nel Machine Learning e viceversa. E questo significa che la gestione delle problematiche di sicurezza nei progetti IT/ OT vengono verosimilmente affrontate con applicazioni integrate in architetture più ampie, implementando strategie di Security essenzialmente guidate dalle piattaforme (e non autonomamente determinate dalle esigenze di business o dalle caratteristiche specifiche dei processi). Secondo IDC, nei prossimi anni assisteremo a una convergenza maggiore degli investimenti tra queste aree per sviluppare modelli tecnico-organizzativi di Augmented Security che oltrepasseranno i tradizionali approcci di "embedded intelligence" dove gli analytics sono soltanto integrati negli applicativi, ma non nei processi.

La sicurezza in ambito industriale

[A cura dell'Osservatorio Information Security & Privacy della School of Management del Politecnico di Milano]

La sempre maggiore pervasività della digital transformation nelle aziende viene ben rappresentata dalla contaminazione positiva che negli ultimi anni l'innovazione digitale sta avendo nel contesto industriale, negli ambienti produttivi e nella gestione delle infrastrutture critiche, grazie anche alle agevolazioni studiate a livello istituzionale per l'Industria 4.0. L'avvento di tale paradigma e la crescente diffusione dell'Internet of Things anche in questo campo presuppongono da un lato l'interconnessione di sistemi e dispositivi di produzione originariamente non progettati per tale scopo e, dall'altro, l'integrazione in rete di sensori e macchinari che generano e scambiano enormi moli di dati in tempo reale. Tali elementi contribuiscono, dal punto di vista della security, ad aumentare i rischi, ampliando enormemente la superficie di attacco e creando un panorama complesso e intricato, in cui le minacce indirizzate alle infrastrutture critiche e ai sistemi ICS e SCADA (Supervisory Control And Data Acquisition) sono in continua crescita.

L'Osservatorio Information Security & Privacy, al suo quinto anno di Ricerca, si è posto l'obiettivo di rispondere al bisogno di conoscere, comprendere e affrontare le principali problematiche dell'information security e della data protection e di 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 2019 dell'Osservatorio ha proposto una Survey di rilevazione che ha coinvolto 698 CISO, CSO, CIO, Compliance Manager, Risk Manager, Chief Risk Officer e DPO di imprese italiane. In particolare, sono state coinvolte 180 organizzazioni grandi (>249 addetti) e 501 PMI (tra 10 e 249 addetti).

La gestione dell'OT Security – La Survey dell'Osservatorio Information Security & Privacy

La Survey sulle grandi imprese, oltre a monitorare il mercato dell'information security e il percorso di adeguamento delle aziende ai requisiti imposti dalle normative in materia di data protection, ha dedicato un approfondimento al mondo della sicurezza in ambito industriale, anche denominata OT (Operational Technology) Security[1].

Dalla rilevazione è emerso innanzitutto come gran parte delle organizzazioni sta implementando opportuni strumenti e tecnologie per far fronte alle crescenti minacce: il 68% delle aziende afferma di effettuare security assessment e/o audit su sistemi e reti OT, al fine di

[1] Per OT Security si intende la messa in sicurezza di componenti hardware e software dedicati al monitoraggio e al controllo di processi e asset fisici, prevalentemente in ambito industriale o nei settori che gestiscono infrastrutture critiche (Oil&Gas, Energy, Utilities, Telco).

individuare vulnerabilità e rischi, mentre si attesta al 60% la percentuale che dichiara di aver introdotto soluzioni di sicurezza specifiche in ambito industriale. Tra le tecniche più diffuse emergono la segmentazione della rete e le soluzioni per il controllo degli accessi e la gestione dei privilegi. Altre tecniche che registrano una diffusione rilevante sono monitoraggio rete e analisi log e vulnerability assessment e penetration test. In ottica prospettica, le soluzioni che riscontreranno una maggiore crescita sono i SOC (Security Operation Center) convergenti, i tool di anomaly detection e l'analisi statica/code review per garantire la sicurezza delle applicazioni (**Figura 1**).

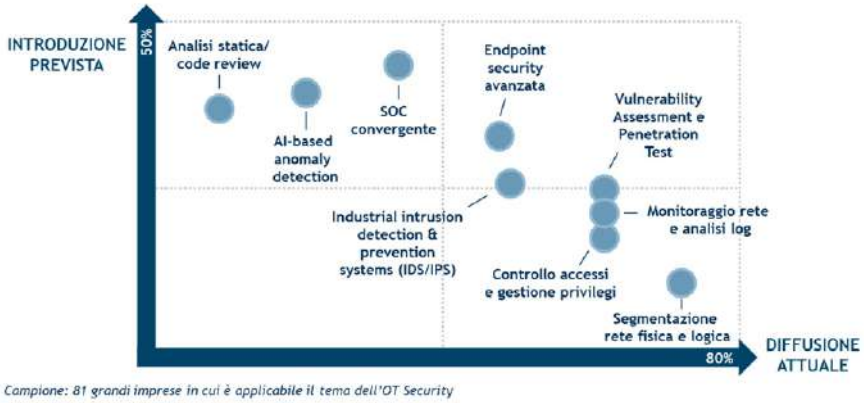


Figura 1: *Gli strumenti e le tecnologie adottate – Fonte: Osservatorio Information Security & Privacy, School of Management Politecnico di Milano*

Le sfide che le aziende si trovano a dover affrontare quando si parla di OT Security non sono però soltanto legate al campo tecnologico, ma anche alla sfera delle competenze e dei modelli organizzativi.
Secondo quanto emerge dalla Survey, il presidio dell'OT Security all'interno delle grandi aziende italiane è gestito in maniera estremamente eterogenea: molto spesso viene demandato alla funzione IT (47%), in alcuni casi (11%) alla funzione Information Security, se diversa dall'IT, e più raramente alla divisione Operations (4%). Esistono poi situazioni in cui la gestione dell'OT Security è demandata a più di una delle funzioni aziendali elencate precedentemente (23%). A completamento del campione, il 15% delle organizzazioni lamenta una totale mancanza di presidio, che non è esplicitamente demandato a nessun soggetto in particolare, sia esso interno o esterno all'organizzazione.

Qualsiasi sia la configurazione scelta, individuare in modo chiaro profili direzionali e di responsabilità in questo campo è molto complesso ed è quindi opportuno prevedere dei meccanismi di coordinamento tra le funzioni IT, Information Security e Operations, anche

attraverso l'istituzione di appositi Steering Committee. Tali meccanismi sono stati attualmente definiti nel 44% delle organizzazioni intervistate.

Un altro fattore approfondito nel corso dell'indagine riguarda i profili di competenze. Nel 48% delle organizzazioni intervistate esistono figure interne con competenze di OT Security, diffuse tra le varie funzioni aziendali: le skills si possono trovare nell'IT (25%), nell'Information Security (15%), nelle Operations (6%) o in altre funzioni (2%).
Il 22% del campione dichiara di non poter attualmente contare sulla presenza di figure specializzate in materia di OT Security, ma di volerle introdurre in azienda entro i prossimi 12 mesi; mentre nel restante 30% le competenze sono assenti e al momento non se ne prevede l'introduzione (**Figura 2**).

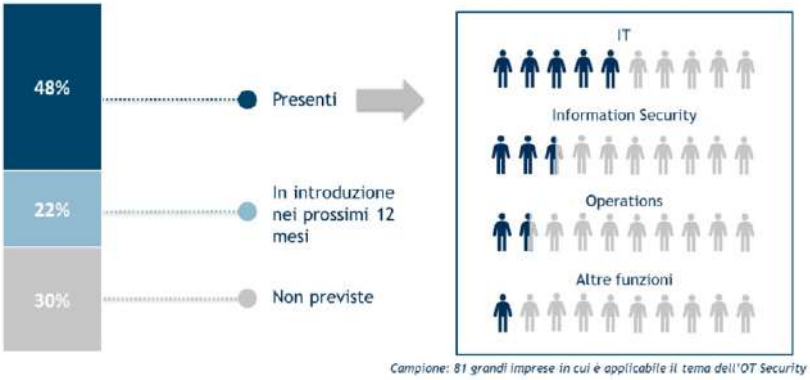


Figura 2: *Le figure specializzate in OT Security – Fonte: Osservatorio Information Security & Privacy, School of Management Politecnico di Milano*

Nel contesto in esame, la consapevolezza dei dipendenti dell'organizzazione rappresenta un elemento imprescindibile per minimizzare i rischi: diventa pertanto essenziale svolgere formazione a tutti i livelli per sensibilizzare il personale aziendale rispetto alle possibili minacce per la sicurezza. Si attesta al 45% la percentuale di aziende in cui è già stata prevista la definizione di programmi di cybersecurity awareness & training che includano il tema industriale; nel 35% dei casi sono inoltre state introdotte specifiche policy comportamentali in materia.

Workshop "Industrial Security 4.0" – La metodologia

Nel corso del 2019 l'Osservatorio ha approfondito il tema della sicurezza in ambito industriale anche attraverso interviste condotte con importanti aziende del settore e un Workshop a porte chiuse dal titolo "*Industrial Security 4.0*". In linea con le finalità di lavoro dell'Osservatorio, durante l'incontro è stata utilizzata una metodologia di lavoro innovativa

che ha visto l'utilizzo di un framework sviluppato dall'Osservatorio e una successiva discussione tra i partecipanti (**Figura 3**).

Figura 3: *Il framework di gioco – Fonte: Osservatorio Information Security & Privacy, School of Management Politecnico di Milano*

In preparazione al Workshop è stata predisposta una lista contenente alcuni scenari di incidente cyber che avrebbero potuto potenzialmente verificarsi in ambiente industriale. Ai partecipanti è stato poi chiesto di selezionare uno o più scenari di preferenza: sulla base dei risultati della votazione sono stati individuati tre scenari di incidente, ciascuno dei quali ha costituito il focus della discussione di uno dei gruppi di lavoro (il dettaglio dei singoli scenari di incidente verrà illustrato in seguito).

L'obiettivo del serious game consisteva nell'individuare le principali contromisure tecnologiche, organizzative e procedurali per far fronte a uno degli eventi di sicurezza precedentemente individuati. Nello specifico, i partecipanti sono stati chiamati a mappare le proprie scelte secondo 3 leve:

- gli strumenti e le tecnologie da adottare per far fronte alla specifica situazione;
- le figure e le competenze da mettere in campo;
- le procedure e le policy da definire e seguire.

L'individuazione delle contromisure doveva inoltre tenere conto di tre diverse fasi temporali:
- prima: quali azioni implementare per prevenire il verificarsi dell'evento di sicurezza;
- durante: quali misure urgenti (non necessariamente pianificate) adottare per contenere gli impatti dell'incidente una volta verificato;
- dopo: quali azioni, anche di medio/lungo periodo, mettere in atto per risolvere l'incidente e/o evitare che lo stesso si ripetesse in futuro.

Durante il serious game ogni partecipante ha innanzitutto compilato individualmente un foglio in cui ha descritto, sulla base della propria personale esperienza, la gestione dello specifico scenario di incidente cyber secondo le leve e le fasi descritte in precedenza.
Successivamente, ogni partecipante ha condiviso il proprio ragionamento all'interno del gruppo ed effettuato una sintesi delle contromisure (tecniche, organizzative e procedurali) che riteneva fosse necessario adottare. Tale sintesi è avvenuta mediante scrittura su un post-it di una o più parole chiave. I post-it sono stati attaccati su un unico cartellone che richiamava il framework già completato individualmente (**Figura 4**).

Figura 4: *Compilazione del framework di gioco – Fonte: Osservatorio Information Security & Privacy, School of Management Politecnico di Milano*

Una volta effettuata la mappatura delle contromisure è stato chiesto ai partecipanti di ragionare sui principali ostacoli all'adozione e alla realizzazione delle contromisure sintetizzate. Ciascuno dei partecipanti è stato pertanto chiamato a contrassegnare con alcuni bollini rossi le misure che considerava più critiche e meno fattibili nello specifico contesto (**Figura 5**). In seguito a tale attività è stata svolta una breve discussione delle motivazioni che hanno giustificato la scelta.

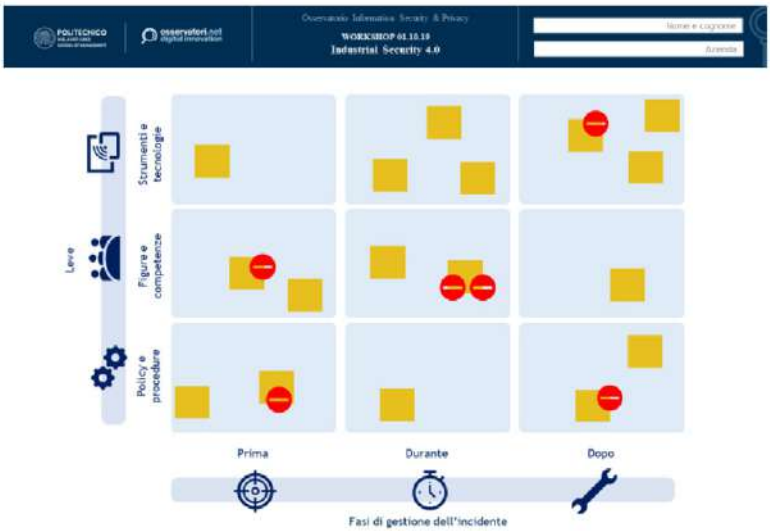


Figura 5: *Mappatura delle criticità sul framework di gioco – Fonte: Osservatorio Information Security & Privacy, School of Management Politecnico di Milano*

Workshop "Industrial Security 4.0" – Gli scenari di incidente cyber e i messaggi emersi

Di seguito si propongono gli scenari di incidenti cyber analizzati nel corso dell'incontro e i principali messaggi emersi dalla discussione tra i partecipanti.

Scenario 1: diffusione di malware attraverso supporti removibili o hardware esterni

Il primo scenario riguardava la propagazione di un malware in ambiente industriale attraverso una chiavetta USB frequentemente usata da un dipendente aziendale in ambiente domestico o a lavoro ed impropriamente introdotta in PC della rete di processo.

A seguito della discussione è emersa innanzitutto l'importanza di lavorare sul tema della gestione del fattore umano, mettendo in atto misure volte a sensibilizzare i vendor e tutti i dipendenti dell'organizzazione, in particolare gli operatori degli impianti.

Si è posto l'accento anche sulla necessità di creare dei comitati deputati ad analizzare la situazione post-incidente e, in generale, sull'importanza di prevedere dei processi in grado di garantire che il Board sia sempre allineato. Sempre a livello organizzativo è fondamentale inoltre adottare specifiche policy in grado di normare la possibilità o meno di poter accedere ai sistemi con dispositivi mobili.

Da un punto di vista delle tecnologie è emersa infine la necessità di avere strumenti tecnologici in grado di identificare e circoscrivere l'effettiva area colpita dall'evento di sicurezza:

tra le tecniche più efficaci è emersa la segmentazione della rete, che viene suddivisa in parti non comunicanti o separate da controlli di sicurezza al fine di confinare un eventuale problema in un unico segmento, evitando che la minaccia si propaghi.

Scenario 2: diffusione di malware attraverso Internet o la Intranet

Il secondo scenario di incidente cyber riguardava invece la propagazione di un malware in ambiente industriale attraverso un attacco che sfruttava vulnerabilità zero-day di un software presente su un browser o applicazione, nonché vulnerabilità o carenze nell'implementazione o configurazione di sicurezza nei protocolli SCADA/ICS.
A livello di detection dell'incidente sono state individuate numerose soluzioni tecnologiche utili a prevenire il verificarsi della minaccia tra cui, ad esempio, asset inventory, SIEM, protezione degli endpoint e sistemi di intrusion prevention, ma si è ravvisata per contro una carenza di strumenti in grado di gestire una situazione post-incidente.
Relativamente all'ambito delle "persone", si è rilevata nella quasi totalità delle situazioni la mancanza di specifiche figure professionali in grado di coniugare competenze di security e competenze OT.
Dal punto di vista delle procedure si è posto l'accento sulla necessità di adottare policy specifiche per i fornitori, mentre è apparso molto critico il tema del patch management, soprattutto nel caso di vulnerabilità zero-day come quello in esame.

Scenario 3: accesso da remoto

Il terzo scenario, infine, era incentrato su un attacco attraverso i punti di accesso da remoto protetti da password di default utilizzati dal personale terzo addetto alla manutenzione di un sistema di controllo industriale.
Qui l'esigenza principale ravvisata atteneva alle procedure e alla gestione della supply chain e riguardava la necessità di agire puntualmente con strumenti contrattuali per fornire standard specifici ai fornitori e svolgere audit per verificarne il loro rispetto.
Anche con riferimento a tale scenario si è posto l'accento sull'importanza di lavorare sulla formazione e creare consapevolezza rispetto a tutti i potenziali effetti di un incidente. È inoltre indispensabile assegnare chiaramente le responsabilità, con un progressivo trasferimento dell'accountability sulle figure responsabili dell'impianto.
Da un punto di vista degli strumenti, le soluzioni di Multi-Factor Authentication (MFA) e di Privileged Access Management (PAM) rappresentano in questo contesto tecnologie chiave per prevenire un incidente di questa tipologia o, in caso venissero implementate ex-post, per evitare che si ripeta.

L'impatto dei deepfake sulla sicurezza delle organizzazioni economiche. Deepfake-as-a-Service.

[A cura di Federica Bertoni)

Breve introduzione al fenomeno.

L'alba di questo nuovo decennio ha visto i deepfake svettare nelle classifiche previsionali stilate dagli esperti di settore sulle principali minacce informatiche del 2020. L'annunciato pericolo deepfake incombe dunque, ora, con grande concretezza anche sulle aziende, le quali, con altrettanta urgenza, dovrebbero farsi trovare pronte ad affrontarlo e a gestirlo nel modo migliore possibile.

Figura 1 *Obama calling Trump a 'dips---' https://www.youtube.com/watch?v=cQ54GDm1eL0*

D'altronde, come potrebbe essere diversamente?
Se guardiamo all'anno appena trascorso, infatti, i deepfake sono balzati agli onori della cronaca occupando sempre di più le prime pagine di testate giornalistiche, cartacee e on line, a livello globale: se n'è discusso vivacemente, non soltanto per gli usi satirici che si fanno dei falsi profondi, anche a scopo dimostrativo ed educativo (si pesi ai deepfake che hanno visto come protagonisti Mark Zuckerberg, Kim Kardashian e Donald Trump)[1], ma

[1] Le creazioni citate sono opera di Bill Posters, artista britannico celebre per i suoi deepfake realizzati allo scopo di sensibilizzare l'opinione pubblica sul problema che i falsi profondi costituiscono per la società. Bill Posters, ad esempio, oltre a impersonare un perfetto Obama in uno dei primi deepfake diventati celebri per l'altissimo livello di realismo raggiunto, ha anche creato l'altro famoso deepfake in cui Mark Zuckerberg dichiara di possedere la vita degli utenti della piattaforma. Anche in questo caso, ...*(segue)*

soprattutto perché, quando il grado di realismo di contenuti audiovisivi artefatti rasenta la perfezione, affossare un personaggio politico, manipolando conseguentemente l'opinione pubblica, durante una campagna elettorale, ad esempio, o danneggiare la reputazione di celebrità, attivisti e, più in generale, di personaggi pubblici ritenuti "scomodi" diventa assai semplice ed estremamente pericoloso.

Attualmente i falsi profondi minacciano molto da vicino anche le organizzazioni economiche: sebbene finora si possano contare pochissimi attacchi deepfake sferrati con successo contro aziende e resi poi di pubblico dominio, tuttavia gli esperti stimano che il loro numero sia destinato a salire rapidamente, poiché le tecnologie sottostanti, non solo diventano sempre più sofisticate, ma incrementano di numero, varietà e si diffondono a dismisura. Non è certo un caso se sono nati veri e propri mercati on line, all'interno dei quali è possibile commissionare per 30 dollari video deepfake, oppure richiedere il servizio di clonazione della voce, spendendo dieci dollari, per ogni 50 parole riprodotte[2]. Si parla in tal senso di commoditizzazione, ovvero di deepfake-as-a-Service. I software che generano falsi profondi sono di fatto alla mercé di chiunque, perché sono semplici da utilizzare, economici e pronti all'uso. Inevitabilmente hanno ingolosito i criminali informatici e bad actor economici, che ne hanno colto tutte le potenzialità, posto che in tale tecnologia vi si cela l'occasione perfetta, l'arma ideale capace di garantir loro guadagni pressoché immediati e particolarmente importanti.

