Nuova edizione ottobre 2023

Rapporto

2023

sulla sicurezza ICT
in Italia

SECURITY SUMMIT

Indice

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

Prefazione

Sono purtroppo costretto a ripetere la stessa frase del Rapporto per l'anno 2022: i dati che leggerete non sono positivi. Soprattutto per l'Italia.

Il fenomeno cybercrime non solo non rallenta, ma accelera e si acuisce ulteriormente come dimostrato dall'impatto medio di ogni incidente, sempre più alto.

È frustrante pensare che nonostante la notevole leva normativa degli ultimi anni, l'aumento da anni double digit della spesa in sicurezza informatica, la crescente capacità e volontà di confronto sinergico fra aziende e pubbliche amministrazioni, l'attenzione mediatica, il miglioramento del rapporto fra PIL e spesa in cybersecurity, l'esponenziale crescita di eventi convegnistici, momenti formativi, seminari, spazi divulgativi per scuole, famiglie, aziende e pubbliche amministrazioni, la crescita del mercato della consulenza, la nascita e oggi la grande diffusione di percorsi di studio, corsi universitari, master, l'aumento delle figure professionalizzate, l'aumento di figure dedicate al tema almeno in parte in aziende, soprattutto medio-grandi, e pubbliche amministrazioni, ancora non si intravede una inversione di tendenza.

Lo sforzo profuso in questi anni è stato eccezionale. Forse unico.

Nonostante tutto questo, che è stato fondamentale e che deve continuare, i risultati in termini di efficacia nel contrasto al fenomeno non ritengo siano soddisfacenti.

Certo, si potrebbe obiettare, i danni potevano essere molto maggiori.
Ma mi sembrerebbe un po' debole come argomentazione e comunque di scarsa consolazione.

Personalmente sono convinto più che mai che pur continuando a profondere il massimo sforzo in tutte le direzioni che sopra succintamente, e sicuramente tralasciandone molte, ho richiamato, si dovrebbe aprire un confronto importante a tutti i livelli in merito alla realistica possibilità di arrivare in un lasso di tempo ragionevole a risultati realmente efficaci in termini di inversione di tendenza.

Ritengo che perlomeno due dovrebbero essere gli ambiti di confronto:

1. se è realistico che ogni azienda e pubblica amministrazione possa diventare ragionevolmente un centro di competenza adeguato o anche solo abbia le risorse per comprare dall'esterno le professionalità necessarie in un contesto nel quale l'evoluzione tecnologica pretende continuamente l'acquisizione di tecnologie che nel tempo devono essere manutenute, aggiornate e rese e mantenute sicure;
2. se sia possibile mettere a fattor comune in termini di economie di scala gli investimenti al fine di evitare che ogni azienda o pubblica amministrazione replichi all'infinito un modello di spesa che tolte le grandissime imprese si risolve in rivoli di poca efficacia.

Si tratta di riflessioni che dovrebbero concentrarsi in modo realistico sulla reale possibilità di far crescere la cultura della cyber in tutti i cittadini di ogni età e professione e di avere un tessuto pubblico e privato che dalle grandi pubbliche amministrazioni centrali e multinazionali fino alle più piccole imprese e studi professionali sia in grado di avere tecnologie manutenute e protette in modo adeguato potendo quindi investire le risorse necessarie.

Una analisi sulla sostenibilità del modello ritengo che sarebbe opportuna al fine di valutare se si stia facendo tutto il possibile o, invece, se siano possibili anche altre azioni per arrivare a un risultato tangibile.

Chiudo con una nota positiva: i casi di information warfare flettono.
Speriamo che i conflitti armati che interessano due zone del mondo in particolare cessino nel più breve tempo possibile.

*** *** ***

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 per il primo semestre 2023.

Oltre 60.000 copie scaricate e più di 500 articoli già pubblicati nei primi 10 mesi del 2023, sono l'evidenza della rilevanza del rapporto CLUSIT ed è quindi importante diffonderlo, leggerlo, farlo conoscere, perché solo dalla consapevolezza può derivare la conoscenza del problema, la capacità di adottare scelte idonee e quindi la sicurezza nostra e di tutti.

Buona lettura

Gabriele Faggioli
Presidente CLUSIT

Introduzione al Rapporto

Il Rapporto inizia con **una panoramica degli incidenti di sicurezza più significativi avvenuti a livello globale (Italia inclusa) nel primo semestre del 2023**, confrontandoli con i dati raccolti nei 4 anni precedenti.
L'analisi degli attacchi in Italia è poi completata dalle **rilevazioni e segnalazioni della Polizia Postale e delle Comunicazioni**, che ci hanno fornito dati e informazioni estremamente interessanti su attività ed operazioni svolte nel corso dei primi sei mesi di quest'anno.
Segue un **approfondimento sulla** evoluzione della **Cybersecurity in ambito manifatturiero/industriale**, con i dati di settore tratti dalle ultime rilevazioni (al 30 giugno 2023) di Clusit, ma non solo.

Riportiamo in seguito i risultati di una **survey su La Cybersecurity nelle piccole e medie imprese**, realizzata in collaborazione con Reti SpA in Lombardia, con focus **nelle province di Varese e Como.**

Questi sono infine i temi trattati nella sezione FOCUS ON:
- **Algoritmi predittivi e approccio risk-based nella gestione delle vulnerabilità. Il contributo del catalogo KEV**, a cura di Cisco
- **Next Generation Security Operation Center**, a cura di Fortinet
- **Analisi di oltre un anno di conflitto russo ucraino tra guerra convenzionale, cyber war e tecnologie avanzate**, a cura di Microsoft
- **Smart mobility API e recharge line come nuovi vettori di attacco**, a cura di BearIT
- **Cyber threat intelligence - Advancing security decision making**, a cura di CrowdStrike
- **Intelligenza Artificiale (IA), dati e cybersecurity triangolazione perfetta o triangolo delle Bermuda Potenzialità e sfide**, a cura di Federica Maria Rita Livelli.

Continuiamo anche in questa edizione del Rapporto le interviste dedicate agli attori istituzionali (Autority, Agenzie, Forze dell'Ordine e Centri di Competenza) con cui il Clusit ha stretto accordi operativi per diffondere la cultura della sicurezza informatica presso le Aziende, la Pubblica Amministrazione e i cittadini.

Riportiamo quindi **un'intervista a Paola Virginio, Presidente di START 4.0 - Centro di Competenza per la Sicurezza delle Infrastrutture Strategiche Digitali,** che contribuisce al Rapporto Clusit con un pezzo su **"Fattore umano: le sfide metodologiche legate alle competenze e alla consapevolezza"**.

Analisi dei principali cyber attacchi noti del 2022 e primo semestre 2023

Italia (sempre più) nel mirino

Come di consueto in questa prima sezione del Rapporto CLUSIT 2023, giunto ormai al suo dodicesimo anno di pubblicazione, analizziamo i più gravi cyber attacchi noti avvenuti a livello globale (Italia inclusa) nei 5 anni precedenti e li confrontiamo con l'analisi degli attacchi noti del primo semestre 2023. La scelta di analizzare alcuni fenomeni dal 2012, e altri "solo" negli ultimi 5 anni, si basa sulla rilevanza delle informazioni analizzate, al fine di comprendere trend significativi, in un mondo dove le evoluzioni sono spesso semestrali e viste più "profonde" nel tempo rischierebbero di essere non rappresentative della realtà attuale.

Osservando la situazione dal punto di vista quantitativo, negli ultimi 5 anni la situazione è nettamente peggiorata, seguendo un trend pressoché costante. Confrontando il numero di attacchi rilevati nel primo semestre 2018 con quelli del 2023 la crescita è stata dell'86% (da 745 a 1.382).
Nello stesso periodo la media mensile di attacchi gravi è passata da 124 a 230 (quasi 8 al giorno).

Oltre a essere aumentata la frequenza, sono aumentati anche gli impatti: la nostra stima della loro "Severity" (indice di gravità) è cresciuta costantemente, il che rappresenta un ulteriore moltiplicatore dei danni.

Considerato che questa analisi riguarda solo attacchi andati "a buon fine" (cioè che hanno generato danni significativi e sono divenuti di dominio pubblico), l'osservazione di queste dinamiche conferma la nostra convinzione che, rispetto al periodo 2011-2017, nell'ultimo lustro si sia verificato un cambiamento sostanziale nei livelli globali di cyber-insicurezza, al quale evidentemente non è corrisposto un incremento sufficiente delle contromisure adottate dai difensori.

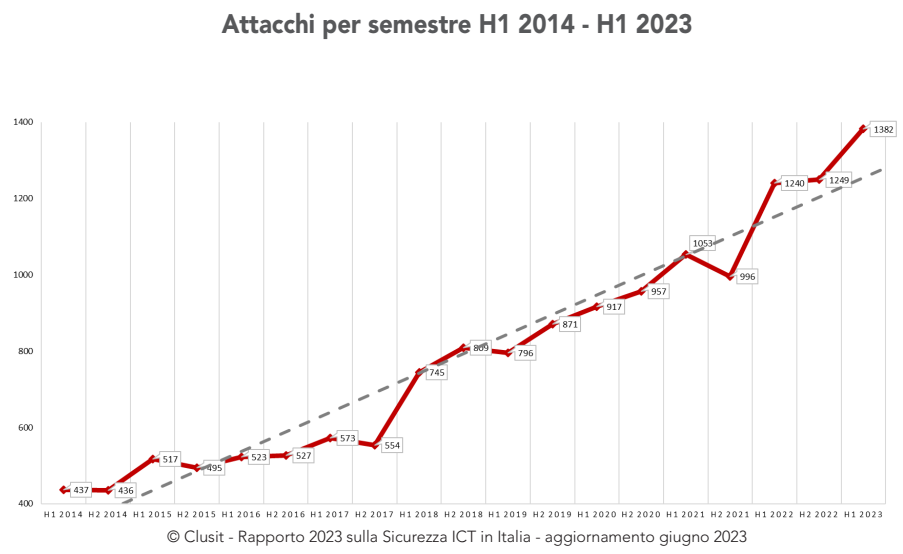


Fig. 1: *Andamento dei cyber attacchi per semestre da H1 2014 a H1 2023*

Come abbiamo scritto commentando i dati del 2021, ormai "siamo di fronte a problematiche che per natura, gravità e dimensione travalicano costantemente i confini dell'ICT e della stessa Cyber Security, ed hanno impatti profondi, duraturi e sistemici su ogni aspetto della società, della politica, dell'economia e della geopolitica".

Nel 2022, a queste dinamiche di fondo, per lo più derivanti dall'aumento delle attività cyber-criminali, si è aggiunto il conflitto tra Russia e Ucraina, che ha scoperchiato un vaso di Pandora di capacità cibernetiche offensive, utilizzate dai contendenti, dai loro alleati e in generale da tutti i principali attori globali, a supporto di attività di cyber-intelligence, di cyber-warfare e di operazioni ibride.

Questo processo di rapida adozione e messa in campo di strumenti cyber-offensivi sofisticati sarà difficilmente reversibile, il che potrebbe causare gravi conseguenze in un mondo già fortemente digitalizzato e sostanzialmente impreparato ad affrontare minacce di questa natura.

Interpretando il quadro che emerge dai dati potremmo affermare che, oltre ai danni crescenti causati dal cybercrime e dalle "normali" attività di intelligence che osserviamo già da anni, dal 2022 siamo entrati in una nuova fase di "guerra cibernetica diffusa", nel contesto di crescenti tensioni internazionali tra superpotenze e di un conflitto ad alta intensità combattuto ai confini dell'Europa.

In questo mutato scenario anche il nostro Paese risulta inevitabilmente coinvolto, come dimostra il significativo incremento (+40%) di attacchi andati a segno nel primo semestre 2023 rispetto al 2022. Va segnalato che l'aumento di attacchi rilevati verso bersagli italiani è percentualmente maggiore rispetto alla crescita osservata a livello globale, che nel primo semestre 2023 è stata pari all'11%.

Già l'anno scorso avevamo scritto "l'Italia è nel mirino", avendo subito il 7,6% degli attacchi globali (contro un 3,4% del 2021). Questo trend si conferma in crescita anche nel 2023, dato che nel primo semestre gli attacchi verso vittime italiane rappresentano il 9,6% del nostro campione totale, a parità di fonti utilizzate. Considerato che l'Italia rappresenta il 2% del PIL mondiale e lo 0,7% della popolazione, questo dato fa certamente riflettere.

Per queste ragioni abbiamo preparato un capitolo specifico e svolto alcune considerazioni puntuali su quanto osservato, nella speranza di contribuire a un incremento della consapevolezza rispetto a queste crescenti minacce per il Paese.

In questo senso auspichiamo che il PNRR, che complessivamente alloca circa 45 miliardi di euro per la "transizione digitale", possa rappresentare per l'Italia l'occasione di mettersi al passo e colmare le proprie lacune (anche) in ambito cyber, e che non abbia come esito un ampliamento incontrollato della superficie di attacco esposta dal Paese, ma al contrario una sua complessiva, significativa riduzione.

Per realizzarsi, questo obiettivo (assolutamente prioritario e strategico) richiederà una governance stringente in ottica cyber security di tutti i progetti di digitalizzazione previsti dal Piano, supportata da una visione politica salda, che non accetti compromessi e pressioni esterne e, finalmente, la valorizzazione delle risorse umane con competenze cyber, in termini di talenti e di esperienze, del Paese, e il loro sviluppo in termini quantitativi e qualitativi.

In questo sarà già centrale il ruolo delle Istituzioni, da quelle con una storia consolidata alle spalle, come l'Autorità Garante per la protezione dei dati personali e le Autorità per i mercati controllati, ad esempio, fino alla più recente, ma già estremamente attiva Agenzia per la cybersicurezza nazionale (ACN).

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

Analisi dei principali cyber attacchi noti a livello globale del 2018-2022 e del primo semestre 2023

In questa sezione offriamo una panoramica degli incidenti di sicurezza di pubblico dominio più significativi avvenuti a livello globale nel primo semestre dell'anno in corso, confrontandoli con i dati raccolti nei 5 anni precedenti.
Lo studio si basa sull'analisi di oltre 17.000 cyber attacchi noti, andati a buon fine e di particolare gravità, a partire dal 2011, che hanno avuto impatti significativi in termini economici, tecnologici, legali, reputazionali, o che comunque prefigurano scenari particolarmente preoccupanti.

Nel periodo che prenderemo in esame, tra gennaio 2018 e giugno 2023 si sono verificati un totale di 11.015 cyber attacchi, suddivisi come mostrato in **Fig. 2**.

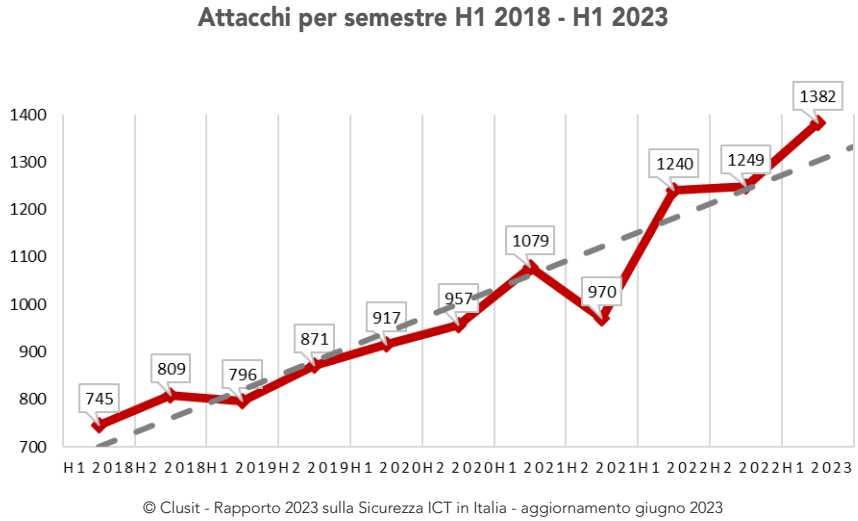


Fig. 2: *Andamento dei cyber attacchi nel periodo 2018 – H1 2023*

Il nostro campione rappresenta il 62% del totale degli incidenti classificati in oltre 12 anni, con una media complessiva di 172 attacchi al mese nell'intero periodo (erano 39 nel 2011, 130 nel 2018, 207 nel 2022 e sono 230 nel H1 2023).

Nel primo semestre dell'anno abbiamo registrato 1.382 cyber attacchi, il numero maggiore di sempre, ed è interessante notare come nel 2023 la realtà abbia superato le previsioni indicate in grigio dalla linea di tendenza stabilita sulla base dei dati 2018-2022.
Il picco massimo del semestre e di sempre si è registrato ad aprile con 262 attacchi.

Nella **Fig. 3** si osserva la distribuzione mensile degli attacchi nel 2023 fino a giugno 2023.

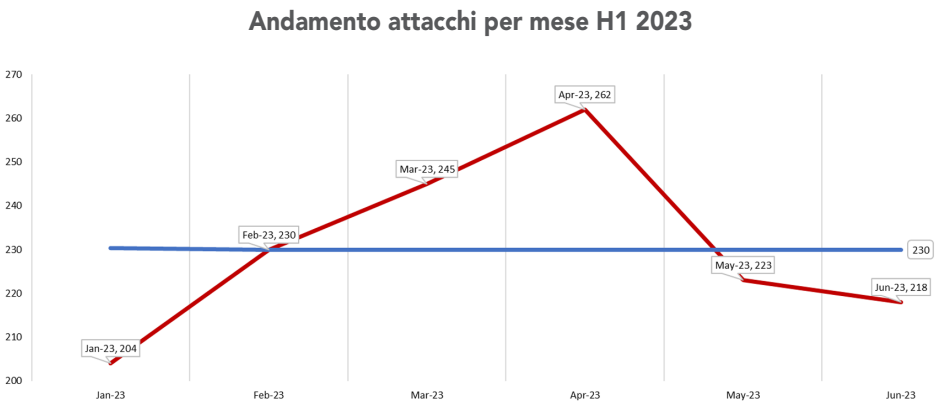


Fig. 3: *Numero di attacchi per mese nel primo semestre 2023*

Come si evince dal grafico, i mesi più attivi caratterizzati da un numero di incidenti superiore alla media (indicata dalla linea blu) sono stati marzo e aprile, mentre febbraio ha registrato un numero di attacchi equivalente al valore medio.