Gli attacchi deepfake in ambito commerciale: casi e numeri.

Durante l'estate 2019 i ricercatori della società di sicurezza informatica Symantec hanno rivelato di aver ricevuto la segnalazione di almeno tre casi di voci di dirigenti clonate per truffare aziende e sottrarre loro ingenti somme di danaro. Si è trattato ogni volta di deepfake audio.

In un tempo in cui il consumo è conversazionale, il proliferare di aziende che basano il proprio core business sull'erogazione di servizi vocali e sull'utilizzo di tecnologie biometriche di autenticazione vocale fa sì che, di contro, lo stesso terreno sia "coltivato" anche da attori malevoli, i quali, con l'implementazione di programmi di voice-mimicking, arricchiscono e aggiornano il proprio arsenale con software intelligenti deputati a replicare la voce umana. Tali tool operano con sommo grado di precisione, affinandosi di giorno in giorno, riuscendo a riprodurre accento, intonazione, inflessione e manierismi del soggetto imitato, fino al modo in cui lo stesso si esprime[3].

---

il falso profondo è stato ideato per testare la capacità di moderazione dei deepfake di Facebook, ritenuta da alcuni esperti debole se non addirittura inefficace.

[2] Henry Ajder, Giorgio Patrini, Francesco Cavalli & Laurence Cullen, "The State Of Deepfakes: Landscape, Threats and Impact", anno 2019, della società Deeptrace, disponibile sul sito https://deeptracelabs.com/resources/

[3] Alcune tecniche impiegate con successo sono l'imitazione, l'attacco replay, il software di modificazione vocale e la sintesi vocale.

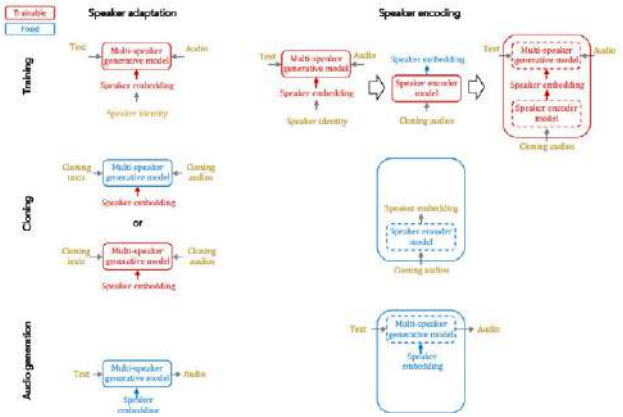


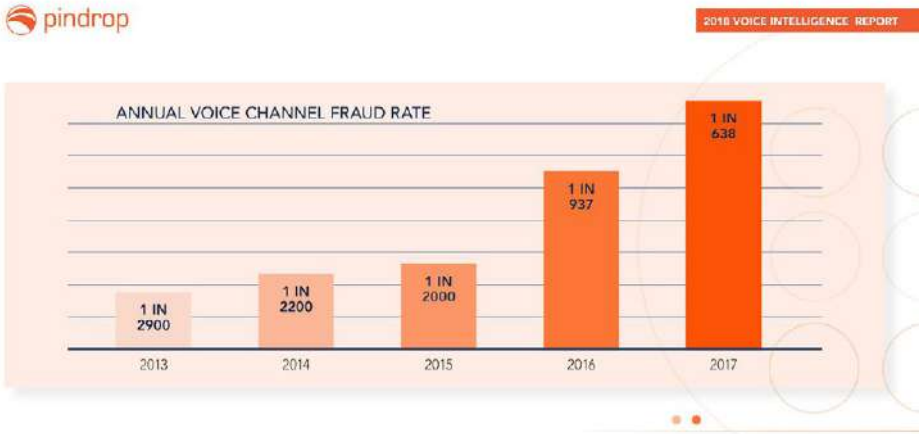
Figura 2 *Speaker adaptation and speaker encoding approaches for training, cloning and audio generation. Credit: arXiv:1802.06006 [cs.CL]*

Per tale ragione, i primi attacchi deepfake scagliati con successo contro alcune imprese sono stati le frodi vocali. Chi non rammenta la notizia rimbalzata di recente su più canali d'informazione che ha visto una ditta energetica britannica cadere, nel marzo 2019, nella trappola di un audio deepfake? Utilizzando la voce sintetica che impersonava il CEO della società madre tedesca, i truffatori hanno potuto replicare fedelmente il parlato del dirigente in questione. L'amministratore della società inglese è stato così ingannato e senza esitare ha adempiuto prontamente alla richiesta di bonifico, così come gli era stata impartita dallo scammer, versando 243 mila dollari sul conto del presunto fornitore ungherese menzionato nella telefonata. Euler Hermes, la società d'assicurazioni francese dell'azienda vittima della frode, ha coperto la perdita nei termini previsti dalla polizza che la società aveva fortunatamente stipulato. Non si hanno tuttavia avuto più notizie delle acquisizioni delle telefonate, ai fini dell'accertamento dell'accaduto, né, ad oggi, i responsabili sono stati identificati e il bottino, instradato attraverso diversi paesi, non è più recuperato.
Il caso non risulta essere isolato[4], ma tale episodio è stato quello che ha avuto maggior eco mediatico, tanto da assurgere a esempio concreto sull'efficacia che un attacco deepfake può imprimere in ambito corporate.

[4] Un'altra vicenda, ad esempio, ha riguardato il finto amministratore delegato di una società finanziaria che ha chiamato un suo dipendente affinché disponesse con urgenza un bonifico bancario di 10 milioni di dollari a un fornitore. Il collaboratore pressato dall'urgenza ha tempestivamente ottemperato al suo compito, anche se l'azione posta in essere violava i protocolli dell'azienda, a dimostrazione che le più antiche strategie di social engineering vanno sempre in porto (in questo caso il senso di impellenza generato nel dipendente dal presunto superiore).

Un altro caso interessante di deepfake si è verificato sempre nel marzo 2019 ai danni di Tesla, quando su LinkedIn e Twitter due account di una fantomatica giornalista di Bloomberg, "Maisy Kinsley", ha cercato di connettersi a 195 shortseller di Tesla. Alcuni di questi shortseller hanno dichiarato che "l'utente" aveva inoltrato loro richiesta di contatto nel tentativo di esfiltrare informazioni. Entrambi gli account sono stati poi rimossi dalle due piattaforme social. La foto di Maisy Kinsley pareva essere stata generata proprio da una GAN, acronimo di "Generative Adversarial Network", ovvero della tecnica di machine learning che sta alla base dell'elaborazione e della produzione di gran parte dei deepfake in circolazione. Bloomberg ha successivamente confermato di non annoverare fra le proprie fila nessuna giornalista di nome Maisy Kinsley. È chiaro come in questo caso l'attacco deepfake posto in essere mirava al furto di dati e ad azioni di spionaggio.

Per quanto concerne, invece, i numeri del fenomeno, vale la pena accennare ai risultati cui sono pervenute due importanti aziende e centri di ricerca che si occupano rispettivamente di biometria vocale e deepfake. Si tratta di Pindrop e Deeptrace.

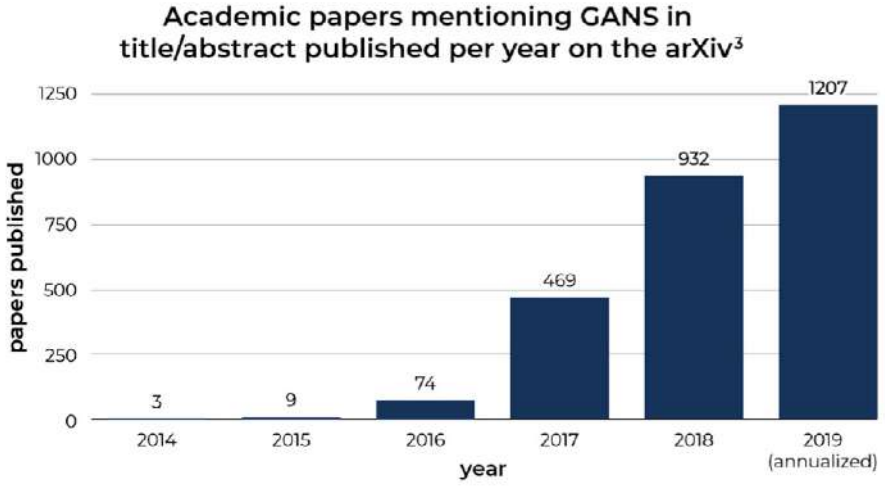


Pindrop, nel suo Voice Intelligence Report del 2019[5] evidenzia che la frode vocale si leva minacciosa sulle imprese, posto che risulta già appurato un aumento dei tassi di sfruttamento di tale tipo di truffa di oltre il 350 per cento, segnando al contempo una sorta di record tagliato nell'arco temporale fra il 2014 e il 2018. Negli anni precedenti, inoltre, non erano certo mancate le avvisaglie all'imminente esplosione del pericolo dei falsi profondi per le organizzazioni economiche: Pindrop aveva infatti svolto un altro studio in cui i dati emersi puntavano già tutti nella medesima direzione: fra il 2013 al 2017 le frodi vocali erano cresciute di oltre il 300 per cento e non manifestavano alcun segnale di rallentamento, con anzi un ulteriore incremento e picco tra il 2016 e il 2017 del 47 per cento, cioè una frode vocale ogni 638 telefonate. Il rapporto di Pindrop dunque dipinge un quadro in cui i tassi di frode sono assai elevati, se si considera che i numeri racchiusi nel resoconto scaturiscono da un imponente lavoro di ricerca condotto attraverso 1 miliardo e più di telefonate fatte ad alcuni dei maggiori call center americani di banche, assicurazioni e società di servizi finanziari. In particolare, negli Stati Uniti risultano verificarsi ogni giorno 90 attacchi di canali vocali al minuto, all'interno di uno scenario dove il mercato di tipo conversazionale cui si faceva riferimento poc'anzi e l'esperienza dei clienti con l'autenticazione vocale vede contemporaneamente trasformare quelle potenzialità di business e di progresso tecnologico anche in un vero e proprio campo minato per le aziende stesse e gli utenti, proprio a causa degli inevitabili utilizzi malevoli che le tecniche d'intelligenza artificiale sottese al vocale hanno inaugurato. Le aree economiche più a rischio sono risultate essere le assicurazioni (1 su 7.500 chiamate fraudolente), il commercio al dettaglio (1 su 325 chiamate fraudolente), il settore bancario (1 su 755 chiamate fraudolente), gli emittenti di carte (1 su 740 chiamate fraudolente), i broker (1 su 1.742 chiamate fraudolente) e le cooperative di credito (1 su 1.339 chiamate fraudolente).

[5] https://www.pindrop.com/lp/white-papers/fraud-intelligence-report-2020/

Pindrop ha rimarcato "come gli attacchi vocali sintetici diventeranno presto la prossima forma di violazione dei dati", tant'è che in un futuro non troppo lontano i truffatori chiameranno i call center servendosi di voci sintetiche per testare se le aziende sono equipaggiate di tecnologie idonee a rilevarle e ciò colpirà in particolar modo gli istituti di credito. Si badi bene che anche le misure di sicurezza biometriche, come il riconoscimento vocale e facciale su cui si fondano le procedure automatizzate KYC, per i clienti delle banche, possono essere compromesse dai deepfakes.

Dal secondo rapporto in esame, cioè quello di Deeptrace, pubblicato a settembre 2019, scaturiscono altri numeri degni di nota: innanzitutto la quantità di deepfake on line e disponibili è doppia rispetto ai dati di dicembre 2018 e cioè è emerso che a settembre 2019 era pari a 14.678, con un incremento dell'84% rispetto all'anno precedente. Anche se si tratta ancora per il 96% di casi di deepfake a sfondo pornografico, il rapporto non manca di esaminare da vicino anche tutti gli altri contesti in cui attacchi di tipo deepfake sono stati perpetrati. Nell'indagine di Deeptrace, infatti, sono snocciolati anche altri dati e numeri meritevoli d'attenzione e riguardano il trend sui paper accademici che citano le GANs e di come anche dei falsi profondi abbia preso piede la c.d. commoditizzazione, tanto che anche per essi è nata l'ormai famigliare formula "as-a-Service" (-aaS).



L'età aurea dell'ingegneria sociale.

Il problema principale che i deepfake incarnano è che con essi si finisce per veder sgretolata quasi del tutto la capacità di giudizio, cioè l'autonomia di distinguere fra ciò che è autentico e ciò che non lo è.

In un mondo in cui il verosimile s'impone per il tramite della sofisticatezza insita nelle

tecnologie dell'intelligenza artificiale e del machine learning, essere non più padroni delle proprie decisioni è già realtà, con conseguenze sul piano della volontà e della libertà personale di scegliere, poiché viene a mancare quel substrato d' informazioni veritiere e reali su cui orientarsi. Come se non bastasse, tutto ciò accade, il più delle volte, senza che ce ne si accorga, se non altro nel momento in ci sarebbe bisogno di consapevolezza, vedendo così sfalsati anche i piani dei tempi e modi del proprio agire personale.

Figura 3 *Immagini di 100mila persone inesistenti ma del tutto realistiche create dalla startup 'Generated Photos', utilizzando la tecnologia GAN (Generative Adversarial Network). Lo scopo? "Democratizzare la fotografia creativa", ha dichiarato la giovane azienda.*

La ragione per cui i deepfake costituiscono un fenomeno infído, un pericolo grave, concreto e attuale è rintracciabile già nel termine stesso che li rappresenta: il "deepfake" è un falso profondo, un insieme di contenuti video, audio, o audio-visivi contraffatti in maniera così superba da sfiorare la perfezione. I falsi profondi sono in grado di erodere la capacità stessa della società intera di essere d'accordo non soltanto su ciò che è vero ma su ciò che è addirittura reale[6]. "L'essere umano non è razionale, come ci ostiniamo a credere, bensì ha una visione del mondo che è emotiva e percettiva" ha puntualmente evidenziato Walter Quattrociocchi[7] ed è in questo solco tracciato dall'emotività umana e percettiva che i deepfake s'insinuano e attecchiscono. La viralità, l'audience illimitato del Web e le altre caratteristiche proprie dell'ambiente cibernetico fanno poi il resto, esasperandone gli effetti.

6 Cfr. Franklin Foer, Reality's End. The current era of "fake news" may soon seem quaint. Video manipulation is eroding society's ability to agree on what's true – or what's even real", The Atlantic, May 2018, pp. 15-18

7 Giulia Bona, Walter Quattrociocchi: come ti prevedo le fake news, in "Scienza in Rete", https://www.scienzainrete.it/articolo/walter-quattrociocchi-come-ti-prevedo-le-fake-news/giulia-bona/2018-04-03

Per tali motivi i deepfake segnano un salto di qualità dell'ingegneria sociale, che con essi fa un balzo in avanti, entrando nella propria età dell'oro.
Inoltre, anche le migliori tecniche per individuare i falsi profondi potrebbero essere compromesse dalla stessa natura umana, che si sa essere e sarà per sempre l'anello debole della catena. Come è stato autorevolmente evidenziato da Areeq Chowdhury di Future Advocacy[8]: "*Dobbiamo essere consapevoli che non importa quanti strumenti mettiamo in circolazione, ci sarà sempre una certa percentuale di persone che non crederà a uno strumento di verifica.*". Come a dire che sussiste anche un'inclinazione naturale a consumare mezzi di comunicazione falsi. I deepfake sono del resto intrinsecamente idonei a corroborare le opinioni di tutti quei soggetti-utenti che, possedendo delle concezioni esclusive e circoscritte su determinati temi, cadono più facilmente nei c.d. tranelli cognitivi di conferma[9]. Se si rammenta che ciò avveniva e ancora avviene con le fake news, appare evidente come tale evenienza possa realizzarsi con una probabilità di successo nettamente maggiore con fake d'acciaio, quali possono essere considerati i deepfake. I falsi profondi provocano cecità anche di fronte a segnali di avvertimento: quando la qualità dei contenuti falsi è altamente credibile, verosimile, il livello di vigilanza degli utenti cala drasticamente, fino a precipitare.

I rischi: dall'impersonificazione diretta al rafforzamento delle tecniche di frodi economiche preesistenti.

Si è già detto dei ruoli che l'economia conversazionale e il vocale assunto a interfaccia primaria nel mondo IoT giocano nello sviluppo dei deepfake; si è accennato altresì anche alle tecniche delle Generative Adversarial Network (GANs) e alla commoditizzazione dei software di deepfake. Chiaramente tutti questi fattori per sortire efficacia non solo debbono essere messi in relazione e accordati fra loro, ma ancor prima necessitano di essere combinati con quella materia prima, grezza indispensabile per la realizzazione stessa dei deepfake. I video aziendali, le call commerciali, le apparizioni sui media, così come i keynotes delle conferenze e le presentazioni sono il tipo di materiale che è facilmente reperibile in Rete in abbondanza ideale per addestrare un sistema di AI a costruire, ad esempio, il modello perfetto della voce di un CEO, di un amministratore delegato, ad esempio. È opportuno osservare che anche se la tacnologia sottostante non risulta ancora perfetta, i cybercrook ne sono consapevoli e aggirano i limiti mettendo a punto artefatti come il rumore di fondo di un aeroporto, di un'auto.

[8] "Future Advocacy is a non-partisan consultancy ancd think thank working a t the intersection of advocacy, global affairs, and technology", www.futureadvocacy.com

[9] Per un approfondimento in tal senso, si veda Ana Lucía Schmidt, Fabiana Zollo, Antonio Scala, Walter Quattrociocchi, "Polarization Rank: A Study on European News Consumption on Facebook", all'indirizzo https://arxiv.org/pdf/1805.08030.pdf

Figura 4 *"Spinello in diretta per Elon Musk" e non è un deepfake.*
Fonte: https://www.adnkronos.com/fatti/esteri/2018/09/08/spinello-diretta-per-elon-musk-tesla-crolla-borsa_AfYK6dTJdcxKAw0GK6UdZJ.html

Da quanto appena descritto si evince che plasmare un deepfake e utilizzarlo contro un'organizzazione economica diventa agevole. I deepfake stanno diventando mainstream e nei casi d'impersonificazione diretta i rischi principali sono rappresentati da azioni d'ingegneria sociale pressoché perfette, atti di manipolazione del mercato e da meccanismi di estorsione. Si pensi alle seguenti ipotesi nient'affatto scolastiche, in cui un video deepfake mostri un amministratore delegato che annunci artatamente una fusione o dia false cattive notizie sulla propria azienda, provocando così il crollo (o l'impennata) del prezzo delle azioni e sabotando il marchio, a tutto vantaggio dei competitor[10]. Deepfake del genere poi, potrebbero anche inguaiare legalmente gli stessi vertici aziendali con un effetto a cascata su funzionari, responsabili[11] finanche sui dipendenti. Nemmeno deve essere trascurato il comportamento tenuto da influenti leader economici, soprattutto se abitualmente o anche solo talvolta essi agiscono "sopra le righe", poiché in tali casi diventano i bersagli ideali per i deepfake. Un esempio che può valere per tutti è Elon Musk: nel marzo 2018 il CEO di Tesla si è fumato realmente uno spinello in diretta, durante un'intervista bevendo anche del whiskey[12].

[10] In un recente rapporto di New Knowledge emerge che il 78% dei consumatori ritiene la disinformazione pericolosa per la reputazione dei brand aziendali.

[11] Così, Douglas Mapuranga, Chief Information Officer della Infrastructure Development Bank of Zimbabwe e presidente del capitolo dell'organizzazione no-profit ISACA per la sicurezza delle informazioni di Harare.

[12] Appare forse superfluo riferire che successivamente si è verificato un crollo del 6% delle azioni della società, con una perdita di 3.1 miliardi di dollari, oltre alle dimissioni di due dirigenti dell'azienda.