Nella **Fig. 4** una rappresentazione sintetica delle medie mensili negli ultimi 5 anni e mezzo:

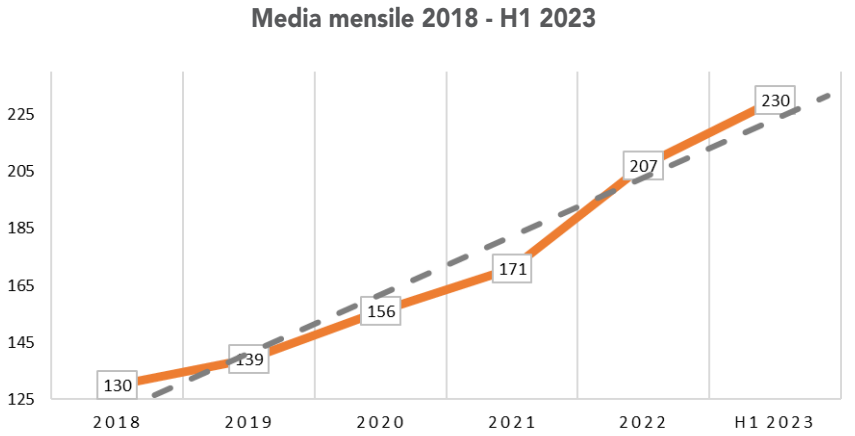


Fig. 4: *Andamento delle medie mensili nel periodo 2018-H1 2023*

Anche in questo caso, già dal 2022 i dati superano i trend indicati in grigio dalla linea di tendenza.

Distribuzione degli attaccanti per tipologia (2019 – H1 2023)

Analizzando lo storico degli attaccanti dal 2019 al primo semestre 2023 (**Fig. 5**) si nota che si mantiene la prevalenza degli attaccanti del tipo "cybercrime", proiettando il semestre sull'anno, con un andamento regolarmente in crescita come numero di attacchi. La crescita, sia pure con numeri più bassi, si mantiene anche per le altre tipologie di attaccanti. In particolare, per il cybercrime nel 2022 si osservano oltre 2.000 attacchi (2.043) che scendono a 259 per spionaggio e sabotaggio, a 103 per information warfare e a solo 84 per l'attivismo.

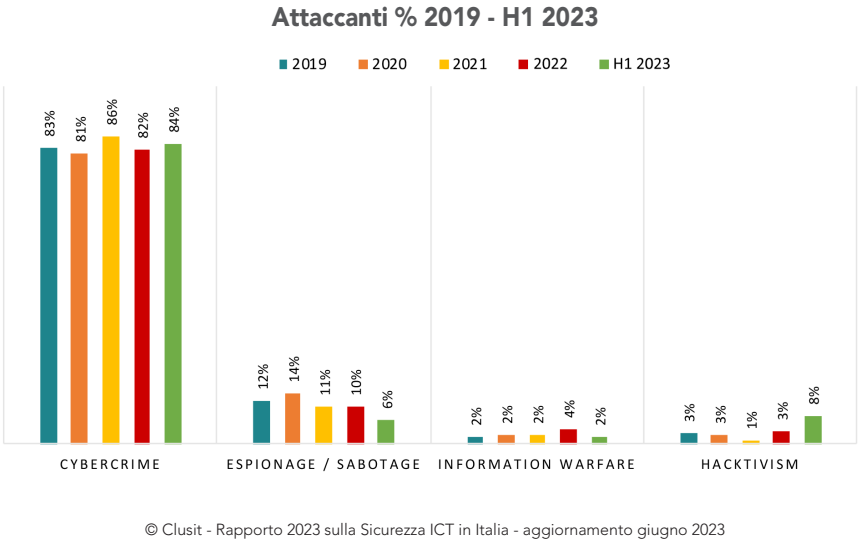


Fig. 5: *La distribuzione percentuale degli attaccanti tra il 2019 -H1 2023*

Ad inizio anno gli stessi dati in termini percentuali consentivano una lettura da un punto di vista diverso; infatti, gli attaccanti per la tipologia Cybercrime erano in leggera flessione rispetto al 2021 (82% contro 86%) con uno scarto di ±1 punto percentuale rispetto a 2020 e 2019 e in aumento di 3 punti percentuali rispetto al 2021.
Il calo percentuale della tipologia Cybercrime andava a "vantaggio" dell'Information warfare che raggiungeva il 4%, tornando ai valori del 2018, dopo aver subito una leggera decrescita dal 2019 al 2021 (2pp.). La stessa considerazione valeva anche per l'attivismo, che dopo una continua decrescita di un punto percentuale all'anno dal 2018 al 2021 (dal 4% all'1%), nel 2022 ritornava al 3%.

Infine, lo spionaggio/sabotaggio perdeva un punto percentuale rispetto al 2021, dopo aver raggiunto il massimo del 14% nel 2020, all'epoca soprattutto a causa di azioni di spionaggio industriale legato al Covid (principalmente verso enti di ricerca, laboratori, cliniche, etc…). Si può supporre che la crescita di Information warfare e soprattutto di attivismo possa essere stata effetto, almeno in parte, della guerra in Ucraina, che ha stimolato le azioni anche "digitali" degli attivisti e ha sollecitato la diffusione di informazioni di propaganda e contro-propaganda. Tale crescita, assieme a quella dell'hacktivism sembrava, come detto sopra, tratteggiare uno scenario in cui si sia ridotta la portata del "comune" cybercrime, il che rende ancora una volta importante sottolineare come in valore assoluto queste tre categorie abbiano raggiunto, nel 2022, i propri massimi storici.
Nel primo semestre 2023, invece, vediamo come le dinamiche tendano a somigliare di più a quelle degli anni precedenti, con il cybercrime in crescita e tutte le altre categorie in calo, a parte un picco di azioni di hacktivism, che passa dal 3 all'8%. Sarà importante tenere sotto osservazione, a fine 2023, gli eventuali impatti della nuova guerra in Medio Oriente su questi trend.

La rappresentazione a torta dei dati percentuali (**Fig. 6**) mostra con immediatezza l'enorme preponderanza degli attaccanti Cybercrime: è comunque un settore che attira grande attenzione da parte del crimine, probabilmente per i significativi risvolti economici legati alla sempre maggiore diffusione degli attacchi ransomware, nonché il picco di hacktivism che passa dal 3 al 8%.

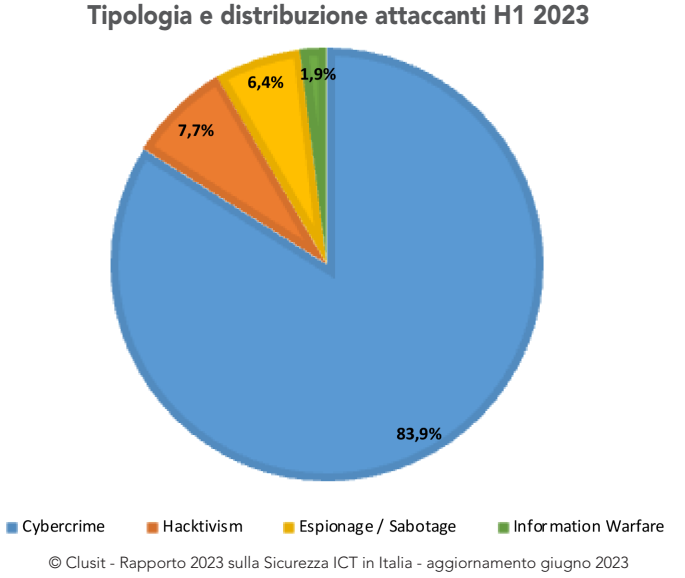


Fig. 6: *Andamento percentuale della tipologia di attaccanti nel H1-2023*

Distribuzione delle vittime per categoria (2019 – H1 2023)

Nel primo semestre dell'anno Multiple Targets è il settore maggiormente preso di mira (20% degli eventi totali).
Seguono Healthcare (14,5%), l'ambito Governativo / Militare / Law Enforcement (11,7%), ICT (11,4%), Financial / Insurance (10,5%) e Education (7,1%).

Insieme questi 6 settori rappresentano oltre il 75% degli incidenti globali classificati nei primi sei mesi dell'anno.

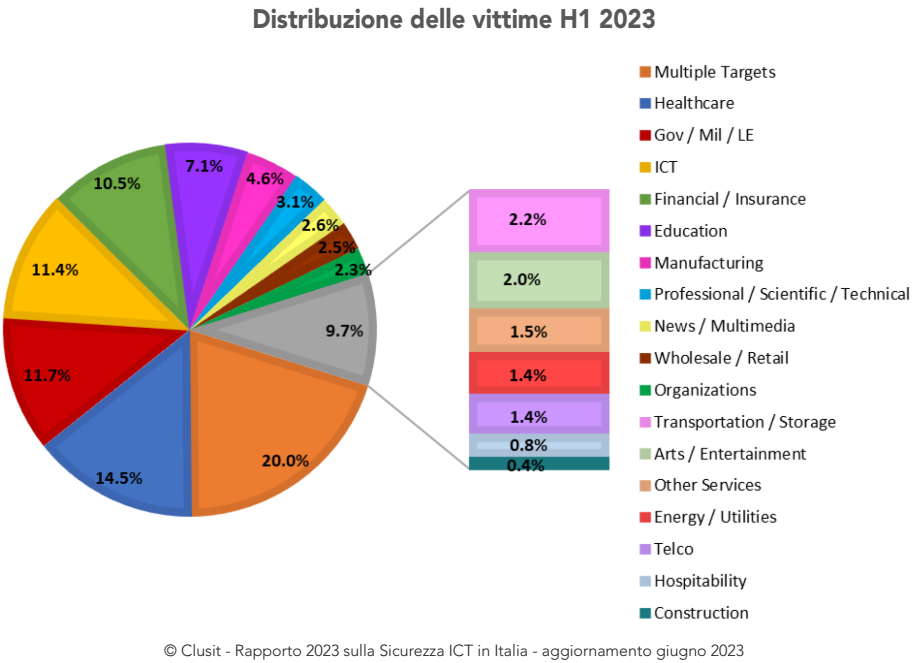


Fig. 7: *Andamento percentuale della tipologia di vittime nel primo semestre 2023*

Il confronto con gli anni precedenti mostra variazioni limitate rispetto al 2022.
Diminuiscono leggermente gli attacchi verso i Multiple targets (-2 punti percentuali, pp. rispetto all'anno precedente), segno che, per quanto gli attacchi di "a strascico" che puntano a colpire il maggior numero di vittime contemporaneamente siano sempre convenienti, la tendenza emergente è che le azioni criminali stanno diventando più mirate.