Un altro aspetto importante quando si esaminano i rischi dei falsi profondi è la viralità della Rete. Attraverso di essa il danno che i deepfake infliggono si realizza prima che il falso possa essere eliminato o etichettato come non autentico, rendendo di fatto vana l'opera di rollback.
Sempre con riferimento ai rischi d'impersonificazione diretta, se ad oggi l'attenzione si è concentrata soprattutto sulle telefonate aziendali messe raffinatamente a repentaglio dai falsi profondi, ad esse si aggiunge un'ipotesi ulteriore e tutt'altro che fantasiosa: si tratta di un attacco deepfake tramite videocall commerciali: s'immagini l'impersonificazione sintetica di un cliente su Skype, mentre gli vengono forniti dettagli sensibili su un determinato progetto.

Figura 5 *"Scammers use CEO voice 'deepfakes' to con workers into wiring cash", https://ethhack.com/2019/09/forget-email-scammers-use-ceo-voice-deepfakes-to-con-workers-into-wiring-cash/*

I falsi profondi rappresentano dunque uno strumento senza eguali per impersonare gli individui ed esaltare le possibilità di successo delle frodi, anche in contesti tradizionalmente "sicuri" o che si ritengono forti della propria compliance dal punto di vista normativo e degli standard in materia di sicurezza e privacy. Per tale motivo è fondamentale sottolineare come i deepfake siano sfruttati dai criminali per irrobustire i più antichi schemi di frodi informatiche. Si sa che l'e-mail spoofing per così dire "tradizionale" provochi alle imprese perdite per miliardi di dollari. Gli studiosi stimano ora che i deepfake innalzeranno il livello di realismo alla richiesta di trasferimento di denaro, prevedendo che i falsi profondi saranno adottati anche per lanciare imponenti campagne di spearphishing, senza contare l'impiego volto all'affinamento delle diverse tipologie di attacco degli account mail aziendali (Business

Email Compromise, BEC): dal Bogus Invoice Scheme al CEO Fraud, dall'impersonazione di un avvocato al furto di dati, fino ai ransomfake.

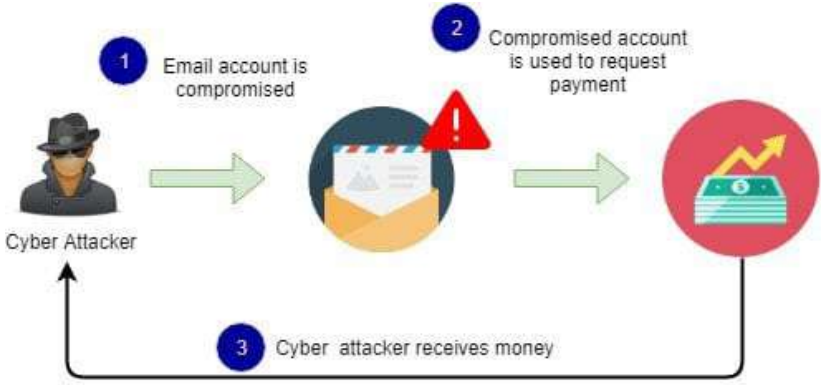


Figura 6 *"BEC Attacks: How Email Account Compromise Works", https://resources.infosecinstitute.com/bec-attacks-email-account-compromise-works/#gref*

Una criticità ulteriore è infine rinvenibile nella moltitudine di servizi disponibili in Rete per occultare l'identità di chi sta dietro ai deepfake. Per tale ragione deepfake non solo incarnano di per sé un rischio grave e reale, ma possono rappresentare un attacco scagliabile contro chiunque da un attaccante alla cui identità risulta arduo risalire, lasciando di fatto la vittima scoperta di adeguate possibilità di difesa, anche a posteriori.

Considerazioni finali: contromisure e mitigazione del rischio.

Gli analisti sono concordi nel ritenere che gli attacchi deepfake alle organizzazioni economiche saranno inevitabili, posto che individuare e bloccare i falsi profondi prima che vengano immessi e fatti circolare on line sia matematicamente impossibile. Tuttavia sussistono alcune misure che le aziende possono adottare per fronteggiare l'emergenza e attenuare l'impatto dannoso che i deepfake sono in grado di arrecar loro.

In primo luogo, i dipendenti delle aziende devono essere istruiti sui pericoli che i deepfake rivestono e su come possono essere individuati. In attesa che una soluzione tecnologica di contrasto efficace possa essere sviluppata[13] e messa a punto, le aziende non debbono affatto

[13] Nella blockchain, ad esempio, è intravista la possibilità di autenticare contenuti audio, video e audiovisivi. Si veda anche il libro bianco dei ricercatori Symnatec, Vijay Thaware e Niranjan Agnihotri, "AI Gone Rogue": Exterminating Deep Fakes Before They Cause Menace", che indaga su come l'apprendimento automatico potrebbe essere proficuamente impiegato per individuare e contrastare i deepfake. Alcuni ricercatori stanno sviluppando dei metodi per mappare la "provenienza" dei contenuti video e audio, a prescindere dal fatto che siano collegati o riconducibili a siti ritenuti affidabili. Un'altra soluzione che alcuni studiosi stanno vagliando ...*(segue)*

astenersi dal pubblicare on line contenuti multimediali dei propri dipendenti, poiché ciò comprometterebbe il rapporto col pubblico e gli azionisti, danneggiando il business, prima ancora che sia colpito da un deepfake.

Figura 7 *https://www.nist.gov/itl/applied-cybersecurity/tig/back-basics-multi-factor-authentication*

Le imprese dovrebbero quindi focalizzarsi sul rilevamento dei deepfake il più presto possibile dopo l'upload dello stesso, al fine di mitigarne gli effetti nocivi. Ciò dovrebbe avvenire attraverso la collaborazione con partner tecnologici specializzati, anche in vista delle risposte. Una volta che un deepfake fosse individuato, un'unità di crisi legata all'ufficio comunicazione con il pubblico dell'azienda potrebbe tempestivamente procedere con una strategia di contronarrazione rispetto al contenuto veicolato dal falso profondo.

In terzo luogo, anche se l'azienda può contare su una buona ciberassicurazione, è possibile che tali minacce non siano ancora ricomprese nella polizza stipulata. Il trasferimento del rischio non deve mai sostituire una solida strategia di sicurezza informatica, che deve essere

è quella di creare occhiali stampati in 3D pensati proprio per i dirigenti aziendali e che, una volta indossati consentono di eludere i meccanismi di riconoscimento facciale. Altre start-up stanno rendendo disponibile una tecnologia in grado di timbrare le immagini con una filigrana a mo' di autenticazione. L'idea potrebbe anche essere estesa all'hardware dei telefoni cellulari. Fra le misure preventive c'è chi chiede a coloro che pubblicano codice per la creazione di deepfake di sviluppare anche misure di verifica.

costantemente aggiornata ai rischi emergenti: così l'azienda dovrebbe approntare protocolli anti-deepfake, con i dipendenti formati su come poter identificare una telefonata o un video truffaldini e che sappiano aderire senza eccezioni di sorta a un processo di approvazione in due fasi, per qualsiasi richiesta di trasferimento di denaro. Fondamentale è infine l'autenticazione multifattore per l'accesso a tutti i sistemi aziendali.
In generale, le sfide che i deepfake stanno lanciando sono essenzialmente quattro e riguardano molto da vicino il settore corporate. La prima è correlata alla pronta individuazione dei falsi profondi, al momento della loro pubblicazione; la seconda è ascrivibile al fenomeno di contenuti controversi additati come deepfake, nonostante siano autentici[14].
La terza sfida guarda alla regolamentazione sulla creazione dei deepfake e, in particolare, se e quali limiti ci debbano essere e come debbano essere eventualmente posti. La quarta concerne la limitazione dei danni e la gestione dell'impatto dei deepfakes e la responsabilità per la limitazione dei danni.

Ciò che è certo è che non sia possibile ipotizzare adeguate soluzioni di contrasto ai deepfake che siano soltanto d'impronta informatica e normativa. Pensare eticamente nel processo di evoluzione e di diffusione delle nuove tecnologie risulta essere una condicio sine qua non, poiché da qui dipende la costituzione di un rinnovato senso di responsabilità a livello globale, per tutti, cittadini e imprese.

[14] Yasmine Green, il direttore di ricerca di Jigsaw Google ha coniato per tale fenomeno la definizione de "Il dividendo del bugiardo" ("The liar's dividend").

Business Continuity & Resilienza, leve fondamentali per una società sempre più globalizzata e digitalizzata

[A cura di Federica Maria Rita Livelli]

Scenario

La *Business Continuity (BC)* è una pratica imprescindibile per garantire la resilienza di qualsiasi organizzazione. Fa riferimento alla ISO 22301:2019 (recentemente revisionata), che stabilisce i requisiti per un efficiente *Business Continuity Management System (BCMS)*. Trattasi di una disciplina che trasforma l'elementare buonsenso, dagli effetti di per sé aleatori, in una calibrata immissione di sviluppi razionali, come dire in una *scienza,* che, partendo da dati di esperienze certe, conduce a risultati certi.

La ISO 22301:2019 definisce la BC come *"la capacità di un'azienda di continuare ad erogare prodotti e servizi ad un livello accettabile, a fronte di eventi avversi di ogni genere che potrebbero verificarsi"*. La BC supporta in modo continuo la costruzione ed il miglioramento del livello di resilienza delle organizzazioni. Pertanto, i *Business Continuity Plan* (BCP) – quali documenti che riportano le soluzioni di preparazione e recovery messe in atto dalle aziende - costituiscono un elemento fondamentale per garantire il successo, a lungo termine, di qualsiasi organizzazione.
Attraverso l'implementazione della BC si prende consapevolezza della congiuntura che potrebbe sopravvenire e di come prepararsi ad affrontarla, gestendo al meglio quei processi e quelle attività necessari per poter tornare a erogare prodotti e servizi critici dopo un'interruzione.

Inoltre, la ISO 22316:2017 (parte della famiglia delle ISO 22300) relativa alla Resilienza Organizzativa, definisce la Resilienza come *"la capacità di un'organizzazione di assorbire gli shock e di adattarsi ad un contesto in continua evoluzione"*.

Nel mondo attuale, altamente digitalizzato e globalizzato, è sempre più importante saper coniugare la BC e la Resilienza in modo tale da essere preparati ad affrontare qualsiasi tipo di interruzione e cambiamento. Ricordiamo, inoltre, che la norma ISO 22301:2019 è di supporto alla norma ISO 27001:2017 (riguardante il sistema di gestione della sicurezza delle informazioni) che richiede che i servizi/processi relativi alla sicurezza informatica siano posti in continuità.

È doveroso ricordare che la norma ISO 22301:2019 supporta la gestione di tutti i tipi di discontinuità o interruzioni di servizio, le cui cause non sono necessariamente solo quelle legate al blocco/indisponibilità dei sistemi informatici, nonostante il supporto informatico, nelle sue varie forme, sia altamente integrato e indispensabile in tutte le realtà aziendali.

Business Continuity & Resilienza: lo stato dell'arte

Il "*BCI Horizon Scan Report 2019*", pubblicato dal Business Continuity Institute (BCI), UK fornisce lo scenario delle principali minacce reali e percepite dalle organizzazioni a livello globale, oltre ad attestare come la BC contribuisca a sviluppare la resilienza aziendale.
Il report identifica i 10 Top Risks che caratterizzeranno i prossimi mesi: le prime quattro posizioni sono rispettivamente occupate dagli attacchi cyber e dalla violazione dei dati (per la prima volta al primo posto rispetto agli anni precedenti), dalle interruzioni sistemi IT e telecomunicazioni, dalle condizioni metereologiche e geologiche estreme (i.e. uragani, terremoti ecc.), seguiti dalle interruzioni dei servizi forniti dalle infrastrutture critiche.

Fonte: The BCI Horizon Scan Report 2019

Il tema degli attacchi cyber è quanto mai "*caldo*" ed è diventato oggetto di priorità nelle agende dei vari Board, considerando anche il fatto che gli attacchi non sembrano accennare a inversione di rotta, anzi crescono esponenzialmente. Alcune tipologie di attacchi cyber possono altresì dar luogo a blocchi dell'operatività in forma diretta o indiretta. Si pensi agli attacchi DDoS o Ramsomware, oppure alla necessità di "*isolare*" un servizio al fine di contenere una minaccia o un allargamento dell'"*infezione*" cyber. Alcuni esempi: nel 2018, l'attacco alla posta elettronica certificata ed ai sistemi informatici dei Tribunali Italiani, con paralisi di tutti i sistemi operativi che consentono il funzionamento quotidiano della giustizia civile; a luglio 2019, l'attacco alla Bonfiglioli Riduttori, con blocco della produzione e richiesta di ingente riscatto; l'attacco tra ottobre e novembre 2019 a Eurobet che ha colpito molti provider italiani creando notevoli disservizi su migliaia di siti web; a fine novembre 2019 l'attacco all'Ospedale Fatebenefratelli di Erba, le cui attività sono state congelate per giorni e più 35mila radiografie rese inaccessibili e per cui è stato richiesto; ad inizio dicembre 2019 l'attacco a Iren Ambiente, i cui siti, ma anche i numeri verdi, sono stati messi fuori uso.

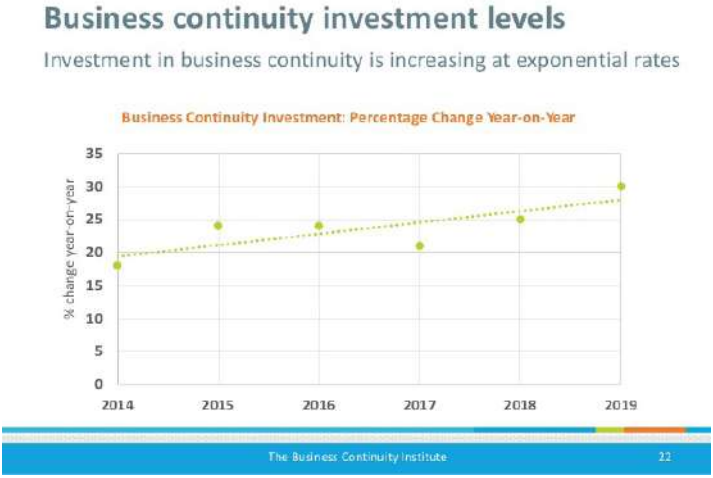
E non basta: ad accrescere le soggetti operanti, organizzazioni e istituzioni, sia aggiungono le condizioni metereologiche avverse ed i disastri naturali, così come le varie crisi socio-geopolitiche, la cosiddetta guerra dei dazi e la Brexit.

Ne consegue che si rende sempre più necessario garantire la resilienza delle organizzazioni attraverso l'implementazione di BCP e una efficiente gestione dei rischi: un necessario approccio olistico che coinvolge nel processo non solo la funzione di BC, ma anche quelle di Cyber Security, Disaster Recovery, di Crisis Management e Risk Management, nonché di Supply Chain Management, come evidenziato da circa il 61% degli intervistati per il "*BCI Horizon Scan Report 2019*", che sostiene essere fondamentale che tutti contribuiscano alla resilienza organizzativa.

Sempre secondo il suddetto report, per quanto riguarda gli impatti finanziari, i costi relativi alle interruzioni di serviti IT, nel complesso, sono quantificati in più $500 milioni all'anno.

Fonte: The BCI Horizon Scan Report 2019

Inoltre, secondo il report *"The State of Cyber Resilience 2019"* di Accenture, nei prossimi 5 anni i costi addizionali ed i mancati ricavi delle aziende, dovuti a cyber attack, a livello mondiale si stima possano raggiungere i $5.200 miliardi a fronte di una stima di 75 miliardi di dispositivi connessi ad internet.
Lo scenario altamente articolato degli ultimi anni ha comportato, negli ultimi 5 anni, un costante trend di crescita degli investimenti in BC, che sono passati da un 18% nel 2014 ad un 30% nel 2019, i.e. + 12% a testimonianza della maggior consapevolezza dei benefici derivanti dall'incorporazione dei principi indicati nel ISO 22301:2019 per contrastare minacce, rischi e crisi sempre più invasivi.



Fonte: The BCI Horizon Scan Report 2019

Come riportato dal "*BCI Organizational Resilience Report 2019*", la BC ricopre un ruolo sempre più importante unitamente al Risk Management, al Crisis Management ed alla Cyber Security. Le 5 funzioni top, determinanti per il raggiungimento della resilienza organizzativa, risultano essere la BC ed il Crisis Leadership & Management al primo posto (87,3%), seguite dalla funzione di Disaster Recovery (73,4%), dal Risk Management (72,2%) e l'Information Security (57%).

Fonte: The BCI Organizational Resilience Report 2019

Le certificazioni ISO 22301 rilasciate, secondo l'"*ISO Survey 2019*", a fine 2018, sono state n. 1506 a livello globale.
Secondo quanto riportato dal "*BCI Horizon Scan Report 2019*", solo il 14% degli intervistati risulta avere una Certificazione ISO 22301, mentre il 55% applica le linee guida dello standard senza conseguire la certificazione e il 4% intende implementare tali linee guida in futuro.
I dati rivelano come la cultura della BC non sia ancora sufficientemente diffusa, anche se si ritiene che i dati accertati siano destinati a crescere: infatti, la certificazione risulta essere sempre più un parametro richiesto per essere conformi alle cogenti normative - soprattutto dopo l'avvento dell'Industria 4.0 – per partecipare a gare pubbliche e private, come dimostrazione della capacità di garantire la continuità nella fornitura di prodotti e servizi, nella supply chain e nella logistica a fronte di incidenti ed eventi avversi.

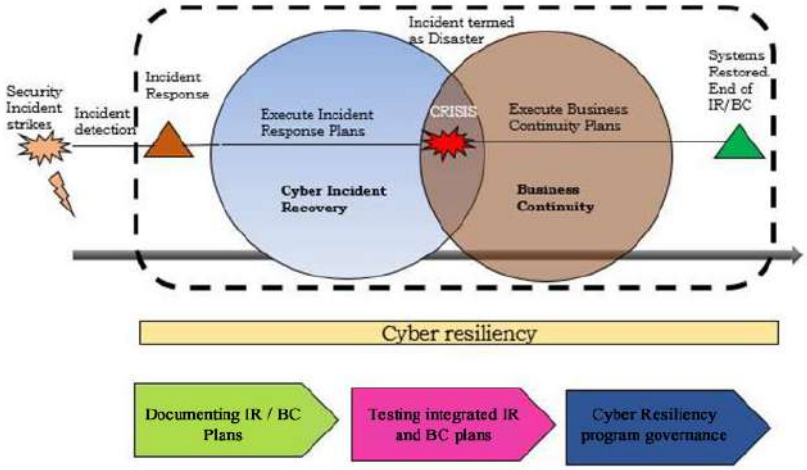
Fonte: The BCI Horizon Scan Report 2019

Business continuity & resilienza digitale: una "santa alleanza" contro i cyber crimini

IL NEMICO. Nell'attuale scenario altamente digitalizzato e globalizzato il cyber risk costituisce uno dei rischi con maggiori effetti, risiedendo nelle interconnessioni dei rischi correlati al capitale umano, al business, ai cambiamenti normativi, alla tecnologia e a quelli politici e ambientali e difficile da mitigare ed impossibile da evitare al 100%.
I cyber attack aumentano ogni anno per volume e complessità e hanno impatti economici sempre più ingenti sulle organizzazioni. Secondo il report *"Global Fraud and Risk Report"* della società di consulenza Kroll, i costi che un'organizzazione deve sostenere per la bonifica, dopo un cyber attack, possono essere molto più costosi della prevenzione, specialmente se operanti in settori altamente regolamentati come la sanità o la finanza.
La società di consulenza strategica Gartner di Stamford (Connecticut) ritiene che le interruzioni IT e i fermi macchina imprevisti possano arrivare a costare $5.600 al minuto.

LA DIFESA. Dinanzi a questo spettro inquietante, le organizzazioni devono essere in grado di affrontare gli attacchi cyber sempre più frequenti. Le organizzazioni devono essere in grado di prevenire i cyber attack per salvaguardarne l'integrità, la disponibilità e la riservatezza dei dati e garantire i processi critici.

Si rende più che mai necessario progettare un sistema di BCMS che, in caso di cyber attack, attraverso una strategica ed olistica coniugazione di piani di BC e Disaster Recovery e Crisis Management riesca ad aumentare la resilienza organizzativa dell'organizzazione.



Rappresentazione grafica di una risposta ad un incidente cyber e funzioni di Business Continuity

A tale proposito, nel "*Cost of Data Breach Report 2019*" del Ponemon Institute di Traverse City (Michigan), si evidenzia come la concertazione di cyber security e di BCMS possa contribuire a ridurre considerevolmente il tempo medio di risposta alla violazione oltre ad evitare il verificarsi di ulteriori incidenti in futuro. Pertanto, attraverso BCP ben strutturati si riesce a mantenere attive ed operative le attività aziendali riuscendo così a ridurre di circa $9, per record, i costi di data breach.

Considerando che oltre l'80% dei cyber attack sono dovuti al fattore umano, sarà sempre più necessario una "*Human Centric Cyber Security & Resilience*", per: identificare il rischio legato al comportamento degli utenti; implementare programmi adeguati di training utilizzando dinamiche ludiche, simulando attacchi al fine di sviluppare negli utenti modelli comportamentali solidi; mantenere hardware e software sempre aggiornati; gestire al meglio le proprie credenziali di accesso ai sistemi; sviluppare una cultura digitale e della cyber security non solo all'interno dell'azienda, ma anche all'esterno del perimetro aziendale (i.e. fornitori e clienti) aumentando in questo modo l'*awarness* degli attori coinvolti soprattutto a fronte di una esponenziale interconnessione e condivisione di dati digitali.

A che punto siamo in Italia?

In Italia la pratica della BC continua a diffondersi, unitamente al Risk Management, sia per garantire una maggior resilienza organizzativa sia per essere conformi alle normative vigenti ed agli standard obbligatori.

La ISO 22301:2019 e le *"Good Practices Guidelines" (GPG)* del BCI, UK sono diffuse tra le banche, gli istituti finanziari e le infrastrutture strategiche. Si sta assistendo anche ad un graduale incremento della diffusione dello standard nella Pubblica amministrazione o nelle consociate di gruppi internazionali che hanno la necessità di avere anche in Italia società certificate.

Non è disponibile al momento un censimento ufficiale aggiornato. Da quanto scaturisce dalla banca dati di Accredia, alla data del 8.11.2019, in Italia n. 78 organizzazioni hanno conseguito la certificazione ISO 22301.

In Italia è altresì difficile reperire una casistica ufficiale di buoni esempi di implementazione di BC, cosi come di casi che non hanno potuto beneficiare di un'implementazione efficace dello standard, in quanto vi è una reticenza da parte delle aziende a rendere disponibili questi dati, se non costrette per adempimenti normativi.

Interessante notare come - secondo quanto riporta la ricerca "*I Risk Managers in Italia ed in Europa*" pubblicata da ANRA nel 2019 - i risk manager italiani ritengono prioritaria la gestione dei rischi operativi relativi agli asset e alla BC, a testimonianza di un trend positivo di diffusione della cultura della resilienza e della necessità di un approccio olistico e non più per silos.

Fonte: "I Risk Managers in Italia ed in Europa" - Ricerca ANRA 2019 in collaborazione con Ferma - 2019

Conclusioni

Le organizzazioni, operanti in un sistema sempre più articolato e interconnesso, non possono più da agire come monadi, bensì devono convertirsi in un sistema articolato e pragmatico, grazie alle metodologie di BC, Resilienza, Risk Management e Cyber Security, in grado di attuare un cambio culturale contaminando le organizzazioni con la cultura della prevenzione e della pianificazione delle strategie di recupero, dimostrando come i vari BCP (i.e. *Privacy, Data Protection & GDPR, Cyber Risk, Cyber Security, Disaster Recovery, Supply chain e Logistica, ecc.*) contribuiscano a convertire le sfide in opportunità.

È dunque necessario affidarsi ad un approccio olistico che tenga in considerazione la sicurezza delle piattaforme dei sistemi usati ed adottare un *corpus* di policy sempre aggiornato, un'adeguata e costante formazione del personale, un commitment trasversale, insomma, tra tutte quelle che sono le principali funzioni aziendali.

Fonti (in ordine alfabetico)

- *Banca Dati (aggiornata al 8.11.2019) – Accredia, ITALIA*
- *BCI Good Practices Guidelines 2018 – BCI, UK*
- *BCI Horizon Scan Report 2019 – BCI, UK*
- *BCI Organizational Resilience Report 2019 – BCI, UK*
- *Cost of Data Breach Report 2019 – Ponemon Institute, USA*
- *Global Fraud and Resilience Report 2019 – Kroll, USA*
- *I Risk Managers in Italia ed in Europa – Report 2019 – ANRA, ITALIA*
- *ISO Survey 2019 – ISO, SVIZZERA*
- *The State of Cyber Resilience 2019 – Accenture, USA*

Mobile App italiane: una lente di ingrandimento sul loro stato di salute e sulle vulnerabilità più diffuse

(A cura di Luca Capacci, Alfonso Solimeo e Stefano Taino)

L'ambito mobile nell'ultimo decennio è andato sempre più imponendosi tra i principali attori nel palcoscenico informatico: la pervasività di device quali smartphone e tablet nella vita quotidiana, è sotto gli occhi di tutti. Al 2019, nel mondo, sono presenti oltre 3 miliardi di smartphone a fronte di una popolazione di circa 7.6 miliardi: in Italia, su una popolazione di circa 59 milioni di persone, sono presenti oltre 36 milioni di smartphone [1], con una crescita sul 2018 di oltre 2 milioni.

	Popolazione	Smartphone	Incidenza
Mondo	7.6 miliardi	3.2 miliardi	42.1%
Italia	59.2 milioni	36 milioni	60.8%

Tabella 1: *Incidenza degli smartphone sulla popolazione [1]*

Principale vettore di questo cambio di prospettiva sono le mobile app, le quali animano i principali sistemi operativi sul mercato, *iOS* e *Android*, rispettivamente di *Apple* e *Alphabet* (aka *Google*). I due colossi si dividono il mercato, sia mondiale che italiano: il primo occupa circa il 24% del mercato mondiale e il 25% del mercato italiano, mentre *Android* si impone per il 74% sia nel mercato mondiale che in quello italiano [2] - [3]. In questo duopolio, il sistema operativo di Cupertino offre, tramite l'*App Store*, circa 1.8 milioni di mobile app, mentre il sistema operativo made in *Google* offre, tramite il *Play Store*, circa 2.1 milioni di mobile app [4].

Lo scenario attuale

Grazie a questi numeri e all'immediatezza per la quale è possibile accedere a svariati servizi di utilizzo quotidiano tramite le mobile app, la fruizione di servizi B2C è in ascesa, così come l'utilizzo di smartphone e tablet sul luogo di lavoro, viste anche le sempre più numerose politiche BYOD (Bring You Own Device).

Dati sensibili, sia personali che aziendali (i.e. username, password, dati bancari, immagini, etc), sono quindi manipolati e utilizzati giornalmente dalle mobile app: il 60% degli endpoint che li sfrutta sono di tipo mobile [5]. In questo scenario la sicurezza delle mobile app diventa di fondamentale importanza, poiché si stima siano il principale vettore utilizzato dai cyber-criminali [6] per poter sferrare attacchi informatici a danni di persone e aziende: dalla diffusione di malware allo spionaggio industriale, passando per il furto di dati sensibili.

Il 2019 è stato un anno molto prolifico da questo punto di vista: in gennaio è stata trovata una vulnerabilità nell'app di *FaceTime*, diffusissimo servizio *Apple* per effettuare videochiamate, che permetteva di spiare i contatti chiamati, ricevendo l'audio dei loro dispositivi prima che questi potessero effettivamente rispondere [7]. *Android* non è certamente esente da questo tipo di problematiche: un'applicazione per il meteo, pre-installata su device *Alcatel* e disponibile al download sul *Play Store* (oltre 10 milioni di download), era equipaggiata con un malware, che trasferiva informazioni sensibili su server cinesi *TCL* – azienda cinese che produce gli smartphone *Alcatel* - e sottoscriveva abbonamenti a pagamento [8]. Vi sono anche stati casi che hanno colpito mobile app presenti su entrambi i sistemi operativi: emblematico il caso di *WhatsApp*, la principale app di messaggistica al mondo che conta oltre 1.5 miliardi di utilizzatori. Una vulnerabilità scoperta a maggio 2019 permetteva l'installazione di un software di sorveglianza sul dispositivo obiettivo [9]. Questi è solo una piccola parte di quanto accaduto nel solo 2019.

Attacchi informatici come quelli descritti, che utilizzano come vettore i device mobili e le mobile app, sono destinati a salire: *Symantec* ha stimato che su 36 smartphone, uno di essi ha installata un'applicazione ad alto rischio [10], mentre *RSA* in un suo report del 2018 ci conferma la rapida ascesa di frodi protratte tramite mobile app: nel 2015 erano il 7%, nel 2018 si è passati al 40%, con un incremento annuale del 16% [11].

	Mobile App	Mobile Browser	Web
2015	7%	42%	51%
2016	18%	37%	45%
2017	25%	36%	39%
2018	40%	31%	29%

Tabella 2: *Vettori per frodi informatiche [11]*

Alla luce di questi numeri e fatti di cronaca, la sicurezza delle mobile app diventa di primaria importanza.

Gli standard di sicurezza e le best practice nel settore mobile

Il settore dell'*information security* ha prestato, quindi, sempre maggiore attenzione all'ambito mobile: l'*OWASP – Open Web Application Security Project*, uno dei principali attori che si occupa di formazione e sviluppo di una cultura di sicurezza informatica, ha lanciato nel 2013 il *Mobile Security Project*, che fornisce risorse, materiale e linee guida per sviluppare e manutenere mobile app sicure. All'interno di questo progetto è stata sviluppata la *OWASP Mobile Top 10* [12], che si occupa di stilare una classifica dei principali rischi di sicurezza per le mobile app.

OWASP Mobile Top 10 2016 [12]

Ogni posizione della classifica rappresenta una potenziale classe di vulnerabilità e le caselle sono ordinate secondo la loro diffusione: per ognuna di esse è presente una descrizione generale, con esempi pratici e i principali consigli per la verifica e risoluzione. Con il tempo, la classifica è diventata uno standard *de facto* tramite il quale verificare i principali aspetti di sicurezza di una applicazione mobile.

Il settore mobile, inoltre, non è esentato dal rispettare i principali standard di sicurezza. Come il PCI-DSS [13], gestito dal *Payment Card Industry Security Standards Council*, che regola gli operatori che elaborano, trasmettono o manipolano dati di carte di credito: sin dal 2013 sono stati inclusi i device mobili, e di conseguenza le mobile app che vi girano, nello scope di compliance, tramite la pubblicazione del *PCI Mobile Payment Acceptance Security Guidelines* [14].

A livello europeo, invece, è necessario prestare attenzione al recente regolamento europeo *GDPR – General Data Protection Regulation* [15] relativo al trattamento dei dati personali, e alla direttiva europea *PSD2* [16] per la protezione dei dati finanziari: nello sviluppo, rilascio e utilizzo delle mobile app, bisogna tenere conto del rispetto degli standard coinvolti. In caso contrario, oltre ad abbassare il livello di sicurezza per l'utente e/o l'organizzazione, si rischia di incorrere in pesanti multe, come già successo a *Google*, multata in Francia per 50 milioni di euro per violazione del *GDPR* [17].

I test di sicurezza delle mobile app: equivoci e errori

I test di sicurezza diventano così un passaggio fondamentale nel ciclo di vita delle mobile app: mentre nel campo delle web application si può fare affidamento a metodologie e

strumenti rodati e affidabili, il campo mobile è relativamente nuovo e, anche a causa di ciò, sono presenti alcuni equivoci i quali possono portare ad errori nell'analisi del livello di sicurezza delle mobile app [18].

"I test di sicurezza per le Web Application sono i medesimi delle Mobile App"

Molto spesso vengono utilizzate le stesse metodologie e gli stessi test di sicurezza, sia per le web application che per le mobile app: nel primo caso bisogna ricordare la presenza del browser, necessario per l'interazione, che introduce una sorta di isolamento della web application da testare dal client. Nel caso delle mobile app, invece, deve essere considerato in aggiunta l'intero sistema operativo sottostante (i.e. Android, iOS) che può interagire con l'applicazione mobile. Altra importante differenza è sicuramente la localizzazione e la disponibilità del codice sorgente: mentre nelle web application è conservato esclusivamente sul server e l'esito della sua esecuzione viene inviato *on demand* al browser per quello che viene richiesto dal client, in una applicazione mobile esso è completamente all'interno del pacchetto che la compone, rendendo necessaria un'analisi del codice per intero. Questa fattispecie, oltre ad ampliare la superficie di test (e di attacco), vede la messa in campo di ulteriori capacità tecniche: se con le web application i test vengono eseguiti, nella maggior parte dei casi, intercettando e analizzando le comunicazioni tra il client e la web application, con le mobile app bisogna effettuare anche azioni di reverse engineering, così da avere a disposizione il codice dell'applicazione a partire dal pacchetto, e, inoltre, le comunicazioni da analizzare non sono solo basate su HTTP, ma anche su altri protocolli e tecnologie.

"I test di sicurezza statici sono sufficienti per le mobile app"

Se i test di sicurezza per le web application sono dinamici per natura, vista la necessaria interazione tra il client (i.e. browser) e la web application in azione (i.e. sito web di e-commerce), quando si parla di test di sicurezza delle mobile app, troppo spesso si pensa alla mera analisi del codice che la compone. Ma utilizzando unicamente questo approccio verrebbe a mancare l'analisi di tutto quello che riguarda i flussi di dati in movimento: con un approccio dinamico, basato su test di sicurezza con la mobile app in esecuzione, si riescono a determinare anche vulnerabilità che possono essere dovute a comunicazioni di rete con il backend o a flussi di dati in percorsi non visitabili staticamente.

"Le mobile app sono testate e verificate da Apple e Google, quindi sono sicure"

Apple e Google prima di pubblicare le mobile app sui rispettivi store effettuano dei controlli. Questi però mirano soprattutto a controllare il rispetto dei termini di uso dell'ecosistema messo a disposizione dello sviluppatore: dalle API dei sistemi operativi fino ai Framework di sviluppo, passando per il regolamento degli store. Eventuali problemi di data leakage o privacy, vulnerabilità di componenti terze o dovute a comportamenti dinamici dell'applicazione, non vengono presi in considerazione. Sono molti, infatti, i casi di mobile app malevole e vulnerabili pubblicate sugli store i.e. [8].

Metodologie e pattern ad-hoc

Alla luce di queste considerazioni, si può affermare che nei test di sicurezza delle mobile app è necessario applicare delle metodologie e dei pattern appositi: bisogna prevedere sì un'analisi statica, ma bisogna accompagnarla ad un'analisi dinamica, in modo tale da esplorare tutte le eventualità e tutti i comportamenti. Approcciando la sicurezza delle mobile app, quindi, bisogna realizzare che si ha di fronte un'architettura complessa e che abbraccia svariate tecnologie e competenze: solo con questa visione si può realmente testare una mobile app.

Le Mobile App italiane e la sicurezza

Anche le aziende e le organizzazioni italiane hanno cominciato ad aggredire il mercato delle mobile app in maniera più decisa, permettendo così un accesso ai servizi offerti anche da mobile.

Basti pensare che le aziende *incumbent* italiane offrono sugli store una media di 3.7 mobile app, contro le 3.5 delle aziende operative negli U.S.A.: le aziende di telco arrivano a proporre 12 mobile app. Inoltre, il 48% di queste aggiunge funzionalità rispetto al classico sito web dell'azienda, mentre nel 20% dei casi si possono sfruttare funzionalità completamente diverse. Se si considera poi che il 43% permette di effettuare acquisti, mentre il 17% di effettuare pagamenti remoti, con la quasi totalità di esse che sfrutta le peculiarità del mobile (i.e. geolocation, notifiche push, biometria, etc.) [19] ecco che si rendono necessarie, per la sicurezza delle mobile app, le metodologie e i pattern dedicati.

La composizione delle mobile app di aziende italiane

Analizzando le più popolari mobile app, in termini di download, di aziende italiane sui due maggiori store, notiamo che si ha una situazione molto variegata: la maggior parte appartiene al mondo *Finance* – i.e. banche, pagamenti elettronici, etc. - su entrambi gli store (33% delle mobile app), mentre il secondo posto, nel mondo Android è occupato dal settore *Gambling* – i.e. lotterie, scommesse, etc. – con il 12% delle mobile app, nel mondo iOS è occupato dal settore *Shopping* con l'11% delle mobile app.

	Android	iOS
App Native	147	71
App Ibride	64	52
TOT	211	123

Tabella 3: *Campione mobile app più popolari, in termini di download, afferenti aziende italiane Fonte: CryptoNet Labs s.r.l.*

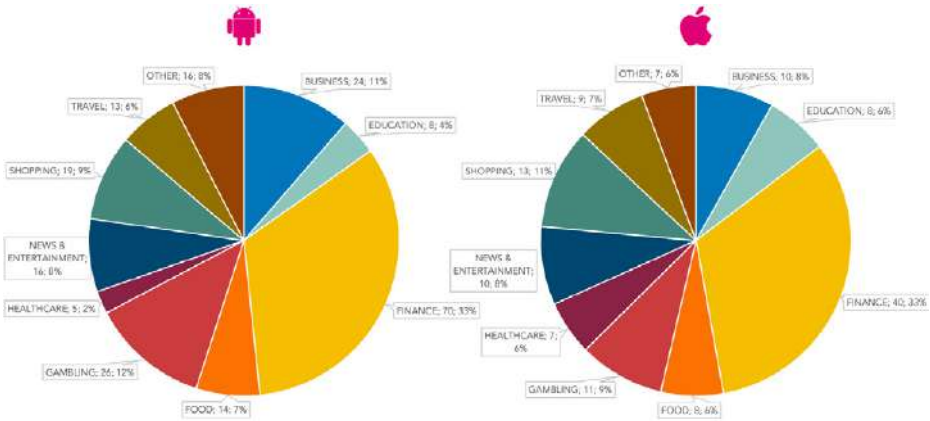


Grafico 1: *Settori commerciali delle più popolari mobile app di aziende italiane. Fonte: CryptoNet Labs s.r.l.*

Il settore Gambling va invece ad occupare il terzo posto nel mondo iOS con il 9% delle mobile app, mentre in Android troviamo il settore Business – i.e. servizi logistici, servizi postali, servizi professionali, etc. – con l'11% delle mobile app. Gli altri settori occupati da aziende italiane possono essere osservati nel **Grafico 1**.

Le vulnerabilità riscontrate

Sono varie le tipologie di vulnerabilità riscontrate nelle mobile app più popolari: si va dal data leakage, tramite il quale è possibile carpire dati sensibili, all'utilizzo di comunicazioni insicure (e.g. non cifrate) passando per un *encryption* debole mediante l'uso di cifrari considerati ormai obsoleti. Nella tabella successiva si può osservare la tassonomia analizzata circa le vulnerabilità.