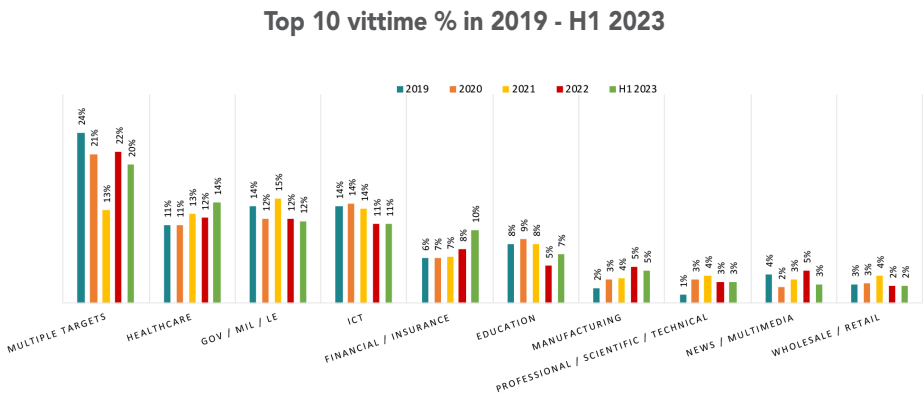


Fig. 8: *Le prime 10 categorie di vittime colpite in valore percentuale*

Meno colpito anche il settore News / Multimedia (3% degli incidenti totali nel H1 2023, -2 pp.), che negli anni precedenti era stato particolarmente preso di mira anche a causa di numerose azioni di propaganda e disinformazione da imputare al conflitto europeo.
Aumentano invece gli attacchi verso i settori sanitario, finanziario e Education (+2 pp. per ognuno), tre ambiti che per la loro strategicità si dimostrano sempre convenienti dal punto di vista degli attaccanti.

Restano sostanzialmente stabili gli attacchi verso i settori Gov / Mil / LE, ICT, Manufacturing, Professional / Scientific / Technical e Wholesale / Retail.

Distribuzione generale delle vittime per area geografica (H1 2023)

La lettura dei dati della distribuzione geografica percentuale delle vittime (**Fig. 9**) restituisce indirettamente la fotografia di come stia variando la digitalizzazione nel mondo e quanto sostanzialmente nessuno si possa più considerare al riparo dalle minacce della Cyber Security. È bene tuttavia sottolineare che per alcuni continenti come (Oceania e Africa) le informazioni sulle violazioni informatiche siano certamente limitate e quindi non rappresentative della situazione reale.

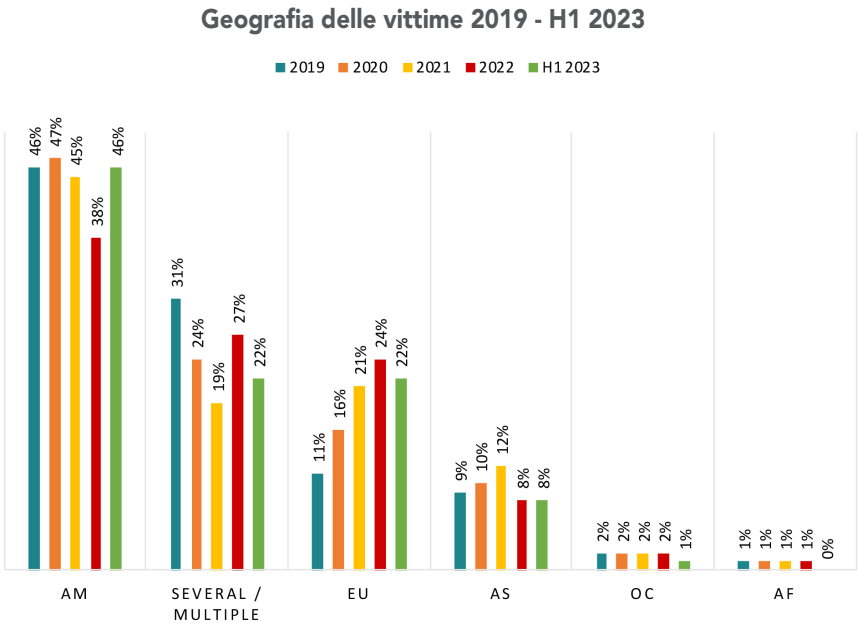


Fig. 9: *Distribuzione geografica percentuale della tipologia delle vittime nel periodo 2019-H12023*

Le Americhe nel loro complesso tornano ai valori 2021 dopo essere diminuite nel 2022 di 7 punti percentuali rispetto al numero di vittime. Un'ipotesi, come meglio analizzato nel capitolo dedicato alle pubbliche amministrazioni, potrebbe essere una maggiore recrudescenze nei confronti degli stati uniti e delle sue Organizzazioni, all'interno del conflitto russo-ucraino.

Diminuiscono nettamente gli attacchi verso vittime in località multiple (-5 pp.), un ulteriore segnale che nel 2023 i trend mostrino una preferenza verso azioni più mirate.

Scende di poco avvicinandosi ai valori 2021 l'Europa, che resta comunque teatro di oltre un quinto delle violazioni globali.
Restano invece sostanzialmente invariate le altre zone del mondo.

La **Fig. 10** presenta uno zoom sui dati H1 2023, confermando la preponderanza percentuale di vittime in America nel 2022 (46,5%), contro Europa al 22% e Asia all'8%.
Quasi un quarto degli attacchi è avvenuto parallelamente verso bersagli posti in diversi Paesi (21,7%), oltre a oceania (1,3%) e Africa (0,4%).

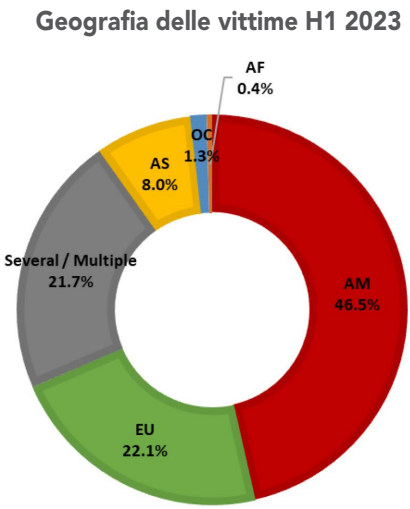


Fig. 10: *Distribuzione geografica delle vittime nel primo semestre 2023*

Distribuzione delle tecniche di attacco (2019 – H1 2023)

Nel primo semestre 2023 la categoria che mostra numeri assoluti maggiori è ancora una volta "Malware", che sia pure in leggera flessione (**-1,3 pp.**) rappresenta il **35.7%** del totale. Le tecniche sconosciute (categoria "Unknown") sono al secondo posto con il **21%**, con una diminuzione di **3 punti percentuali** rispetto al 2022, superando la categoria "Vulnerabilità" (che cresce però d**i 4,8 pp.**) e "Phishing / Social Engineering" (in diminuzione di 3,4 pp.), mentre "Tecniche Multiple" rappresenta l'8% del totale (scendendo di **1,4** pp.).
In concomitanza con l'aumento di attività riferibili ad Hacktivism e information Warfare, gli attacchi DDoS, pur pochi in valori assoluti, crescono di **3,8 pp.**, mentre rimangono stabili quelli realizzati tramite "Identity Theft / Account Hacking" (+0,3 pp.).

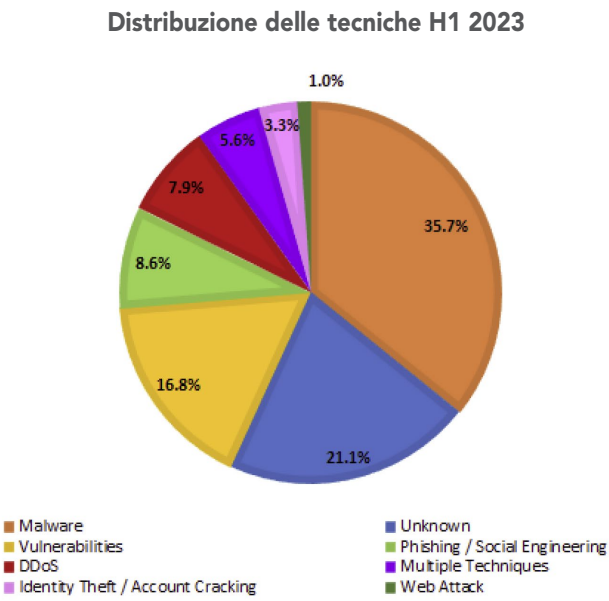


Fig. 11: *Distribuzione delle tecniche di attacco nel primo semestre 2023*

Il **21%** di "tecniche sconosciute" è principalmente dovuto al fatto che molti attacchi analizzati (oltre un quinto del totale) diventano di dominio pubblico a seguito di un "data breach", nel qual caso le normative impongono di inviare una notifica agli interessati, che non comprende necessariamente una descrizione precisa delle modalità dell'attacco (che normalmente quindi non viene fornita).

La crescita della categoria "Vulnerabilità" include, oltre allo sfruttamento di molte falle note, anche una significativa crescita nell'uso di exploit "0-day", utilizzati nel primo semestre 2023 anche da gruppi cybercriminali (p.es. Cl0p) per realizzare numerosi attacchi di tipo "ransomware".