Categoria	Vulnerabilità	
Data leakage	Sensitive data stored in the private folder of the mobile app: - Username - Password - Token Token disclosed via SharedPreference AllowBackup flag is not false or UIFileSharingEnabled flag set to True	Internal IP address leakage External data storage Apache Cordova CVE-2016-6799, CVE-2014-3502, CVE-2014-1881, CVE-2014-1882 World readable files Public Shared Preferences iOS storage protection level mis-configured
Reverse engineering	Lack of obfuscation	
Tampering	Lack of root / jailbreak detection Unused requested permissions Android APK certificate signed with key shorter than 2048 bits	Stack Smashing Protection (SSP) not enabled Automatic Reference Counting (ARC) not enabled Apache Cordova CVE-2017-3160, CVE-2015-1835, CVE-2014-3500
Insecure Communication	Insecure HTTP URLs detected Insecure HostnameVerifier Insecure TrustManager App Transport Security mis-configured ATS allows TLS 1.0 or 1.1	Ciphers not supporting Perfect Forward Secrecy (PFS) allowed Apache Cordova CVE-2015-5256, CVE-2014-3501, CVE-2015-5207, CVE-2015-5208, CVE-2012-6637
Weak Encryption	Insecure DES cipher Insecure MD2, MD4, MD5 hash algorithm Insecure SHA-1 hash algorithm Insecure ECB encryption mode	Insecure RC4 cipher Predictable random data generation Apache Cordova CVE-2015-8320

Tabella 4: *Tassonomia delle vulnerabilità riscontrate Fonte: CryptoNet Labs s.r.l.*

Nel **Grafico 2** possiamo osservare come queste vulnerabilità sono distribuite sui due sistemi operativi: in Android la maggior parte delle vulnerabilità riguardano il *Tampering* – colpito il 98% delle mobile app – e il *Data Leakage* – colpito il 94% delle mobile app. In iOS, invece, le principali vulnerabilità riguardano l'utilizzo di *Comunicazioni Insicure* (91% delle

mobile app) e di una *Encryption Debole* (89% delle mobile app).
Sebbene non vi siano categorie che possono essere considerate al sicuro, visto le alte percentuali, si nota che vulnerabilità afferenti al *Tampering* e al *Data Leakage* risultano essere le meno diffuse su iOS (63% e 70%), mentre in Android risultano essere le vulnerabilità appartenenti a *Comunicazioni Insicure* e *Reverse Engineering* (36% e 61%).

Grafico 2: *Diffusione delle vulnerabilità per tipologia Fonte: CryptoNet Labs s.r.l.*

Effettuando un focus sui singoli sistemi operativi possiamo notare come i tre settori più rappresentati in Android – Finance, Gambling e Business – hanno la percentuale minore di vulnerabilità riscontrate nella tipologia *Comunicazioni insicure* (Grafico 3), lasciando intendere una discreta attenzione sui protocolli e le procedure utilizzati nel trasmettere dati. D'altro canto, però vi sono problemi nel trattare dati sensibili sul dispositivo stesso, infatti le percentuali di vulnerabilità trovate crescono se si va ad analizzare la tipologia *Data Leakage*. In iOS (Grafico 4), invece, i tre settori più rappresentati – Finance, Shopping e Gambling – vedono la miglior performance nella tipologia *Tampering*, mentre la situazione peggiora per le vulnerabilità di tipo *Comunicazioni insicure* (Finance e Gambling) ed *Encryption debole* (Shopping).

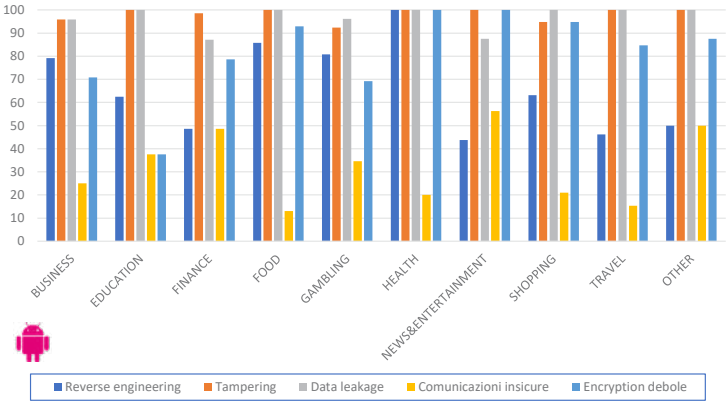


Grafico 3: *Diffusione delle vulnerabilità per tipologia e settore - Android Fonte: CryptoNet Labs s.r.l.*

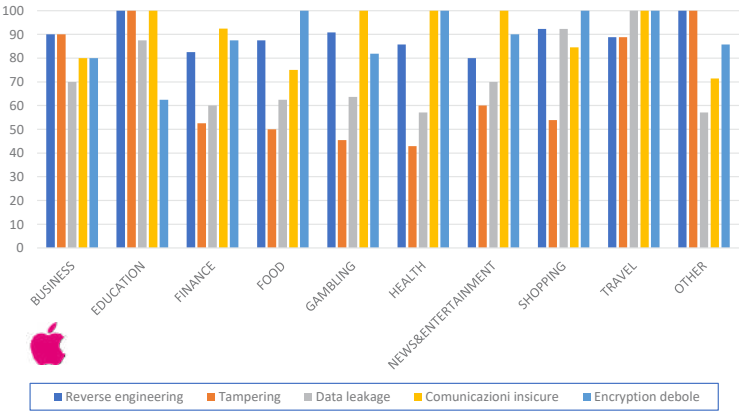


Grafico 4: *Diffusione delle vulnerabilità per tipologia e settore - iOS Fonte: CryptoNet Labs s.r.l.*

Un altro interessante punto di lettura è sicuramente la percentuale di presenza di vulnerabilità riconducibili alla OWASP Mobile Top Ten 2016, che possiamo osservare nel Grafico 5. Si può subito evincere come la tipologia di vulnerabilità più diffuse coincida per entrambe le piattaforme: le mobile app di aziende italiane, quindi, non fanno eccezione e risulta che la maggior parte delle problematiche di sicurezza riscontrate appartengano alla

categoria individuata come principale dalla OWASP Mobile Top Ten, ossia *Improper Platform Usage*, un utilizzo errato della piattaforma e delle funzionalità messe a disposizione.

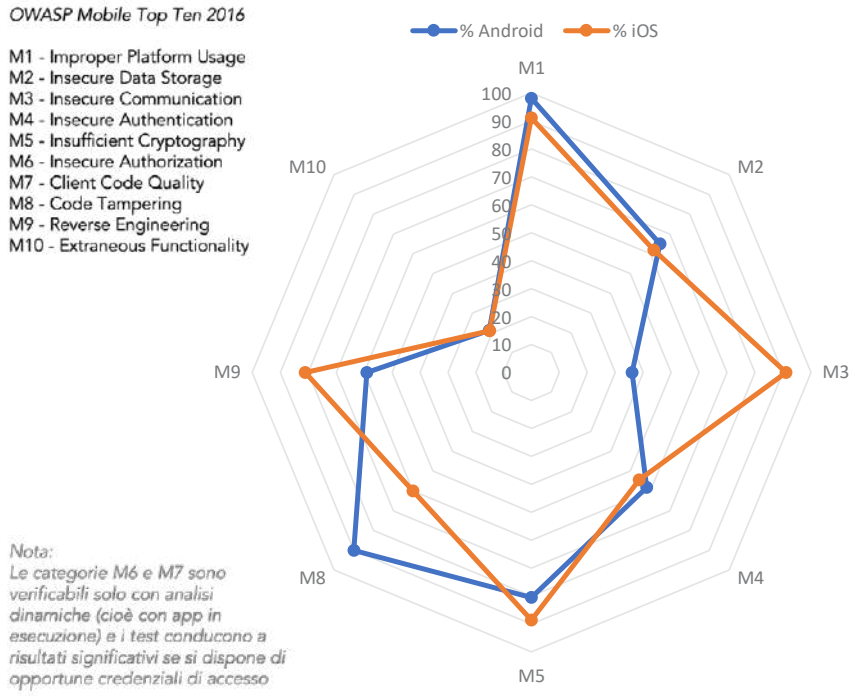


Grafico 5: *Diffusione delle vulnerabilità per categorie OWASP Fonte: CryptoNet Labs s.r.l.*

Conclusioni

Le mobile app necessitano di un paradigma personalizzato per testarne la sicurezza: le categorie utilizzate fino ad ora per le web application non riescono e non possono abbracciare le peculiarità del mondo mobile. L'Italia segue i trend mondiali e in alcuni casi li anticipa, spostando molto del traffico e delle funzionalità dai classici siti web verso le mobile app: quest'ultime sono sempre più protagoniste nel fornire i servizi delle aziende.

Infatti, ormai tutte le principali aziende italiane, in tutti i settori, utilizzano una o più mobile app per interagire con i loro clienti ed è quindi necessario porre una sempre maggiore attenzione sulla sicurezza di queste mobile app, le quali manipolano dati personali, da dati inerenti alla persona fino a dati finanziari. Le vulnerabilità riscontrate ci dicono innanzitutto che i punti di attenzione, e quindi le competenze e le tecnologie, devono essere diversi a seconda del sistema operativo utilizzato, poiché quanto trovato su Android non sempre tro-

va corrispondenza in iOS e viceversa: conferma anche il fatto che la presenza di un intero sistema operativo con cui interagire, cambia radicalmente lo scenario rispetto ad una web application.

Gli standard di sicurezza possono senza dubbio fornire degli utili indicatori nella ricerca di vulnerabilità: l'OWASP Mobile Top Ten ci fornisce una cartina tornasole, più che mai reale, su quali siano le maggiori vulnerabilità presenti nel panorama mobile. Ma ormai non deve essere più finalizzata solamente ad un esercizio tecnico e così come tutti gli standard prettamente tecnici, devono indirizzare verso la compliance di standard e regolamenti, come il PCI-DSS e il GDPR, i quali, in caso di non rispetto, hanno una pesante ricaduta sull'azienda, sia in termini di immagine che in termini di multe, e sull'utente. Per questo motivo, i test di sicurezza delle mobile app devono necessariamente entrare nel loro ciclo di vita.

Lo stato di salute delle mobile app del panorama italiano evidenzia come vi siano ancora molti problemi in ambito *security*, ma anche di come questo possa essere ritenuto fisiologico in un settore che sta crescendo molto velocemente. Per recuperare terreno sul campo della sicurezza delle mobile app, è necessario introdurre nuove capacità tecniche verticali all'interno del ciclo di sviluppo, e fare sì che la sicurezza nel mondo mobile, con le sue nuove metodologie e i suoi nuovi pattern, venga messa in campo sin dall'inizio del ciclo di sviluppo.

Bibliografia

[1] Newzoo, «Newzoo Global Mobile Market Report 2019,» 2019. [Online]. Available: https://newzoo.com/insights/trend-reports/newzoo-global-mobile-market-report-2019-light-version/.

[2] S. G. Stats, «Mobile Operating System Market Share Worldwide,» 2019. [Online]. Available: https://gs.statcounter.com/os-market-share/mobile/worldwide.

[3] S. G. Stats, «Mobile Operating System Market Share Italy,» 2019. [Online]. Available: https://gs.statcounter.com/os-market-share/mobile/italy.

[4] Statista, «Number of apps available in leading app stores as of 3rd quarter 2019,» 2019. [Online]. Available: https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/.

[5] Zimperium, «State of Enterprise Mobile Security Report,» Zimperium, 2019.

[6] Pradeo, «Mobile Security Report,» Pradeo, 2019.

[7] ZDNet, «Severe vulnerability in Apple FaceTime found by Fortnite player,» 30 Gennaio 2019. [Online]. Available: https://www.zdnet.com/article/apple-facetime-exploit-found-by-14-year-old-playing-fortnite/.

[8] TechRadar, «Pre-installed malware discovered on Alcatel smartphones,» 19 Febbario 2019. [Online]. Available: https://www.techradar.com/news/pre-installed-malware-discovered-on-alcatel-smartphones.

[9] M. Srivastava, «WhatsApp voice calls used to inject Israeli spyware on phones,» Financial Times, 14 Maggio 2019. [Online]. Available: https://www.ft.com/content/4da1117e-756c-11e9-be7d-6d846537acab?segmentid=acee4131-99c2-09d3-a635-873e61754ec6.
[10] Symantec, «2019 Internet Security Threat Report,» 2019. [Online]. Available: https://www.symantec.com/security-center/threat-report.
[11] RSA, «RSA QUARTERLY FRAUD REPORT: Q2 2018,» 2018. [Online]. Available: https://www.rsa.com/en-us/offers/rsa-fraud-report-q218.
[12] OWASP, «OWASP Mobile Top 10,» [Online]. Available: https://www.owasp.org/index.php/OWASP_Mobile_Top_10#tab=Main.
[13] P. S. S. Council, «Protezione congiunta del futuro dei pagamenti,» [Online]. Available: https://it.pcisecuritystandards.org/minisite/env2/.
[14] PCI, «PCI Mobile Payment Acceptance Security Guidelines,» Febbraio 2013. [Online]. Available: https://www.pcisecuritystandards.org/documents/Mobile_Payment_Security_Guidelines_Merchants_v1.pdf.
[15] G. u. d. Europea, «Testo del GDPR,» [Online]. Available: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32016R0679.
[16] G. u. d. Europea, «Testo PSD2,» [Online]. Available: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32015L2366&from=EN.
[17] P. Tarsitano, «Sanzione GDPR a Google, monito per le aziende italiane: ecco perché,» Cybersecurity360, 22 Gennaio 2019. [Online]. Available: https://www.cybersecurity360.it/news/sanzione-gdpr-a-google-monito-per-le-aziende-italiane-ecco-perche/.
[18] A. Snyder, «Debunking the Top 3 Myths About Mobile Application Security Testing,» NowSecure, [Online]. Available: https://www.nowsecure.com/blog/2019/07/24/debunking-the-top-3-myths-about-mobile-application-security-testing/.
[19] O. D. I. -. P. d. Milano, «Mobile App: l'offerta delle principali aziende incumbent e dei pure player digital in Italia,» Politecnico di Milano, 2019.

Sicurezza nel settore sanitario – Perché gli ospedali sono così violabili?

[A cura di Filip Truță, Bitdefender]

Come la maggior parte degli altri settori, quello sanitario soffre di un'eccessiva fiducia nelle proprie capacità di eludere le minacce informatiche. Ottenere una certa resilienza informatica nel settore sanitario sta rapidamente diventando una questione di vita o di morte, con una nuova ricerca[1] che illustra come gli ospedali che hanno subito attacchi ransomware abbiano anche sperimentato un aumento degli attacchi di cuore fatali.
Dal 2005, gli hacker hanno sottratto più di 300 milioni di cartelle cliniche, andando a colpire circa un consumatore su 10 per quanto riguarda l'assistenza sanitaria, in base alla Black Book Market Research[1]. Gli studi mostrano anche che un terzo di tutte le violazioni di dati segnalate riguarda l'assistenza sanitaria, più di qualsiasi altro settore. La ragione è piuttosto semplice. Le cartelle cliniche sono il tipo di dati sottratti più prezioso venduto sul Dark web, con acquirenti disposti a pagare fino a centinaia di dollari per una singola cartella. Infatti, in questi preziosi file si trovano codici fiscali, informazioni personali identificabili, dati finanziari e altri dettagli molto preziosi e utilizzabili per furti d'identità e frodi.
Negli ultimi tempi, ransomware ed estorsioni sono diventati i tipi di attacco più frequenti contro gli ospedali. Gli istituti medici non possono permettersi tempi di inattività quando ci sono in gioco le vite dei pazienti, perciò sono disposti spesso a pagare il riscatto in cambio delle chiavi per sbloccare i propri sistemi e dati medici. I criminali informatici lo sanno e ovviamente sfruttano la cosa a proprio vantaggio. Ma la domanda è perché gli ospedali sono così violabili? Per rispondere, dobbiamo prima comprendere com'è formata l'infrastruttura di una struttura sanitaria.

L'anatomia di una struttura sanitaria

Il numero di dispositivi medici connessi, sistemi e applicazioni in una grande unità sanitaria è sbalorditivo, infatti, può includere desktop, server, terminali informatici ai letti, dispositivi di diagnostica per immagini, chioschi self-service, dispositivi medici impiantabili, sistemi di cartelle cliniche elettroniche (EHR), software di gestione, sistemi PACS (sistema di archiviazione e trasmissione di immagini), sistemi di fatturazione medica, portali per i pazienti, impieghi cloud pubblici e tantissimi altri sistemi datati a cui i medici si affidano per salvare vite umane. Questa vasta gamma di dispositivi, sistemi e applicazioni crea un'enorme superficie di attacco. Molti di loro non possono essere dotati di difese tradizionali (ad esempio, un antivirus), mentre i team IT sono spesso riluttanti a impiegare i più recenti fix di sicurezza per paura di rompere il dispositivo o impedirne l'utilizzo. Ciò crea un circolo vizioso che gli aggressori hanno imparato a sfruttare con un appetito sempre insaziabile.
Un esempio lampante, lo scorso anno gli autori di ransomware hanno infettato centinaia

[1] https://finance.yahoo.com/news/healthcare-data-breaches-costs-industry-130000324.html

di studi medici e dentistici prendendo di mira due soli fornitori di servizi IT. Gli ospedali che esternalizzano i propri servizi di EHR sono estremamente sensibili a quello che viene chiamato un "attacco alla catena di approvvigionamento", in cui gli hacker raggiungono la propria vittima per comprometterne la rete attraverso i partner della sua catena di approvvigionamento. In questo modo sono state violate persino organizzazioni più preparate dal punto di vista informatico. In base al National Institute of Standards and Technology (NIST)[2], gli autori delle minacce puntano intenzionalmente ai fornitori più piccoli per sfruttare l'anello di collegamento più debole.
Sfortunatamente, investire in qualcosa che non genera profitti non è una priorità dei direttori ospedalieri. Il presidente della Black Book Market Research, Doug Brown, ha evidenziato che i budget ristretti nel settore sanitario, nonché l'onere dei sistemi datati, hanno ostacolato le capacità di molti nel settore di investire nelle proprie difese.
"Per gli ospedali, sta diventando sempre più difficile trovare dollari da investire in qualcosa che non genera profitti", ha dichiarato[3] Brown.

Gli incidenti informatici sanitari sono molto costosi

Gli incidenti informatici costano più all'assistenza sanitaria che per qualsiasi altro settore. Ogni cartella clinica persa o rubata può costare oltre 400 dollari a un'unità sanitaria, rendendo quindi un attacco informatico di successo piuttosto costoso. Perché, allora, non investono nelle garanzie necessarie? Come Richard Clarke, il consigliere speciale del presidente per la sicurezza informatica, ha dichiarato agli esperti di sicurezza alla RSA Conference nel 2002, "Se spendi di più per il caffè che per la sicurezza informatica, sarai hackerato. Inoltre, ti meriti di essere hackerato."
Clarke, ovviamente, aveva ragione. Oltre all'immensa superficie d'attacco, la mancanza di una leadership dedicata alla sicurezza nelle unità sanitarie costituisce un altro ostacolo per la sicurezza sanitaria. Inoltre, in un ospedale è difficile trovare un Chief Information Security Officer. E il personale medico è notoriamente poco preparato in materia di sicurezza informatica. Ecco perché è più facile per un aggressore ingannare un dipendente ignaro con una semplice truffa di phishing piuttosto che cercare di violare le difese di una rete ben protetta.

La carenza di competenze in materia di sicurezza informatica

Una mancanza di proattività nella sicurezza informatica mette ulteriormente a rischio le organizzazioni sanitarie. In genere, le strutture mediche rispondono alle violazioni, ma non adottano misure per prevenirle.
Una grande sfida in questo senso è la carenza di competenze in materia di sicurezza informatica, che riguarda praticamente tutti i settori, non solo l'assistenza sanitaria. Trovare, ingaggiare e trattenere dipendenti con le competenze necessarie è difficile e costoso.

---

2 https://csrc.nist.gov/publications/detail/nistir/8276/draft

3 https://finance.yahoo.com/news/healthcare-data-breaches-costs-industry-130000324.html

Poi c'è il problema delle minacce interne. Uno degli errori più frequenti che i dipendenti commettono è l'invio di documenti riservati a destinatari errati.
I dipendenti possono anche trasferire documenti di lavoro su e-mail personali, caricarli su siti di condivisione dei file o copiarli su unità rimovibili, come chiavette USB, non solo riflettendo una scarsa attenzione in termini di sicurezza informatica, ma infrangendo anche la legge (se si pensa a regolamenti come HIPPA e GDPR). Ancora peggio, i rapporti mostrano che il personale medico è facilmente vittima di truffe di phishing, il vettore di attacco preferito dagli hacker.
In realtà, la carenza di competenze può anche andare oltre a questa prima linea di difesa. Anche gli amministratori di sistema possono commettere degli errori. Configurazioni di sistema errate, gestione delle patch poco attenta e l'uso di nomi utente e password predefiniti sono tra gli errori più comuni.
Fornire una formazione di base sulla sicurezza informatica ai dipendenti è un buon inizio per alleviare alcuni dei problemi. I fornitori e distributori di servizi sanitari potrebbero fare un ulteriore passo e offrire una formazione sulla sicurezza agli operatori di tecnologia interni interessati a tale carriera, lavorare con università locali e formare amministratori, sviluppatori e altre figure professionali in aree che possano influire direttamente sulla sicurezza, come la gestione delle configurazioni per gli amministratori e pratiche di sviluppo sicure per gli sviluppatori.

Trovare una cura alla cyber-malattia dell'assistenza sanitaria

Gli istituti sanitari hanno molte opzioni per colmare non solo le lacune di competenze umane, ma anche dotare le infrastrutture della tecnologia necessaria per difenderle dai pericoli sia dall'esterno che dall'interno.
La prima cosa da fare per le organizzazioni sanitarie è analizzare completamente la propria rete per identificare ogni dispositivo e applicazione che possa fungere da punto di accesso. Mantenere un inventario ed eseguire audit regolari è assolutamente obbligatorio nel mondo connesso di oggi.
Seconda cosa, implementare controlli di sicurezza per monitorare chi ha accesso ai dati delle informazioni dei pazienti. Il controllo dell'accesso ai dati dei pazienti e la limitazione di tale accesso in base alle necessità sono estremamente importanti per garantire che i dati dei pazienti non finiscano nelle mani sbagliate. È anche importante gestire e monitorare i privilegi degli utenti finali, eseguire controlli in background sulle attività online di un dipendente prima di garantirne gli accessi e usare meccanismi di segregazione della rete per un miglior controllo e sicurezza.
Parlando di sicurezza della rete, Network Traffic Analytics eccelle nel proteggere l'Internet of Medical Things (IoMT) e altre applicazioni mediche specializzate, poiché fornisce una visibilità completa sull'intera infrastruttura. Una distribuzione NTA ideale utilizza l'apprendimento automatico e l'analisi comportamentale con approfondimenti derivanti dalle informazioni cloud sulle minacce per rilevare minacce per ogni entità, gestite o non gestite, per il traffico di rete cifrato o non cifrato.

Conformità

Quando si tratta di proteggere i dati dei clienti, le istituzioni sanitarie devono rispettare non solo le disposizioni generali, come il Regolamento generale sulla protezione dei dati (GDPR) dell'Unione Europea e il California Consumer Privacy Act (CCPA) degli Stati Uniti, ma anche le proprie normative incentrate sull'assistenza sanitaria, come l'Health Insurance Portability and Accountability Act (HIPAA) e l'Health Information Technology for Economic and Clinical Health Act (HITECH).

I requisiti HIPAA/HITECH per la privacy e la sicurezza coprono una vasta gamma di aree tecnologiche all'interno delle organizzazioni sanitarie, tra cui siti web, dispositivi medici, cartelle cliniche elettroniche e sistemi di archiviazione e trasmissione delle immagini (PACS).

Nessuna singola tecnologia può soddisfare tutti i requisiti di conformità che gli ospedali devono affrontare oggigiorno. Tuttavia, può essere una buona idea usare soluzioni facilmente flessibili, impiegare un'architettura di contenitori virtuali e operare su una qualsiasi piattaforma di virtualizzazione, accelerando l'impiego. Consolidando il controllo di sicurezza su endpoint fisici, virtualizzati e mobile attraverso una console di gestione unificata, le attività possono essere semplificate, eliminando le singole soluzioni. L'impiego e la gestione della protezione per endpoint fisici, virtualizzati e mobile devono essere semplificati attraverso l'integrazione con importanti servizi di virtualizzazione e gestione delle directory.

Sarebbe quindi ottimale equipaggiare il proprio dipartimento IT di un firewall a due vie, un rilevamento delle intrusioni, un sistema di anti-phishing, un filtro web e un controllo utente e web per bloccare minacce sempre più diversificate contro i sistemi degli utenti finali e gli endpoint dei server. La soluzione deve supportare un'adozione controllata delle policy di bring-your-own-device (BYOD), applicando la sicurezza in modo coerente su tutti i dispositivi degli utenti finali. Di conseguenza, è possibile controllare anche i dispositivi mobile e proteggere le informazioni aziendali sensibili archiviate su di essi.

Infine, la soluzione dovrebbe rispondere ai requisiti HIPAA per garantire la protezione dai malware e mantenere l'integrità delle informazioni sulla salute personale (PHI) tramite una protezione anti-virus, anti-malware e web. Ciò consente alle organizzazioni di rispettare le regole di sicurezza, permettendo l'implementazione e l'applicazione di policy di sicurezza a livello aziendale, nonché il rilevamento, il monitoraggio e la correzione degli incidenti di sicurezza. Data l'estrema importanza della sicurezza delle informazioni per motivi che vanno oltre la semplice conformità normativa, le organizzazioni devono sviluppare una strategia di sicurezza che sia completa e affidabile. Questi strumenti sono elementi vitali di tale strategia.

Tendenze IT che avranno un impatto sui professionisti italiani nel 2020[1]

[A cura di Maurizio Taglioretti, Netwrix]

Nell'ottobre del 2019 Netwrix ha condotto un sondaggio online con 1.045 professionisti IT a livello globale circa i loro progetti IT più attesi per il 2020. Ciascun rispondente ha selezionato fino a cinque principali priorità IT dall'elenco predefinito, con la possibilità di aggiungere le proprie priorità. Questo articolo presenta i risultati principali per le aziende italiane.

Tendenze che influenzeranno le aziende italiane nel 2020

Riportiamo ora le principali tendenze che avranno un'influenza sulle scelte delle aziende italiane nel 2020, come emerso dal sondaggio.

1. Le aziende cercheranno di misurare l'efficacia della cibersicurezza conducendo regolari report e KPI (indicatori chiave delle prestazioni).

Man mano che le aziende scelgono di destinare maggiori risorse alla sicurezza dei dati, i consigli di amministrazione pretenderanno che tali investimenti svolgano un duplice compito: migliorare la sicurezza delle risorse informative e guidare l'azienda, aumentando la produttività degli utenti o riducendo la spesa per le operazioni legali e di conformità. Richiederanno metriche specifiche e report periodici per dimostrare che questi obiettivi sono stati raggiunti. Pertanto, i CIO e CISO dovranno cimentarsi nello sviluppo di metriche di sicurezza al fine di monitorarne il successo e fornire al consiglio report significativi e utili. Per presentare queste informazioni in modo efficace, avranno bisogno non solo di conoscenze tecniche, ma anche di notevoli capacità comunicative e disponibilità finanziaria.

2. La riservatezza dei dati diventerà una necessità per tutte le aziende, indipendentemente dal settore, che guiderà la creazione di nuovi servizi alle imprese.

Nel 2020 la privacy dei dati diventerà una priorità per un numero ancora più elevato di aziende in tutto il mondo. Ad esempio, gli stati degli Stati Uniti adotteranno norme sulla privacy simili al GDPR e al CCPA, che alla fine si tradurranno in un regolamento federale che non escluderà nessuna azienda.

Poiché le leggi sulla privacy dei dati richiedono il consenso per la raccolta di questi e vietano la raccolta di una quantità di dati maggiore del necessario, o la conservazione di questi per un periodo di tempo più lungo del dovuto, si ripercuoteranno drasticamente sulle pratiche di marketing, raccolta e conservazione dei dati.

Pertanto, i CIO e i CISO dovranno ottenere una conoscenza più approfondita dei dati rac-

1 I dati riportati in questo articolo sono tratti da Netwrix 2020 IT Trends Report (https://www.netwrix.com/2020ittrendsreport.html)

colti, del luogo in cui vengono archiviati e del modo in cui vengono utilizzati dai dipendenti. Di conseguenza, il mercato vedrà nuove offerte, che combinano insieme servizi legali e IT, per aiutare le aziende a comprendere i vari obblighi di conformità e sviluppare piani attuabili per ottenere, conservare e dimostrare la conformità.

3.Le aziende avranno difficoltà a soddisfare le richieste di accesso ai dati, ma inizialmente saranno poche le conseguenze dovute a inosservanza.

Con l'entrata in vigore del GDPR, nel 2020, le aziende saranno messe alla prova per soddisfare le richieste di accesso ai dati (DAR) entro il periodo di tempo richiesto (30 giorni). Poiché la localizzazione di tutti i dati associati a un individuo può essere un compito piuttosto complesso, le aziende che hanno già ricevuto frequenti reclami da parte dei consumatori correranno il rischio, particolarmente elevato, di essere bombardate da richieste di accesso ai dati se i consumatori si presenteranno in massa per trarre vantaggio dalla nuova normativa. Tuttavia, le autorità devono ancora stabilire i processi per stabilire se le aziende hanno effettivamente fornito o cancellato tutte le informazioni relative a una richiesta di accesso ai dati (DAR), quindi inizialmente l'attuazione risulterebbe troppo complessa. Tuttavia, poiché le normative sulla privacy sono soggette a modifiche, le aziende dovranno effettivamente vedersi applicate delle sanzioni per non aver rispettato i DAR. Pertanto, i CIO e i CISO dovranno stabilire metodi efficienti per compiere le ricerche di dati, al fine di ridurre al minimo i rischi di multe, azioni legali e danni alla reputazione dell'azienda.

4. Le aziende renderanno la formazione sulla sicurezza parte integrante delle responsabilità professionali dei dipendenti.

Molte aziende prevedono di aumentare i servizi di formazione e consulenza sulla sicurezza informatica. Per giustificare l'aumento del budget, i CIO e i CISO saranno chiamati a dimostrare alla proprietà che questo percorso formativo è efficiente ed efficace. Di conseguenza, è preferibile che coinvolgano tutto il personale direttivo dell'azienda (dirigenti e quadri) per garantire che il contenuto e le metodologie della formazione corrispondano alle esigenze dei vari gruppi di dipendenti. Ciò significa che la questione della sicurezza non riguarderà più esclusivamente il team responsabile della sicurezza. In effetti, man mano che cresce e si diffonde l'importanza dell'educazione alla cibersicurezza degli utenti finali, le aziende confronteranno tra loro le prestazioni dei diversi team interni all'azienda. Se questa rivalità determinerà alcuni miglioramenti nel comportamento degli utenti, alla fine i responsabili dei settori di attività (LoB) avranno delle metriche di sicurezza per i loro dipendenti collegate al loro compenso come strumento per ridurre la superficie di attacco dell'intera azienda.

5. La carenza di competenze IT accrescerà l'urgenza dell'automazione.

Per supportare le crescenti esigenze aziendali, i team IT dovranno migliorare la loro efficienza ed efficacia. Per migliorare cercheranno di trovare tecnologie quali l'automazione dei processi tramite Robotic Process Automation (RPA) per sem-

plificare le attività di routine, compresi vari processi di sicurezza e conformità. Ovviamente le aziende hanno sempre cercato di automatizzare le attività di routine. Ma la grave carenza di personale IT con esperienza che occupa posti di lavoro inerenti la sicurezza conferma l'urgenza. I CIO e i CISO esamineranno in maniera più ponderata gli strumenti di automazione per liberare le risorse IT, così da potersi dedicare alla perenne necessità di proteggere l'azienda e i suoi dati.

6. Le soluzioni basate sull'intelligenza artificiale diventeranno un nuovo obiettivo per gli attacchi e le aziende faranno fatica a difendersi.

Man mano che le aziende implementano soluzioni basate sull'intelligenza artificiale (AI) e sull'apprendimento automatico (ML), gli avversari prenderanno di mira quei sistemi. Le aziende cercheranno soluzioni per proteggere i propri sistemi, in particolare quelli coinvolti in processi operativi o decisionali critici per l'azienda. Sfortunatamente, nei prossimi anni troveranno poche soluzioni disponibili sul mercato. Nel 2020, i ricercatori continueranno a sperimentare metodi per cui le soluzioni basate sull'intelligenza artificiale (AI) e sull'apprendimento automatico (ML) possono essere deviate o utilizzate in modo improprio e i risultati saranno utilizzati sia dai fornitori, per sviluppare soluzioni di sicurezza informatica, sia dagli avversari, per realizzare attacchi mirati.

Le immagini delle pagine seguenti riportano le 10 priorità per l'IT in Italia e nel mondo, secondo le risultanze del sondaggio.


LE 10 PRIORITÀ TOP
PER L'IT IN ITALIA
63% SICUREZZA DEI DATI
52% PRIVACY DEI DATI
51% CONSAPEVOLEZZA DELLA CYBER SECURITY TRA I DIPENDENTI
48% INTEGRAZIONE DI SOLUZIONI ESISTENTI
37% TRASFORMAZIONE DIGITALE
30% INVESTIMENTI NELLA FORMAZIONE DEL PERSONALE IT
29% RISPETTO DELLE NORMATIVE SULLA CONFORMITÀ E SULLA PRIVACY
25% MIGRAZIONE SU CLOUD
22% IMPLEMENTAZIONE DI SOLUZIONI BASATE SULL'IA
23% GESTIONE DELLA CONOSCENZA
netwrix


LE 10 PRIORITÀ TOP
PER L'IT NEL MONDO
74% SICUREZZA DEI DATI
53% AUTOMAZIONE DELLE OPERAZIONI MANUALI
51% CONSAPEVOLEZZA DELLA CYBER SECURITY TRA I DIPENDENTI
43% PRIVACY DEI DATI
37% MIGRAZIONE SU CLOUD
34% INTEGRAZIONE DI SOLUZIONI ESISTENTI
33% TRASFORMAZIONE DIGITALE
29% CONFORMITÀ ALLE NORMATIVE
23% GESTIONE DELLA CONOSCENZA
20% ACQUISIZIONE DI TALENTI IT
netwrix

Email security: i trend italiani del 2019

[A cura di Rodolfo Saccani, Libraesva]

Invece di partire dai numeri per poi trarre le conclusioni stavolta faremo l'opposto: iniziamo da quelli che sono i trend dell'anno, dalle lezioni che abbiamo appreso e da quello che ci possiamo aspettare nel 2020. Usando come linea guida i trend più significativi, entreremo nel dettaglio dei numeri nel corso dell'esposizione.
Le statistiche fornite da qui in avanti sono state calcolate su un campione di 10 miliardi di email ricevute in Italia nel 2019. Il campione comprende tipologie di traffico eterogenee (aziende di ogni dimensione, ISP/MSP, consumer, education, istituzionale, etc) in modo da poter essere considerato rappresentativo del traffico email in Italia.

Un anno di transizione

Dal punto di vista della difesa perimetrale che riguarda le email, il 2019 non è stato un anno caratterizzato da novità particolarmente rilevanti. Questo non significa che non siano emersi problemi o che non siano stati causati danni anche gravi, ma chi aveva adeguato per tempo le proprie difese ha vissuto un anno meno movimentato dei precedenti.
Le metodologie di attacco e le minacce sono andate raffinandosi in modo incrementale divenendo più efficaci e più pervasive ma non abbiamo rilevato grandi discontinuità.
La quantità di posta indesiderata ha oscillato tra il 60% e l'80% con un andamento più regolare rispetto allo scorso anno. Questo non è un parametro particolarmente significativo ma l'assenza di ampie oscillazioni a cui eravamo abituati nel corso dell'anno sembra in linea con un periodo di evoluzione e non di rivoluzione.

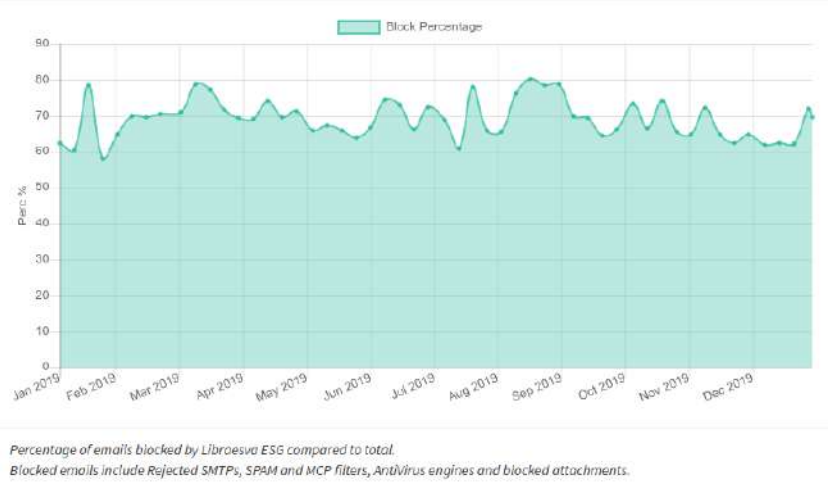


Figura 1: *Flusso di posta indesiderata nel 2019 in Italia (fonte: Libraesva)*

Business email compromise

Gli attacchi mirati (detti anche BEC o Whaling) sono in crescita ormai da oltre due anni. Sono gli ormai "classici" tentativi di impersonare un dirigente per indurre a fare transazioni o rivelare informazioni confidenziali.
Ormai questi attacchi non sono più una novità e non fanno neanche più notizia, sono così diffusi (circa una mail su mille) da essere condotti in buona parte in modo semi-automatico con un messaggio di approccio inviato in modo seriale e la cui efficacia non è particolarmente elevata.
Questo però non deve farci abbassare la guardia perché anche all'estremo opposto, cioè quello degli attacchi mirati e sofisticati (molto meno numerosi ma molto più efficaci) si sono fatti progressi.

Aziende di ogni dimensione sono ormai oggetto delle attenzioni degli autori di queste truffe che possono portare a perdite economiche ingenti (in relazione al giro d'affari dell'azienda) e spesso non vengono rese pubbliche.
Le tecniche di attacco spaziano dall'utilizzo di trucchi tecnici alla pura ingegneria sociale. Per quanto il nostro ego possa farci ritenere al di sopra di questi attacchi i dati ci confermano che si tratta di una falsa sicurezza che porta al contrario a renderci più vulnerabili.

Uno dei problemi che questo tipo di truffa pone è proprio la brevità dei messaggi e la loro semantica del tutto in linea con normali messaggi in ambito aziendale: si tratta di mail che offrono pochi appigli agli algoritmi di email security i quali faticano a discriminare un messaggio buono da uno non buono .

I segnali necessari a discriminare questi messaggi devono essere ricavati altrove, a questa esigenza rispondono sistemi di machine learning che dall'osservazione dei flussi di posta apprendono informazioni su quali siano gli interlocutori abituali di individui e organizzazioni.

Figura 2: *Adaptive Trust Engine di Libraesva*

Questi motori, che calcolano punteggi di affidabilità e indici di relazione in base alla frequenza e alla tipologia delle comunicazioni, riescono anche ad evidenziare nuovi interlocutori che si presentano con messaggi dalla semantica inconsueta per un nuovo corrispondente che non ha contatti con la persona a cui è diretta la mail o con la sua organizzazione.

Malware allegato a messaggi di posta

Non possiamo che continuare a registrare quanto siano poco efficaci i sistemi di protezione reattivi, ovvero quelli che si limitano ad identificare minacce note. Il business del ransomware e dei trojan continua ad essere lucroso, l'attività di sviluppo di nuove varianti è incessante e questo porta ad un flusso di nuove varianti che, grazie alla latenza dei sistemi reattivi (signature, pattern, ma anche analisi euristiche) trovano una finestra di alcune ore in cui riescono a passare senza essere intercettate.

L'unica strada realmente efficace è l'approccio proattivo, che rimuove gli strumenti di cui gli autori del malware necessitano: accesso al filesystem ed esecuzione di comandi. Non consentire il passaggio di allegati che sono in grado di fare queste operazioni rappresenta una soluzione estremamente efficace contro varianti ancora non note. Queste "sandbox di nuova generazione", come le abbiamo definite lo scorso anno, sono più rapide di quelle "classiche" basate su virtualizzazione, sono pressoché invulnerabili a tecniche di evasione ma sono purtroppo ancora poco diffuse.

Per comprendere il fenomeno osserviamo questo grafico che rappresenta il numero di allegati malevoli intercettati dai motori antivirus.