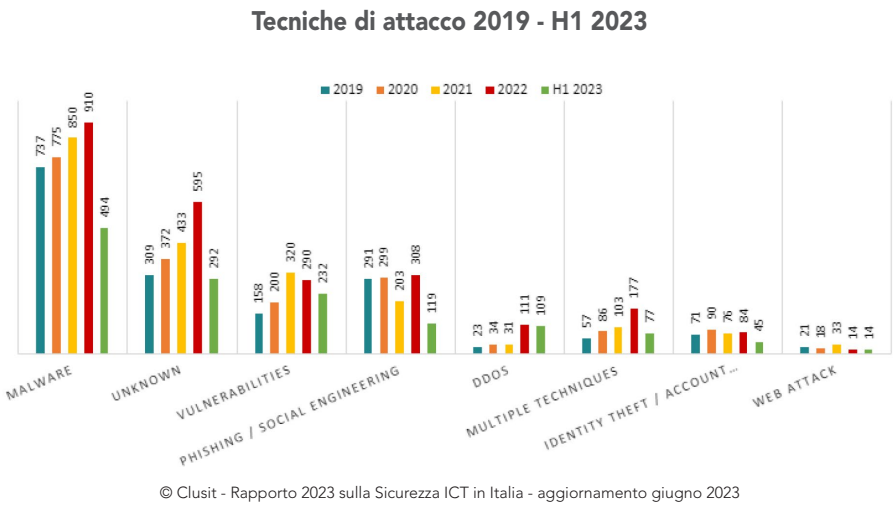


Fig. 12: *Distribuzione delle tecniche di attacco nel periodo 2019 - primo semestre 2023*

Osservando il grafico relativo al periodo 2019 – H1 2023, è necessario considerare che in numeri assoluti gli attacchi rilevati sono quasi raddoppiati. Ad esempio, per quanto riguarda il Malware, anche se in percentuale la categoria è diminuita di 8 punti rispetto al 2019, in valori assoluti il loro numero è aumentato del 34%. La stessa considerazione vale per tutte le categorie di tecniche di attacco.

Analisi della "Severity" degli attacchi

L'analisi della gravità degli attacchi si pone come obiettivo la valutazione degli impatti degli incidenti, sia per quanto riguarda le ripercussioni tecnologiche che quelle economiche, legali e reputazionali.

La severity degli incidenti non necessariamente corrisponde all'aumento dei numeri assoluti, né si può banalmente dedurre dalla tipologia di vittima o dalla tecnica utilizzata, è quindi di fondamentale importanza valutarne l'andamento.

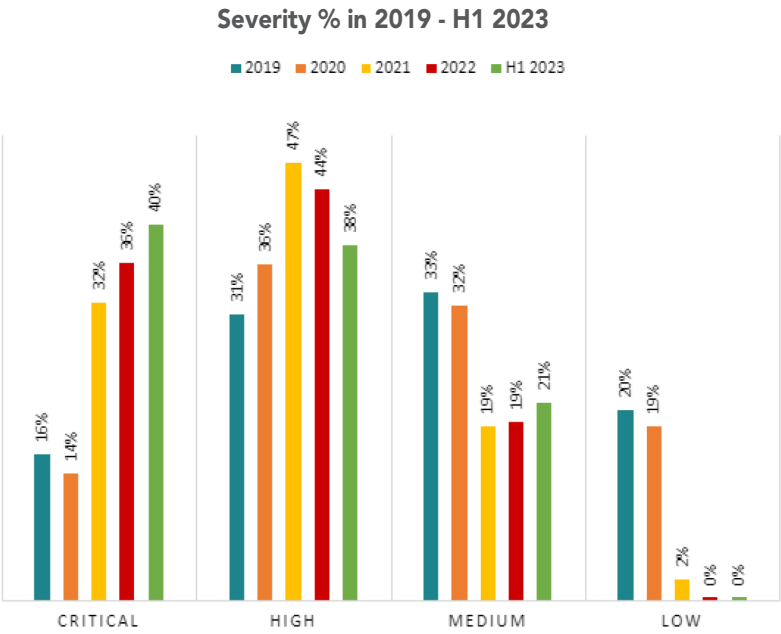
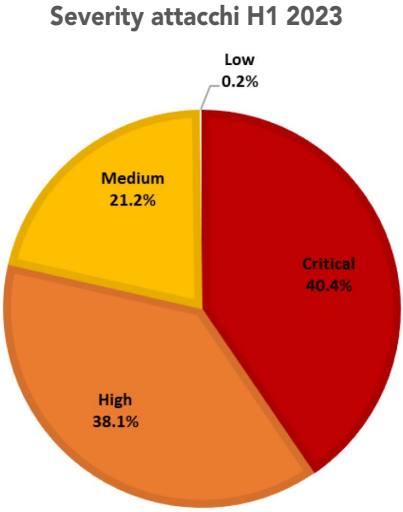


Fig. 13: *Andamento percentuale della Severity degli attacchi nel periodo 2019-H1 2023*

Negli ultimi tre anni si è instaurata una tendenza preoccupante che ha visto prevalere in maniera consistente gli attacchi con Severity "Critical", ovvero che hanno causato danni importanti per le vittime, come ingenti perdite economiche, elevate quantità di dati sottratti o il blocco delle operazioni, mentre gli attacchi a basso impatto tendono a scomparire.

Anche nel primo semestre dell'anno in corso gli attacchi con impatti gravi o gravissimi sono la stragrande maggioranza (78,5% nel H1 2023, 80% nel 2022).
Gli incidenti con impatti medi sono solo un quinto, mentre spariscono quasi del tutto quelli con impatti bassi (**Fig. 14**).

È evidente che il trend che emerge è preoccupante e pericoloso ed è necessario intervenire al più presto per arginare i danni di azioni cybercriminali sempre più impattanti.



© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia - aggiornamento giugno 2023

Fig. 14: *Distribuzione della Severity nel H1 2023*

Peraltro, il dato è sconsolante se abbinato ai risultati delle ricerche in Italia dell'Osservatorio Cybersecurity & Data Protection del Politecnico di Milano[1]: investiamo sempre di più, sebbene non ancora abbastanza, ma subiamo anche più danni. È il sintomo che dovremmo certamente rivalutare gli investimenti, oltre che incrementarli, con un approccio al problema radicalmente differente.

Severity per tipologia di attaccante

L'analisi degli impatti ha senso anche rapportata alla tipologia degli attaccanti.
Il cybercrime, che normalmente è preponderante rispetto alle altre tipologie, nel 2023 ha impatti superiori rispetto all'anno precedente.

Ma l'aspetto più interessante emerge relativamente agli attacchi perpetrati con finalità di spionaggio o cyber warfare che mostrano impatti critici in misura notevolmente maggiore. E il confronto con l'anno precedente mostra che la tendenza è decisamente in aumento.

[1] Atti del Convegno "Cybersecurity: verso un fronte comune" dell'Osservatorio Cybersecurity & Data Protection del Politecnico di Milano

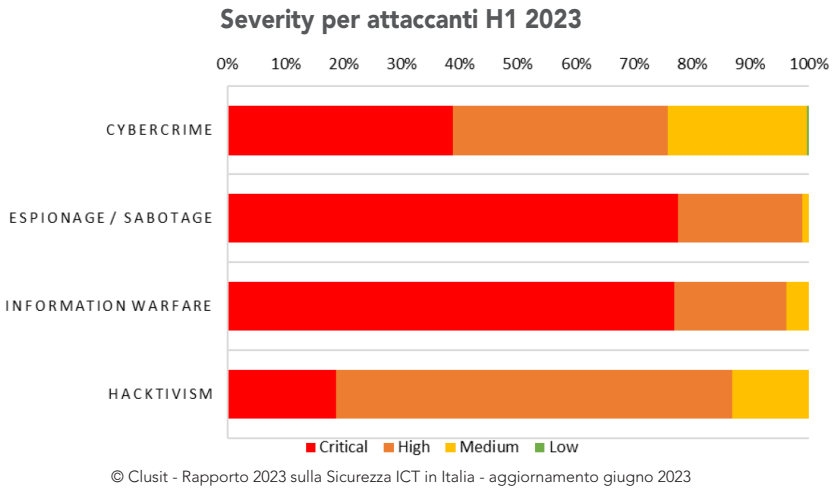


Fig. 15: *Distribuzione della Severity per attaccanti nel primo semestre 2023*

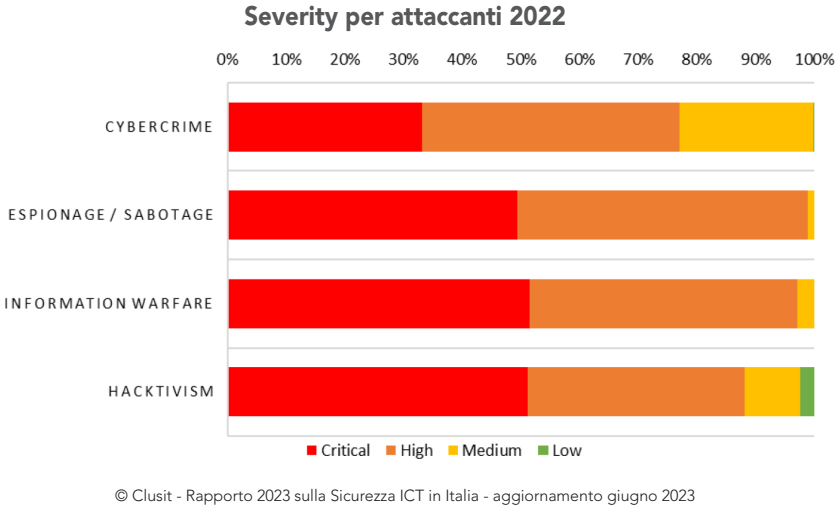


Fig. 16: *Distribuzione della Severity per attaccanti nel 2022*

Gli attacchi con finalità di hacktivism invece, sebbene superiori numericamente rispetto al 2022, nel primo semestre dell'anno si dimostrano meno dannosi.