Figura 3: *Allegati intercettati da engine antivirus (fonte: Libraesva)*

L'efficacia è andata decrescendo nel corso dell'anno ma la cosa più rilevate la notiamo dal confronto con il grafico del numero di allegati malevoli intercettati dai sistemi di sandboxing di nuova generazione:

Figura 4: *Allegati intercettati da QuickSand di Libraesva*

In questo caso i numeri sono di circa un ordine di grandezza più grandi e la forma della curva mostra performance più costanti.

Quali sono i formati più usati tra quelli che veicolano malware?
Il formato più usato (49%) è il formato word binario (.doc), seguito dagli exe (37%), da jar (6%), da docx (1,5%) e da xlsx (1,1%).
Circa il 13% degli allegati in format word (doc e docx) sono malevoli.
Il volume di allegati xls e xlsx è di circa un decimo rispetto agli allegati word. Per gli xlsx la percentuale di allegati malevoli è ancora il 13% mentre per gli xls sale al 22%.
I formati archivio che più spesso contengono malware sono lo zip, seguito da iso, rar e gz.

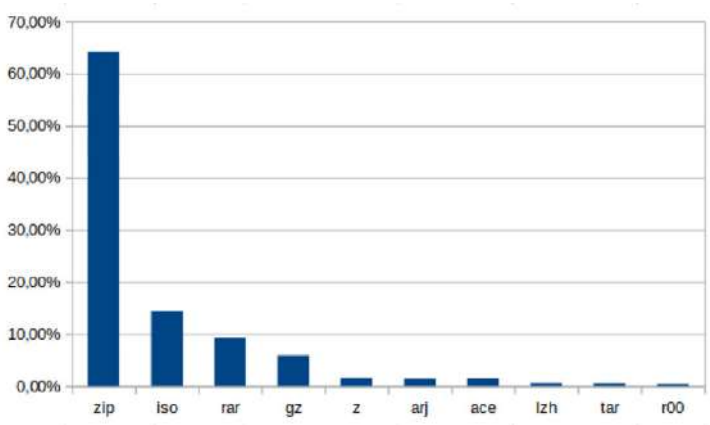


Figura 5: *Formati di archivio più usati per inviare malware*

Sandboxing dei link

Continuano a crescere gli attacchi condotti attraverso link inviati via email, link che puntano a siti di phishing o che forniscono malware.
Spesso questi link puntano a siti legittimi che sono stati compromessi da pochi minuti. Anche in questo caso l'approccio reattivo, quello di bloccare siti malevoli noti, comporta una latenza che lascia passare una parte considerevole delle minacce.

I sistemi di sandboxing dei link si stanno diffondendo ma le implementazioni sono per lo più basate su blackist, ovvero ancora una volta un approccio reattivo che blocca quello che è noto e lascia passare quello che non è ancora noto.
Il sandboxing dei link è uno strumento estremamente efficace quando invece compie una analisi attiva del link con l'ausilio di algoritmi in grado di identificare siti malevoli ancora non noti attraverso la rilevazione di tecniche di evasione e toolkit.

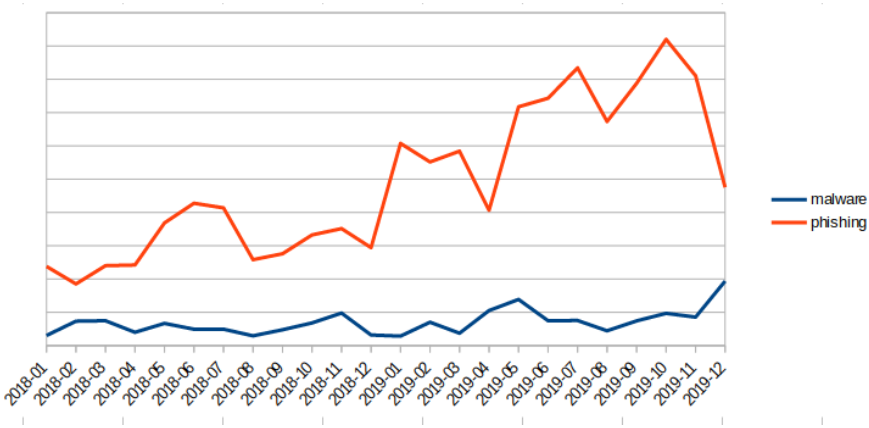


Figura 6: *Link a siti di phishing vs siti di malware intercettati da UrlSand di Libraesva*

Il grafico precedente mostra l'andamento, nel corso degli ultimi due anni, dei link che portano a pagine di phishing in relazione a quelli che portano a scaricare malware.
Possiamo vedere come nell'ultimo anno le campagne di phishing siano cresciute molto più di quanto siano cresciute quelle di malware.

Quante sono le mail che veicolano link?
Il numero di email contenenti almeno un link oscilla tra il 10% e il 20%, abbiamo rilevato una leggera crescita nel corso dell'anno, come evidenziato dal grafico di **Figura 7**.

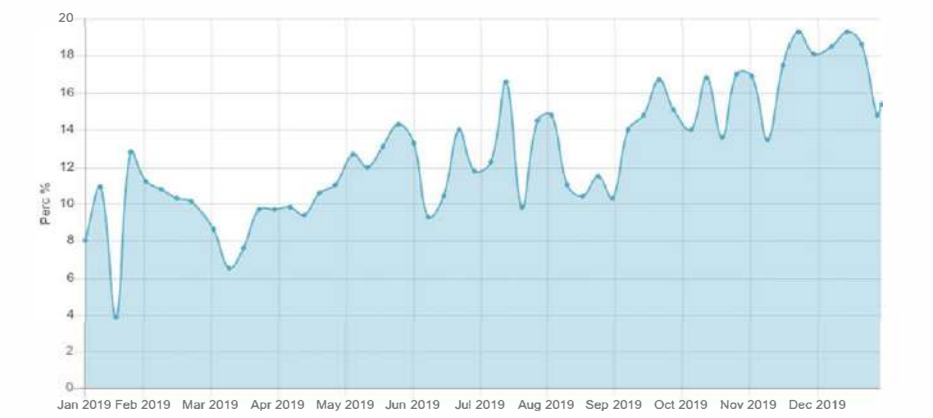


Figura 7: *Percentuale di email contenenti almeno un link (fonte: Libraesva)*

Di tutte queste mail contenenti link solo una su quaranta (circa) vedrà un click da parte dell'utente.
Tra le mail cliccate solo una percentuale molto piccola (tra lo 0,3% e lo 0,7% circa) è malevola.
I numeri sono piccoli perché stiamo parlando di email già sottoposte a controlli di sicurezza, queste sono quindi le mail per cui l'ultima rete di protezione rappresentata dal sandboxing dei link protegge l'utente.
Numeri piccoli in percentuale ma non in termini assoluti: parliamo di centinaia di migliaia di click potenzialmente dannosi che vengono intercettati "all'ultimo istante" (**Figura 8**).
Nel 24% dei casi quando si clicca sul link contenuto della mail viene eseguito uno o più redirect prima di arrivare alla pagina di destinazione, questo vale tanto per le url legittime quanto per le url malevole. E' molto importante che i sistemi di analisi siano in grado di seguire questi redirect in modo attivo e non limitarsi da una verifica (magari solo nei confronti di una blacklist) della url contenuta nella mail.

I siti che ospitano malware e phishing sono spesso siti legittimi che sono stati compromessi o siti costruiti appositamente per una campagna.
Seguendo questi link possiamo scoprire qual è la distribuzione geografica dei siti internet usati per consegnare campagne di malware e phishing in Italia (**Figura 9**).

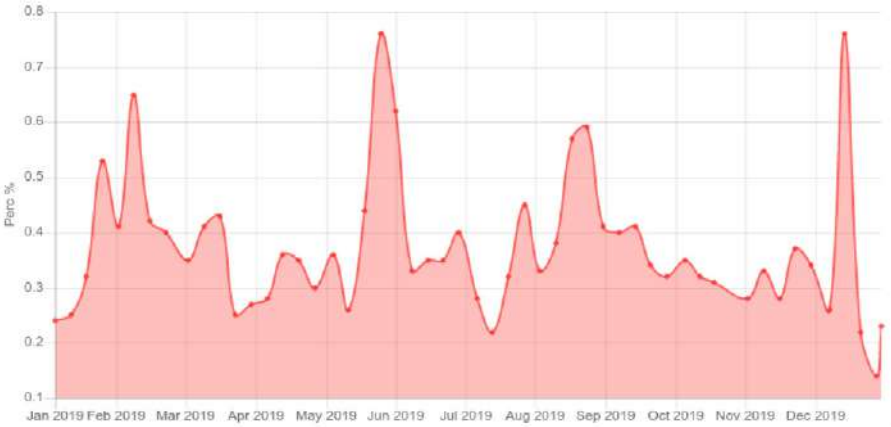


Figura 8: *Percentuale di link malevoli sul totale (fonte: Libraesva)*

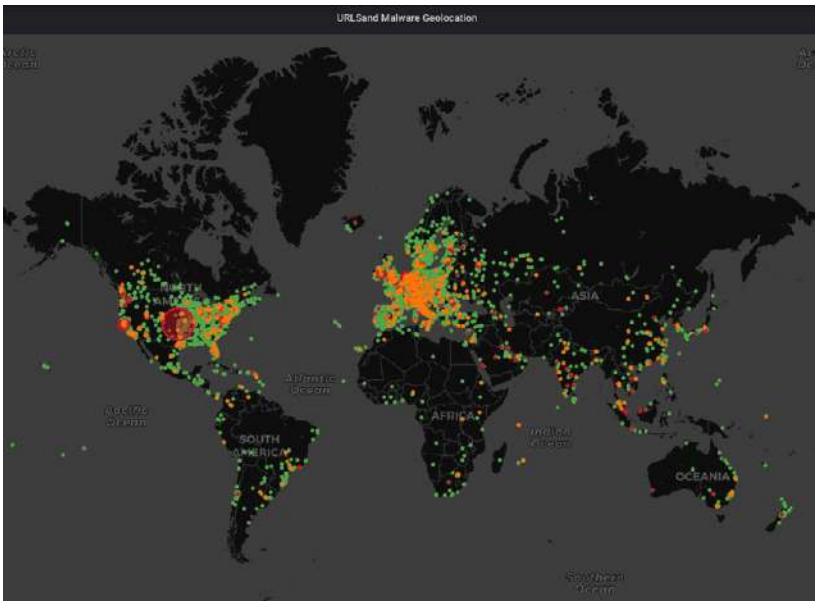


Figura 9: *Distribuzione geografica dei siti a cui puntano link malevoli (fonte: Libraesva)*

Furto di credenziali

Le mail malevole e quelle di spam continuano ad arrivare in buona parte da indirizzi email legittimi che sono stati compromessi. Le credenziali arrivano da tentativi a forza bruta su server SMTP/POP3/IMAP (grazie al fatto che le password sono spesso molto deboli), da campagne di phishing, da database leak e anche da router e dispositivi IoT compromessi che "sniffano" il traffico di rete e mandano al centro di comando e controllo tutte le credenziali che trovano.

Queste credenziali poi vengono utilizzate per l'invio di campagne email da parte di botnet composte da computer compromessi e dispositivi IoT. I device compromessi usano le credenziali fornite dal centro di comando e controllo per inviare email a nome degli utenti ignari.

La cosa più efficace che si può fare per evitare che il proprio account di posta venga compromesso è quella di utilizzare una password robusta e non riutilizzarla altrove.

Casi particolari e curiosità

In marzo abbiamo visto circolare email contenenti il trojan "ramnit", praticamente un cimelio, trattandosi di un malware vecchio di 10 anni. Abbiamo analizzato il sample per curiosità ipotizzando un tentativo di attacco mirato o una vecchia infezione che cerca ancora di auto-propagarsi.

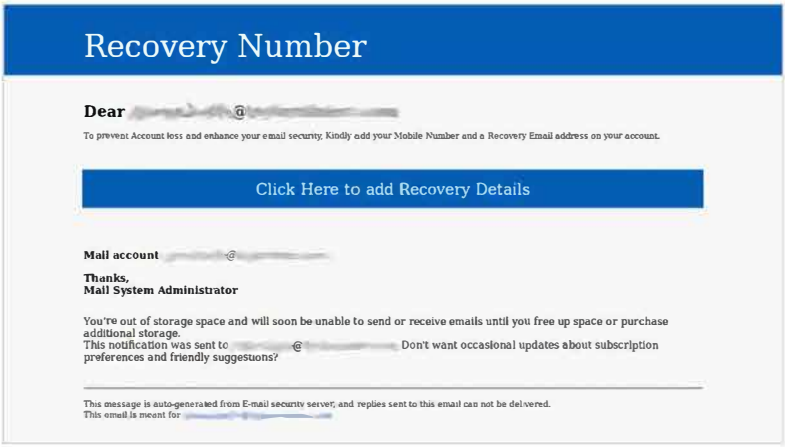


Figura 10: *Una email contenente il ransomware ramnit*

In giugno abbiamo visto tentativi di utilizzo di codice html costruito appositamente per cercare di consegnare link malevoli a client di posta Outlook superando i controlli di sicurezza attraverso l'uso di esensioni html specifiche di microsoft note come "commenti condizionali".

```
<html>
<body>

<!-- [if mso]>
    <p>This is for Microsoft Outlook users:</p>
    <a href="http://malware.website">Visit this website!</a>
<![endif]-->

Thank you!

</body>
</html>
```

Figura 11: *Esempio di utilizzo dei commenti condizionali*

In settembre abbiamo visto utilizzare il google re-captcha per "proteggere" pagine di phishing dalla visita dei crawler di sicurezza. L'idea si è dimostrata molto efficace nell'impedire per lunghi periodi il blacklisting dei siti. In fondo il re-captcha serve proprio per discriminare visitatori umani da bot, in questo caso è stato sfruttato per tenere lontano i bot di sicurezza e al tempo stesso, fornire una falsa sicurezza e un falso senso di legittimità al sito di phishing.

Figura 12: *Un re-captcha in una pagina altrimenti completamente bianca a protezione della vera pagina di phishing*

Figura 13: *La pagina di phishing viene mostrata solo dopo aver superato il re captcha*

Maggiori dettagli su questi argomenti sono disponibili sul security blog di libraesva.

Conclusioni

Tra mail legittime e mail indesiderate le modalità di trasporto e consegna sono sempre più omogenee fino a divenire del tutto indistinguibili quando vengono utilizzati account di posta legittimi.

I sistemi di analisi vengono così privati di elementi tecnici per discriminare i messaggi e devono concentrarsi maggiormente sull'analisi dei contenuti e nel ricavare segnali aggiuntivi attraverso l'apprendimento delle abitudini degli utenti sotto il proprio ombrello di protezione.

E' qui che i prodotti vanno differenziandosi in termini di efficacia. In particolar modo in un paese non anglofono come il nostro l'analisi semantica e il machine learning necessitano di una attenzione specifica del vendor per essere efficaci.

I sistemi reattivi (signature, pattern,etc) continuano a perdere marcatamente di efficacia e i sistemi più attivi (sandboxing di nuova generazione per allegati e link) diventano sempre più determinanti.

GLOSSARIO

Account hijacking	Compromissione di un account ottenuta ad esempio mediante *phising*.
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…).
BCP (Business Continuity Plan)	Documenti che riportano le soluzioni di preparazione e recovery messe in atto dalle aziende.
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).
BYOD (Bring You Own Device)	Politica che consente l'uso di dispositivi personali anche per finalità aziendali.
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.
CNOs (Computer Network Operations)	Tipologia di *Information warfare* finalizzato all'attacco e distruzioni delle informazioni presenti sui sistemi informativi avversari, alla distruzione delle reti e dei sistemi stessi e alla difesa delle proprie.

Cognitive Security	Applicazione all'ambito della sicurezza delle soluzioni di Cognitive Computing.
Context-based access	Tecnica che condiziona l'accesso alla valutazione dinamica del rischio della singola transazione, modulando eventuali azioni aggiuntive di verifica. Ad esempio 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.
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.
CTW (Check-the-Web)	Piattaforma tecnologiche appositamente creata in ambito *IRU* a supporto del monitoraggio e delle indagini nell'ambito di terrorismo in Internet, il cui ruolo principale è di anticipare e prevenire l'abuso terroristico di strumenti online, nonché di svolgere un ruolo consultivo proattivo a tale riguardo nei confronti degli Stati membri dell'UE e del settore privato.

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).
Course of action matrix	Metodologia per l'identificazione, la prioritizzazione e la rappresentazione sinottica delle azioni da intraprendere, in caso di possibili intrusioni. È composta da: due azioni passive: *Discover* e *Detect* cinque attive - *Deny*, *Disrupt*, *Degrade*, *Deceive*, *Destroy*).
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*.

CTI (Cyber Threat Intelligence)	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.
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*
CYBINT (Cyber Intelligence)	Disciplina che trae origine dalla declinazione classica delle attività di intelligence 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.
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.
Data Leakage	Trasferimento non autorizzato di informazioni riservate.
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 Fake	Algoritmi di deep learning in grado di creare foto o video falsi.
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.
Diamond Model	Framework strutturato per l'analisi tecnica di possibili intrusioni. (*Adversary, Infrastructure, Victim, Capability*).
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.
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*.
Digital Scarcity	In una *blockchain* la capacità di rendere non riproducibili informazioni digitali come file o pagamenti.
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.
Evasion	Nell'ambito delle applicazioni di IA attacco che consiste nel confondere la classificazione del dato in ingresso, da parte di un algoritmo precedentemente addestrato, manipolandone il contenuto.

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.
FIDO2	Meccanismo di autenticazione avanzata che standardizza l'uso dei dispositivi di autenticazione per l'accesso ai servizi online, sia in ambiente mobile che desktop.
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.
HMI (Human Machine Interface Systems)	Componente fondamentale dei sistemi IT industriali, che permette all'operatore umano di interagire con gli ambienti di controllo, supervisione e acquisizione dati (supervisory control and data acquisition - SCADA).
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.
HUMINT (HUMan INTelligence)	Disciplina intelligence consistente nella ricerca ed elaborazione di notizie di interesse per la sicurezza nazionale provenienti da persone fisiche. Le sue specificità sono legate alla tipicità della fonte e si sostanziano soprattutto in particolari modalità di gestione. *(Tratto da: Glossario intelligence – Il linguaggio degli Organismi informativi - www.sicurezzanazionale.gov.it)*

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.
IRU (Internet Referral Unit di Europol)	Unità all'interno di Europol preposta a rilevare ed investigare i contenuti malevoli su internet e social media.
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…).
MAAS (Malware as a Service)	Modello di erogazione del codice malevole 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.
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.
MFA (Multi-Factor Authentication)	Autenticazione a più fattori, nella quale si combinano più elementi di autenticazione per rendere più complessa la compromissione del sistema.
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.
Netizen	Soggetto che partecipa attivamente alla attività su internet. Letteralmente cittadino della rete.
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.
OF2CEN (On line Fraud Cyber Centre and Expert Network)	Piattaforma in cui far confluire tutte le segnalazioni provenienti da banche e Forze di polizia su transazioni sospette che avvengono in Rete, in modo da poter analizzare e condividere in tempo reale ogni informazione e bloccare così le operazioni illegali. "Eu-of2cen" (European Union Online Fraud Cyber Centre Expert Network) è il progetto ideato dalla Polizia di Stato, gestito dalla Polizia postale e delle comunicazioni, e finanziato dall'Unione europea per il contrasto al cybercrime finanziario. *(https://www.poliziadistato.it)*

Oracoli	Fonti esterne (API di un sito, output di un oggetto IoT…) alla blockchain per alimentare uno smart contract e scatenarne o influenzarne l'esecuzione.
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.
Phising	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).
Plausible Deniability	Capacità di un soggetto, in genere in posizione gerarchica elevata, di negare di essere a conoscenza di azioni dannose commesse da soggetti di livello più basso, in assenza di prove che possano dimostrare il contrario.
Poisoning	Nell'ambito delle applicazioni di IA attacco che consiste nel contaminare i dati di addestramento per impedire al sistema di funzionare correttamente.
Port Sweeping	Scansione di vari sistemi alla ricerca di una specifica porta in ascolto.
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.