Severity per tipologia di vittima

Anche l'analisi della Severity per settore merceologico mostra risvolti interessanti e non banali.

Indipendentemente dai numeri degli incidenti mostrati in precedenza, come si evince dal grafico in **Fig. 17**, non tutte le tipologie di vittime vengono colpite nello stesso modo.

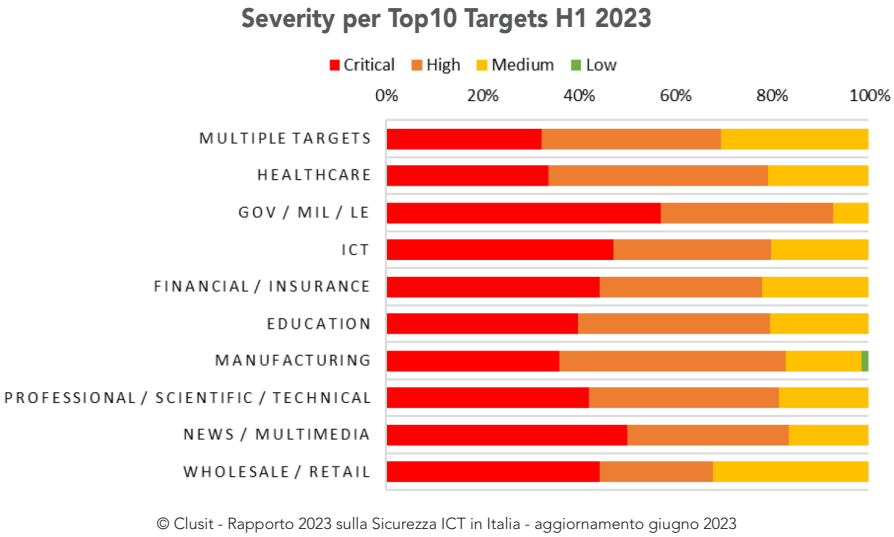


Fig. 17: *Distribuzione della Severity per prime 10 vittime nel primo semestre 2023*

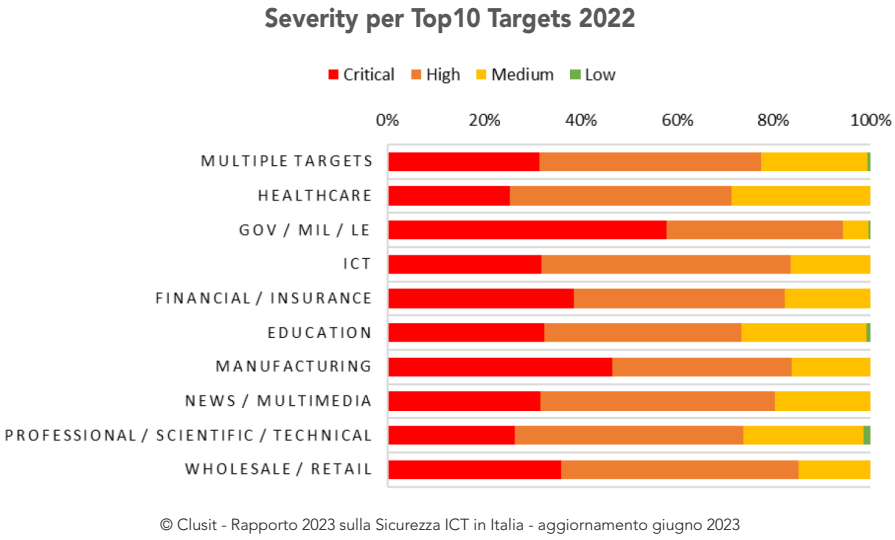


Fig. 18: *Distribuzione della Severity per prime 10 vittime 2022*

La categoria governativa / militare è quella che viene infatti impattata in misura maggiore, una tendenza già evidenziata nel 2022 e che è rimasta costante.

In crescita anche gli impatti verso il settore Healthcare, che resta un bersaglio conveniente sia per attacchi a sfondo economico che per arrecare danni ai servizi fondamentali della società.
Seguono ICT, Financial/Insurance, Education, Professional/Scientific/Technical, News/Multimedia e Wholesale/Retail.

Diminuiscono invece gli impatti verso il settore manufatturiero che, sebbene negli ultimi anni sia stato particolarmente attenzionato, viene quanto meno colpito in maniera meno severa rispetto al 2022.
Restano stabili, infine, le severity verso i Multiple targets, ulteriore conferma che le operazioni cybercriminali si stanno concentrando altrove.

Severity per tecniche di attacco

L'analisi delle severity per tecniche di attacco ci restituisce delle conferme, oltre a qualche novità.
Sebbene il ricorso al malware sia inferiore in percentuale sul totale rispetto al 2022, la criticità resta la medesima e questa tecnica continua non solo a essere la preferita dai cybercriminali, ma anche evidentemente la più efficace.

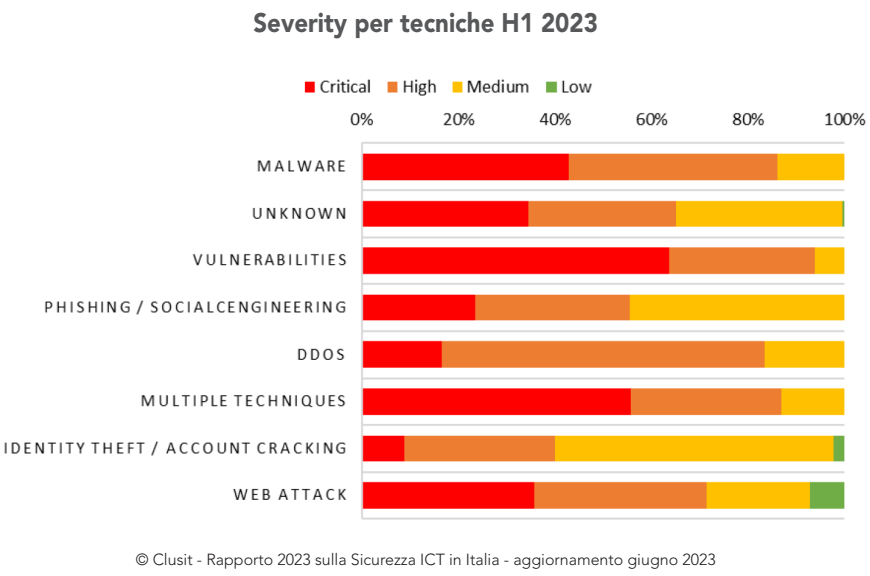


Fig. 19: *Distribuzione della Severity per tecniche di attacco nel primo semestre 2023*

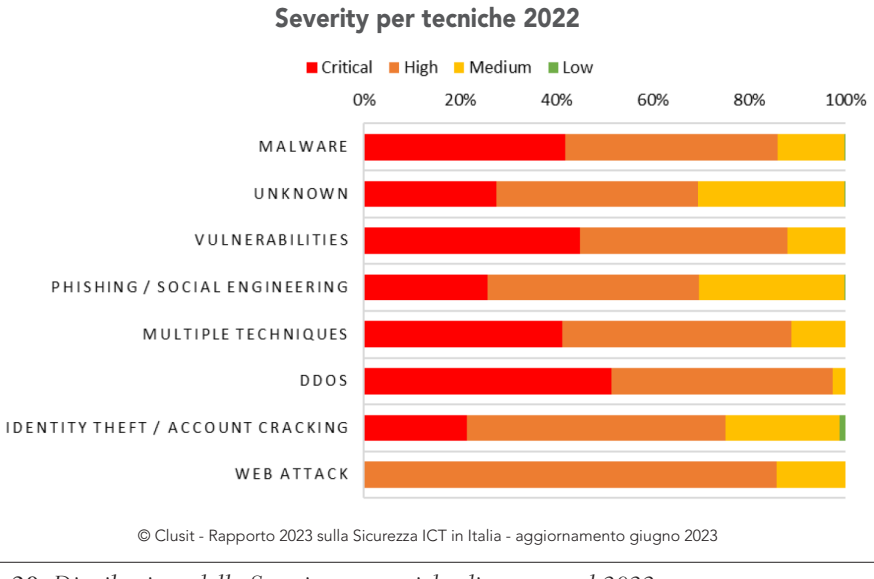


Fig. 20: *Distribuzione della Severity per tecniche di attacco nel 2022*

Aumentano in maniera significativa gli impatti derivanti dallo sfruttamento di vulnerabilità, note o meno, come nel caso degli 0-day, un dato che non stupisce alla luce dei numerosi attacchi perpetrati proprio sfruttando questa problematica nell'anno in corso.
Crescono gli impatti delle tecniche multiple, da sempre indice degli attacchi più sofisticati, che, sebbene inferiori in termini numerici nel 2023, evidentemente sono in grado di creare danni maggiori.
In aumento anche gli impatti creati dalle tecniche sconosciute ("Unknown", prevalentemente riconducibili a Data breach) e Web Attacks.
In discesa, infine, la severity per attacchi di tipo Identity Theft/Account cracking, mentre resta stabile la situazione per quanto riguarda Phishing/Social Engineering.

Analisi degli attacchi in Italia

In questa sezione offriamo un approfondimento sulla situazione italiana, con una panoramica degli incidenti di sicurezza avvenuti nello scorso semestre (H1 2023).

Lo scenario particolarmente negativo già emerso nel 2022 trova conferma anche nel primo semestre 2023: dal 2018 a giugno 2023, nel Rapporto sono stati censiti **505** attacchi noti di particolare gravità che hanno coinvolto realtà italiane, di cui ben **132** (**il 26%!**) si sono verificati solo nei primi 6 mesi del 2023.
Pertanto, come è possibile vedere nel grafico (**Fig. 21**), il dato complessivo 2023 potrebbe non solo confermare la linea di tendenza degli ultimi anni, ma anche superarla nettamente, in continuità con quanto avvenuto nel 2022.

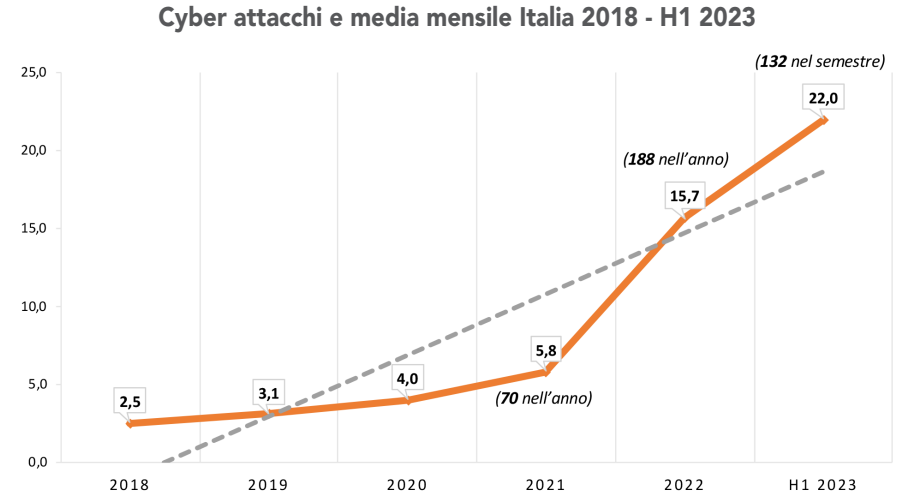


Fig. 21: *Distribuzione dei cyber attacchi e media mensile in Italia nel periodo 2018-H1 2023*

La media mensile – dopo aver registrato nei primi anni di analisi un valore abbastanza contenuto – passa da 15,7 attacchi al mese rilevati nel 2022 a ben **22** attacchi al mese nel primo semestre 2023. Tale tasso di crescita è uno dei principali elementi di preoccupazione per il nostro paese: in tutto il 2022 erano stati rilevati **188** attacchi, che costituivano già un record negativo per il nostro Paese, segnando una crescita del **169%**, quando a livello mondiale si registrava una (già grave) impennata del 21% anno su anno, come emerge dalla **Fig. 22**.

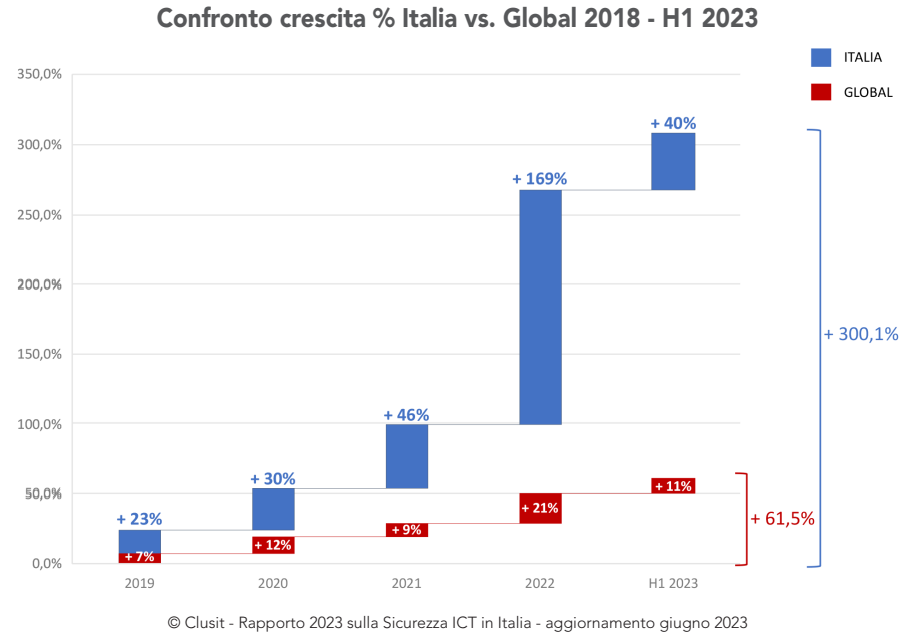


Fig. 22: *1Confronto crescita percentuale Italia vs. Global nel periodo 2018-H1 2023*

Il primo semestre 2023 segna una riduzione della crescita degli attacchi a livello globale, che torna ad attestarsi all'11%, poco sopra al trend anno su anno registrato dal 2019 al 2021. In Italia, al contrario, nel I semestre 2023 registriamo ancora **una crescita del 40%**, **quasi 4 volte superiore al dato globale,** analogamente a quanto avvenuto nel 2021.

Se da un certo punto di vista si potrebbe asserire che stiamo osservando un miglioramento rispetto al 2022, analizzando il grafico di **Fig. 23** è possibile notare come dal 2019 a oggi la crescita percentuale anno su anno in Italia è sempre stata maggiormente sostenuta rispetto al resto del mondo, passando da **3,2 volte la crescita mondiale** 2019 su 2018, a 5 volte nel 2021, **ben 8 volte tanto il ritmo di crescita nel mondo nel 2022**, per tornare a **3,7 volte** del I semestre 2023.

È in conseguenza di tale ritmo di crescita che l'incidenza dei dati italiani ha assunto valori preoccupanti sul campione complessivo mondiale: già nel 2022 il dato italiano rappresentava il 7,6% del totale degli attacchi considerati a livello globale, mentre nei primi 6 mesi del 2023 **gli attacchi in Italia rappresentano il 9,6% di quelli censiti nel periodo**.

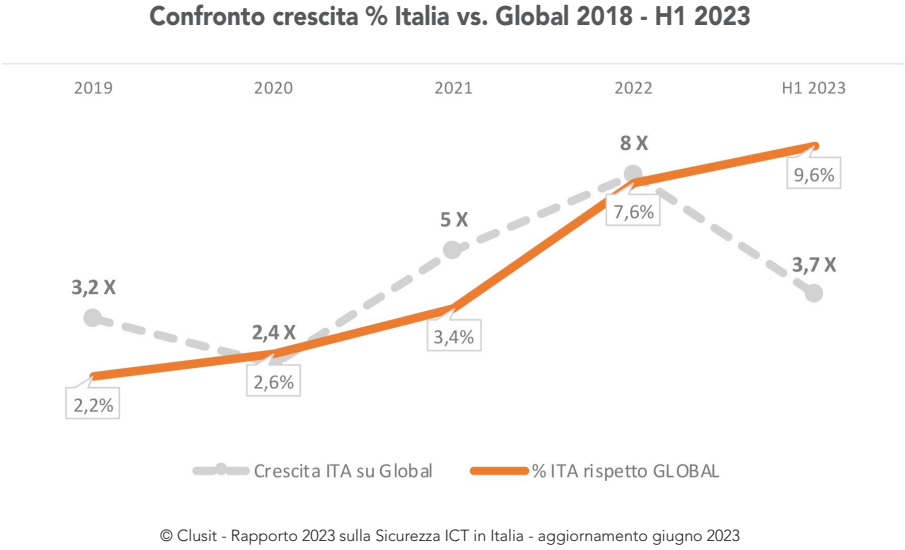


Fig. 23: *Crescita % Italia vs. Global (in arancio) ed entità della crescita italiana rispetto al trend globale (in grigio)*

Come è facile osservare in **Fig. 23**, mentre a livello mondiale dal 2019 al I semestre 2023 gli incidenti sono aumentati del 61,5%, **in Italia la crescita complessiva raggiunge il 300%.**
Questa incidenza preoccupante dell'Italia è confermata anche da report nazionali e internazionali: dalla Ricerca 2022 dell'Osservatorio Cybersecurity e Data Protection del Politecnico di Milano emerge che:

- il 67% delle grandi imprese ha subito un aumento dei tentativi di attacco rispetto all'anno precedente;
- il 14% delle grandi imprese dichiara di aver subito attacchi con conseguenze concrete.

Ancora una volta viene quindi da chiedersi, sulla base di queste informazioni, se il nostro paese stia osservando una particolare recrudescenza e attenzione da parte degli attaccanti rispetto al resto del mondo o se le nostre organizzazioni siano meno preparate a proteggersi dalle minacce informatiche: proviamo a dare qualche risposta, analizzando nel seguito i dati di dettaglio.

Distribuzione degli attaccanti per tipologia (2019 – H1 2023)

Per provare a dare una risposta, analizziamo innanzitutto la tipologia di attaccanti, indicativa delle finalità e propedeutica a capire quali fenomeni prevalenti dobbiamo tenere sotto attenzione.

Come accade a livello globale, la maggioranza degli attacchi noti in Italia si riferisce alla categoria **"Cybercrime"**, che rappresenta il **69%** del totale, con una quota in significativo calo rispetto all'anno precedente.

Sebbene il peso percentuale del Cybercrime stia diminuendo (nel 2022 costituiva il 93,1% degli attacchi), è bene però tenere presente che in termini assoluti gli attacchi sembrano invece mantenere un tasso di incessante crescita, con 91 incidenti rilevati in Italia solo nei primi 6 mesi del 2023.