PSYOPs (Psychological Operations)	"Operazioni psicologiche" consistenti nel far giungere a comunità, organizzazioni e soggetti stranieri informazioni selezionate al fine di orientarne a proprio vantaggio opinioni e comportamenti. *(Tratto da: Glossario intelligence – Il linguaggio degli Organismi informativi - www.sicurezzanazionale.gov.it)*
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).
Resilienza	"La capacità di un'organizzazione di assorbire gli shock e di adattarsi ad un contesto in continua evoluzione". *Definizione da* ISO 22316:2017
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.
SIGINT (SIGnals INTelligence)	Disciplina intelligence consistente nella ricerca ed elaborazione di notizie di interesse per la sicurezza originate da segnali e/o emissioni elettromagnetiche provenienti dall'estero. Le principali branche della SIGINT sono la COMINT e la ELINT. *(Tratto da: Glossario intelligence – Il linguaggio degli Organismi informativi - www.sicurezzanazionale.gov.it)*
Sinkhole	Tecnica per reindirizzare il traffico di rete verso uno specifico server al fine, ad esempio, di analizzarlo.
SIRIUS	Piattaforma tecnologiche appositamente creata in ambito IRU a supporto del monitoraggio e delle indagini nell'ambito di terrorismo in Internet. In particolare consente ai professionisti delle forze dell'ordine, di condividere conoscenze, migliori prassi e competenze nel campo delle indagini sulla criminalità agevolata da Internet, con particolare attenzione all'antiterrorismo.

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.
Smoking Guns	Termine che indica una prova (quasi) certa dell'aver commesso un crimine.
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*.
Tampering	An intentional but unauthorized act resulting in the modification of a system, components of systems, its intended behavior, or data.
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.
VNC (Virtual Network Computing)	Strumento di condivisione del desktop da remoto.
Vetting	Il processo di identificazione dei partecipanti ad una blockchain.
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 2020

Andrea Antonielli, laureato in Giurisprudenza presso l'Università degli Studi di Milano. È Ricercatore presso gli Osservatori Digital Innovation del Politecnico di Milano e si occupa dei temi connessi all'Information Security & Privacy, con particolare focus sulle normative europeee in materia di protezione dei dati personali.

Vita Santa Barletta dottoranda in Informatica e Matematica presso l'Università degli Studi di Bari Aldo Moro svolge le sue ricerche sui temi del "Secure Project Management". L'attività di ricerca si colloca nell'area della Ingegneria del Software con l'obiettivo di definire strumenti e tecniche per lo sviluppo sicuro del software; processi e strutture organizzative per la gestione sicura di progetti software. Ha contribuito all'avvio del laboratorio di Cyber Security dell'Università di Bari, The Hack Space, e ha svolto un periodo di ricerca presso IBM. È attualmente membro del Board del Branch Puglia del Project Management Institute – Southern Italy Chapter.

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.

Federica Bertoni, Informatico Forense certificata CIFI (Certified Forensic Investigator) col massimo del punteggio 125/125, Federica Bertoni è titolare di uno studio-laboratorio fondato 12 anni fa a Brescia e specializzato in Informatica Forense. Laureata in Giurisprudenza presso l'Università degli Studi di Brescia, con una tesi in Informatica Giuridica incentrata sugli aspetti di sicurezza informatica e giuridici del binomio "phishing-privacy", Federica Bertoni è stata Conciliatore presso il Servizio di Conciliazione e Arbitrato della Camera di Commercio di Brescia, in controversie in materia di ICT. Consulente Tecnico e Perito iscritta ad entrambi gli Albi del Tribunale Ordinario di Brescia, svolge attività di CTP per studi legali e aziende e da circa quattro anni a questa parte è stata coinvolta in alcune attività di studio e di ricerca, cui vi si dedica con grande passione, collaborando con le Cattedre d'Informatica Giuridica delle Facoltà di Giurisprudenza delle Università degli Studi di Milano e Brescia. È Affiliate Scholar e Fellow Researcher del Centro di Ricerca Information Society Law Center dell'Università degli Studi di Milano diretto dal professor Giovanni Ziccardi. Membro del Comitato Scientifico di CLUSIT, si occupa di cybercrime dal 2000. È autrice o coautrice di diverse pubblicazioni in materia di Sicurezza Informatica, Diritto dell'Informatica e delle Nuove Tecnologie e Digital Forensics. È autrice del paper "Deepfake, ovvero Manipola et impera. Un'analisi sulle cause, gli effetti e gli strumenti per la sicurezza nazionale, nell'ambito dell'utilizzo malevolo dell'intelligenza artificiale ai fini di disinformazione e propaganda", CIBERSPAZIO E DIRITTO, STEM Mucchi Editore, vol. 20 n. 62 (1-2 - 2019), p. 12-28. Attualmente sta redigendo una monografia scientifica sul voto elettronico, per la collana "Informatica Giuridica" edita da Giuffrè Lefebvre e diretta da Giovanni Ziccardi e Pierluigi Perri.

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 800 articoli e collaborazioni con oltre 30 testate. Ha pubblicato 23 fra libri e white paper alcuni dei quali utilizzati come testi universitari; ha partecipato alla redazione di 13 opere collettive. Già docente del percorso professionalizzante ABI - Privacy Expert e Data Protection Officer in Banca è docente/relatore presso eventi di ISACA/AIEA, ORACLE/CLUSIT, ITER, INFORMA BANCA, CONVENIA, CETIF, IKN, UNISEF, Università Statale di Milano, Università degli Studi Suor Orsola Benincasa Napoli…, Politecnico di Milano, Cefriel... 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.

Danilo Caivano, Professore di Ingegneria del Software e Cyber Security presso il Dipartimento di Informatica dell'Università degli Studi di Bari Aldo Moro, consulente di aziende ed enti soprattutto nell'ambito di progetti di ricerca e sviluppo. Responsabile Scientifico del laboratorio di ricerca SERLAB (serlab.di.uniba.it), Direttore dello short master in Cyber Security, ha contribuito alla realizzazione di The Hack Space, il laboratorio di cyber security dell'Università di Bari. Membro del Board of Director del Project Management Institute Southern Italy Chapter e coordinatore della PMI-SIC Academy. È componente del Comitato Tecnico Scientifico del Distretto dell'informatica Pugliese e del Comitato di Indirizzo Strategico dell'Osservatorio IT.

Luca Capacci ha conseguito la laurea triennale e magistrale in Ingegneria Informatica presso l'Università diBologna. Svolge varie attività di penetration test e progetta e sviluppa la piattaforma Mobile App Driller. Dal 2014 svolge attività di IT Security Engineer, attualmente presso CryptoNet Labs.

Nunzia Ciardi, Dirigente Superiore della Polizia di Stato, è il Direttore del Servizio Polizia Postale e delle Comunicazioni. Laureata in giurisprudenza, con anni di esperienza nel contrasto al cybercrime, 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". È membro componente del Consiglio del "*Women4Cyber*", iniziativa avviata dall'Organizzazione Europea per la Sicurezza Cibernetica (ECSO), volta a implementare il coinvolgimento delle donne nel settore della sicurezza cibernetica. 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 il Centro 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.

Pasquale Digregorio è un ex-Ufficiale d'Accademia che ricopre attualmente la posizione di Vice Capo Divisione del CERT della Banca d'Italia, dove da alcuni anni mette al servizio dell'Istituto la sua esperienza di specialista *senior* di *cyber security* e analista d'*intelligence* sviluppata in circa 20 anni di servizio, svolti presso il Ministero della Difesa e la Presidenza del Consiglio. 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. È autore di alcune pubblicazioni e di un brevetto internazionale; ha partecipato come relatore a diversi eventi e summit (da ultimo ITASEC 2020).

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 a Information Security & Privacy, Big Data Analytics e Digital Identity.

Gabriele Faggioli, legale, è amministratore delegato di Partners4innovation S.r.l. (a Digital360 Company di cui è socio e amministratore). È Presidente del Clusit (Associazione Italiana per la Sicurezza Informatica). 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 sulla responsabilità amministrativa degli enti e nel diritto dell'editoria e del marketing. 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 ad innumerevoli articoli sui temi di competenza ed è stato relatore a molti seminari e convegni.co dell'anno".

Boris Giannetto, lavora nel CERT della Banca d'Italia e si occupa di *cyber intelligence*. È incaricato di curare le iniziative di comunicazione sulla materia. Ha *expertise* su analisi strategica e *positioning*. 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. Ha lavorato 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 come MAECI-UNODC, Parlamento Italiano e UNICRI, con *focus* su temi di sicurezza. 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. Ha pubblicato a livello nazionale e internazionale, partecipando come relatore a diversi eventi e summit (da ultimo ITASEC 2020).

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.

Corrado Giustozzi esperto di sicurezza cibernetica presso l'Agenzia per l'Italia Digitale per lo sviluppo del CERT della Pubblica Amministrazione, membro per i mandati 2010-12, 2012-15, 2015-17 e 2017-20 del Permanent Stakeholders' Group dell'Agenzia dell'Unione Europea per la cybersecurity (ENISA), membro del Comitato Direttivo di Clusit. In trent'anni di attività come consulente di sicurezza delle informazioni ha condotto importanti progetti di audit ed assessment, e progettato infrastrutture di sicurezza e trust, presso grandi aziende e pubbliche amministrazioni. Collabora da oltre venti anni con il Reparto Indagini Tecniche del ROS Carabinieri nello svolgimento di attività investigative e di contrasto del cybercrime e del cyberterrorismo. Ha collaborato con l'Ufficio delle Nazioni Unite per il Controllo della Droga e la Prevenzione del Crimine (UNODC) su progetti internazionali di contrasto alla cybercriminalità. È docente nel Master Universitario di II livello in Homeland Security dell'Università Campus Bio-Medico di Roma, nel Master Universitario di II livello in Intelligence e Sicurezza della Link Campus University, nel Master Universitario in Cybersecurity della LUISS, nel Master in Protezione strategica del sistema Paese della SIOI. È membro del Comitato Scientifico dell'Area di Diritto e Informatica del Collegio Ghislieri – Università di Pavia. Membro di molteplici comitati scientifici e tecnici, giornalista pubblicista e membro dell'Unione Giornalisti Italiani Scientifici (UGIS), svolge da sempre un'intensa attività di divulgazione culturale sui problemi tecnici, sociali e legali della sicurezza delle informazioni. Ha al suo attivo oltre mille articoli e quattro libri.

Federica Maria Rita Livelli è in possesso della certificazione professionale in Business Continuity - AMBCI Certification BCI, UK & Risk Management FERMA Rimap ®. Svolge abitualmente consulenze di Risk Management & Business Continuity oltre a effettuare un'attività di diffusione e di sviluppo della cultura della resilienza presso varie istituzioni ed università. In passato ha ricoperto ruoli in vari ambiti, quali management administration, facility management, procurement, eventi e relazioni istituzionali presso primarie società e multinazionali. È Membro del Board del BCI Italy Forum, Chapter Italiano del BCI (Business Continuity Institute), UK e parte del BCI Professional Conduct Committee, UK, oltre ad essere Socia ANRA ed AIPSA.
Autrice di numerosi articoli inerenti alle tematiche di Risk Management & Business Continuity pubblicati da diverse riviste online, quali Agenda Digitale, CyberSecurity360, InsuranceReview, ISPI Online, RM Magazine.

Diego Pandolfi è Research & Consulting Manager in IDC Italy. Si occupa da oltre 10 anni di progetti di ricerca e di consulenza in diverse aree del mercato ICT, delle tecnologie digitali, dei media e delle TLC. In IDC ricopre il ruolo di Research & Consulting Manager e segue in particolare tematiche innovative ed emergenti, tra le quali blockchain, IoT e edge computing. Prima di entrare in IDC, ha ricoperto il ruolo di consulente, ricercatore e analista di mercato presso altre società di ricerca e di consulenza, sia in Italia sia all'estero. È laureato presso la Facoltà di Economia dell'Università Ca' Foscari di Venezia e ha frequentato un Master presso la SDA Bocconi (School of Management) in Strategia Aziendale.

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 even-

tuali 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.

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 responsabile di svariati Osservatori del Politecnico, quali l'Osservatorio Information Security & Privacy, l'Osservatorio Cloud Transformation, l'Osservatorio Big Data & Business Analytics e l'Osservatorio Artificial Intelligence.

Domenico Raguseo è Responsabile della Unit di CyberSecurity del gruppo Exprivia|Italtel. Precedentemente ha ricoperto il ruolo di CTO della divisione IBM Security nel Sud Europa. Ha una decennale esperienza manageriale e nel campo della cybersecurity in diverse aree. Domenico collabora con diverse università nell'insegnamento su tematiche relative alla cybersecurity sia come Professore a contratto che invitato come lettore per seminari. Domenico è stato IBM Master inventor grazie a una moltitudine di brevetti e pubblicazioni in diverse discipline (Business Processes, ROI, Messages and Collaborations, Networking). Infine, è apprezzato speaker, autore e blogger in eventi nazionali ed internazionali. In particolare, da diversi anni collabora con il Clusit come autore.

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 in delicate indagini in materia di anticorruzione, evasione fiscale, riciclaggio ed attività di polizia giudiziaria e tributaria a carattere nazionale ed internazionale anche nei confronti del crimine organizzato, è stato Ufficiale di Stato Maggiore al Comando Generale della Guardia di Finanza presso l'Ufficio Legislativo e l'Ufficio Telematica. Comandante della GdF nella Provincia di Latina dal 2013 al 2016. Plurilaureato, ha conseguito Master accademici. È abilitato alla professione di Avvocato, Revisore Legale dei Conti e Giornalista Pubblicista. É titolato IASD - Alti Studi della Difesa. Responsabile della Sicurezza IT della Guardia di Finanza dal 2009 al 2013, è stato Project Manager di informatica operativa ed ha redatto la Circolare organica sull'informatica nella Guardia di Finanza, nonché la Guida Operativa per i Finanzieri in materia di "Investigazioni Tecnologiche, Digital Forensics e Data Analysis". È, altresì, docente presso gli Istituti di formazione del Corpo ed Atenei Universitari, in materia di antiriciclaggio e frodi tecnologiche ed ha all'attivo pubblicazioni ed articoli su riviste specializzate in materia giuridica. Dal 2017 riveste l'incarico di Comandante del Nucleo Speciale Tutela Privacy e Frodi Tecnologiche della Guardia di Finanza.

Pier Luigi Rotondo lavora per il team di Technical Enablement IBM. Ha contribuito a molti progetti internazionali su soluzioni di sicurezza per l'Identity e l'Access Management, il Single Sign-on, Security Intelligence la Threat Intelligence. Con una la laurea in Scienze dell'Informazione presso Sapienza Università di Roma, Pier Luigi è coinvolto in attività accademiche su temi di Sicurezza delle Informazioni in Corsi di Laurea e Master presso l'Università di Roma e di Perugia. Per conto di IBM Italia scrive articoli divulgativi, e contribuisce permanentemente dal 2015 al Rapporto Clusit sulla Sicurezza ICT in Italia sul cybercrime nel settore finanziario, 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.

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, società milanese dedicata alla formazione ed alla consulenza in ambito Cyber Security, è Founder e Managing Director di Hackmanac, società che elabora dati sulle minacce Cyber a supporto di attività di Risk Management. Negli anni si è occupata di Social Media Security, ICT Security Consulting & Training e della gestione di progetti di Sicurezza Gestita, quali Vulnerability Management, Penetration Testing, 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 dei papers "La Sicurezza nei Social Media", pubblicato nel 2014 dalla Oracle Community for Security, e «Blockchain & Distributed Ledger: aspetti di governance, security e compliance», pubblicato nel 2019 da Clusit.

Fin dalla prima edizione contribuisce alla realizzazione del "Rapporto Clusit sulla Sicurezza ICT in Italia" curando l'analisi dei principali attacchi a livello internazionale."

Alfonso Solimeo si laurea in Ingegneria Informatica all'Università di Siena e completa il percorso di studi con la Laurea Magistrale in Ingegneria Informatica presso l'Università di Bologna. Acquisisce autonomamente esperienza nello sviluppo web e nella sicurezza informatica. Dal 2010 si focalizza esclusivamente sulla cybersecurity e dal 2018 occupa la posizione di IT Security Engineer presso CryptoNet Labs.

Maurizio Taglioretti, esperto di IT Audit, Security & Compliance è Country Manager Italy & Malta di Netwrix Corporation. Vanta una ventennale esperienza nel settore della sicurezza IT: prima di assumere questo incarico ha ricoperto diversi ruoli di crescente importanza a livello nazionale e internazionale in note aziende di sicurezza informatica. Maurizio è socio Clusit e socio (ISC)2 Italy Chapter, partecipa attivamente come relatore ad eventi sulla Sicurezza e la Compliance.

Stefano Taino, CEO e fondatore di CryptoNet Labs, opera nel campo della sicurezza IT da circa trent'anni, sin dalla sua nascita nel mercato italiano. Ha contribuito alla creazione del CERT-IT nel 1994 presso l'Università di Milano, il primo punto di riferimento per la sicurezza IT in Italia. Le sue competenze coprono una vasta gamma di temi, dalla consulenza su sicurezza e compliance di reti e sistemi informativi a progetti innovativi nei sistemi di controllo industriale e nel campo dell'application security. È speaker per argomenti specifici di IT/OT Security in diversi master e conferenze.

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.

Filip Truță è uno scrittore esperto con oltre un decennio di pratica nel campo della tecnologia. Ha coperto una vasta gamma di argomenti in settori come giochi, software, hardware e sicurezza informatica e ha lavorato in vari ruoli di marketing B2B e B2C. Filip attualmente funge da analista della sicurezza informatica in Bitdefender.

Alessandro Vallega lavora in Partners4Innovation sui temi di Information & Cyber Security, Innovazione e Partnership con il ruolo di Partner. 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 Clusit Community for Security (in precedenza Oracle Community for Security). È coautore, editor o team leader di undici 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.

Giancarlo Vercellino è Associate Research & Consulting Director in IDC Italy. Responsabile per attività di ricerca e consulenza per clienti italiani e internazionali, si occupa di strategia competitiva, indagini di mercato e analisi di scenario, scouting di imprese innovative e ricerca di partner per l'internazionalizzazione. Interviene come speaker e moderatore a conferenze, workshop ed eventi. Partecipa alla conversazione globale tramite stampa, blog, webinar e report. Segue le trasformazioni dei mercati e delle tecnologie digitali, con particolare riferimento al Machine Learning, ai Predictive Analytics e all'Intelligenza Artificiale. Partecipa alla ricerca continuativa IDC e alle attività di consulenza in Italia, e nel suo tempo libero si diletta nella programmazione con R. Prima di IDC, ha lavorato come analista presso diverse fondazioni e centri di ricerca applicata e insegnato economia presso il Politecnico di Torino. Ha un Dottorato in Ingegneria Gestionale al Politecnico di Milano.

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 600 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 CLUSIT.
- Ricerca e studio: Premio "Innovare la Sicurezza delle Informazioni" per la migliore tesi universitaria arrivato alla 15a edizione.
- Le Conference specialistiche: Security Summit (a Milano, Treviso, Verona e Roma)..
- I Gruppi di Lavoro: della Clusit Community for Security.
- Rapporti Clusit: Rapporto annuale, con aggiornamento semestrale, sula sicurezza ICT in Italia, in produzione dal 2012.
- 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 (International 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 ed organizzatore di eventi di alto profilo contenutistico nel mondo finanziario e dell'Ict.

Certificata dalla folta schiera di relatori (più di 700 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 18.000 partecipanti, e sono stati rilasciati circa 14.000 attestati validi per l'attribuzione di oltre 46.000 crediti formativi (CPE).

L'edizione 2020

La 12esima edizione del Security Summit partirà in aprile con gli **Atelier Tecnologici della Security Summit Academy**, iniziativa di formazione online, e in seguito si terrà: il 16 settembre a **Treviso**, il 7 ottobre a **Verona**, il 5 novembre a **Roma** e dal 10 al 12 novembre a **Milano**. Tra i **temi più in evidenza per il 2020**: Cyber Crime, Sicurezza del e nel Cloud, Intelligenza Artificiale, Blockchain, IoT, Industria 4.0., Compliance, GDPR, Certificazioni (professionali, di sistema, di prodotto).

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

Research Partner

www.securitysummit.it