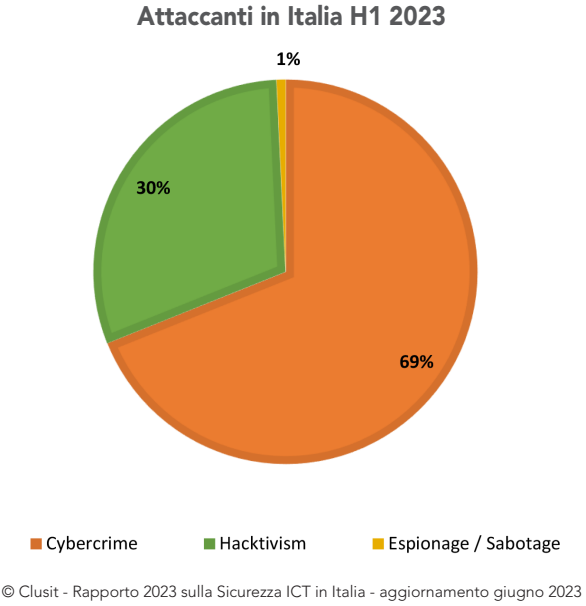


Fig. 24: *Attaccanti in Italia nel primo semestre 2023*

Crescono invece in modo decisamente rilevante gli attacchi classificati come **"Hacktivism"**, che in questo semestre si attestano al **30%** (nel 2022 costituivano il 6,9% degli attacchi). In Italia, gli incidenti afferenti a questa tipologia costituiscono una quota molto superiore rispetto a quella globale (pari al 7,7%): **oltre il 37% del totale degli attacchi con finalità "Hacktivism" è avvenuto nei confronti di organizzazioni italiane**. Si moltiplicano quindi gli attacchi dimostrativi, molto spesso perpetrati con finalità politica, ai danni di enti o aziende del nostro Paese. Analizzando nello specifico gli eventi registrati,

siamo di fronte a tutta una serie di azioni legate alla situazione geopolitica, con particolare riferimento al conflitto in Ucraina, nei quali gruppi di attivisti agiscono mediante campagne rivolte tanto al nostro Paese che alle altre nazioni del blocco filo-ucraino. Sebbene sia più che possibile un legame con il governo Russo (o più in esteso, con Paesi che stanno mantenendo una posizione ambigua nel conflitto in corso), non vi sono prove certe per classificare queste azioni come *state-sponsored attack*, pertanto come è possibile vedere, non risultano azioni afferenti alla categoria "Information Warfare".
Completa il campione l'**1%** di attacchi nella categoria "Espionage / Sabotage":per entità e numerosità, in Italia è la prima volta che si ritrovavano incidenti in questa categoria dal 2020.

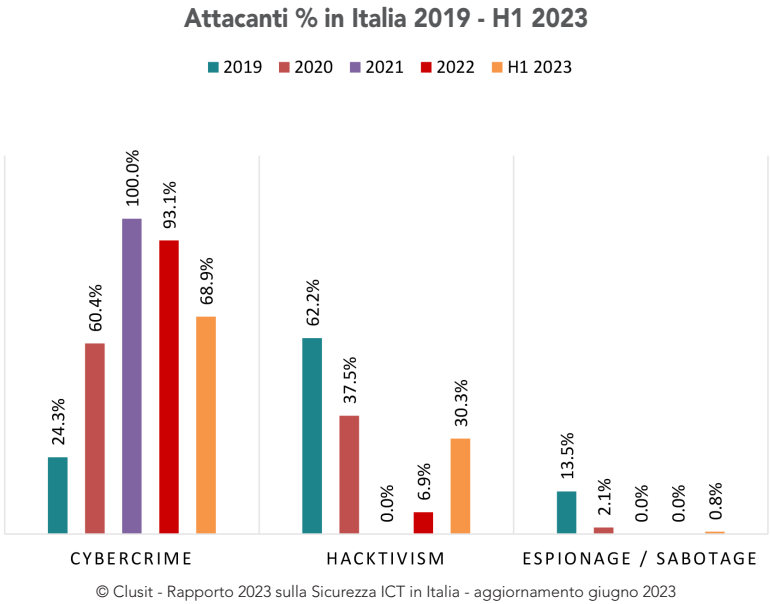


Fig. 25: *Attaccanti in Italia nel periodo 2019-H1 2023*

Distribuzione delle vittime per categoria (2019 – H1 2023)

Guardando alla distribuzione delle vittime, ancora una volta la categoria merceologica per cui si rileva un maggior numero di attacchi è **"Government"** (**23%** del totale), seguita a breve distanza da **"Manufacturing"** (**17%**).
La ripartizione è significativamente diversa rispetto a quella del campione a livello mondiale, in cui le due categorie raccolgono rispettivamente il 12% e il 5% degli attacchi (ricoprendo la terza e la settima posizione).

Gli incidenti rivolti al "Manufacturing" rilevati in Italia, in particolare, rappresentano il **34%** del totale degli attacchi censiti a livello globale nei confronti di questo settore.

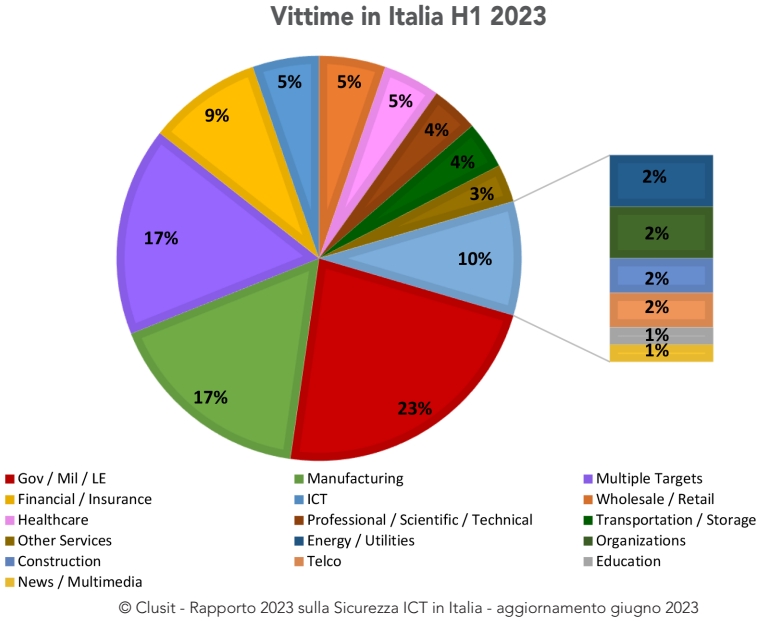


Fig. 26: *Distribuzione delle vittime in Italia nel primo semestre 2023*

Se non è possibile sostenere, semplicemente guardando i dati, che i criminali guardino al nostro paese con maggiore interesse rispetto ad altri, è tuttavia evidente che la percentuale di successo delle loro attività in Italia sia ascrivibile tanto alle peculiarità del tessuto economico e sociale del Bel Paese, quanto ai fattori che influenzano l'evoluzione della digitalizzazione delle imprese e delle pubbliche amministrazioni.
L'accelerazione verso il digitale, forte dell'impulso dato dalla pandemia, ha infatti coinvolto mai come in questi ultimi tre anni le piccole e medie imprese italiane, che da questi dati risultano evidentemente impreparate a sostenere la crescente pressione dei cyber-attack.
A conferma di questo fatto, rispetto al 2022, si rileva un probabile aumento del numero degli attacchi per quasi tutte le aree merceologiche prese in esame, come dimostra una sempre più uniforme distribuzione del grafico a torta. Anche in questo caso, è d'obbligo sottolineare come **la magnitudine delle conseguenze per le vittime non sia correlata alla complessità degli attacchi stessi**.

Il settore che registra il maggiore incremento di incidenti gravi rilevati è "**Financial / Insurance**" (Fig. 27), che balza al quarto posto, con il **9%** di attacchi (era il 3,7% nel 2022). **Il numero di attacchi rivolti a vittime in questo ambito nei primi 6 mesi dell'anno supera il totale degli attacchi avvenuti in tutto il 2022**. Analizzando gli attacchi, uno dei fattori che incide maggiormente su questo trend negativo è la comparsa di un numero sempre più elevato di attori (ad esempio le cosiddette fintech) e il ricorso sempre più ampio all'esternalizzazione di processi e servizi bancari e assicurativi, che rendono questo mercato sempre più frammentato e vulnerabile ad azioni non più rivolte alle organizzazioni più blasonate, che per entità di investimenti e competenze sarebbero probabilmente meno vulnerabili. Se questo andamento si confermasse anche per il prossimo semestre, il tasso di crescita annuo sarebbe del **243%**.
Significativo anche l'aumento riscontrato dalla categoria "**Multiple Targets**", che passa dal 10,6% del 2022 al **16,7%** del primo semestre 2023; tale aumento è in contro-tendenza rispetto al resto del mondo, che vede una riduzione dal 22% del 2022 al 20% nel I semestre 2023. Si tratta di attacchi non mirati, campagne generalizzate, che in Italia sono ancora oggi causa di incidenti con effetti consistenti, sebbene nel Bel Paese **incida in modo meno rilevante che nel resto del mondo** (al 20% del totale delle tipologie di vittime). Anche in questo caso valgono le osservazioni fatte precedentemente: se l'andamento si confermasse anche per il prossimo semestre, la crescita sarebbe del **120%**.
Aumentano, sebbene in maniera più contenuta, anche le quote dei settori "Transportation / Storage" e "Gov / Mil / Le", mentre diminuisce leggermente il peso percentuale di "Manufacturing" e "ICT" (sebbene, in entrambi i casi, gli attacchi in valore assoluto risultino in aumento).

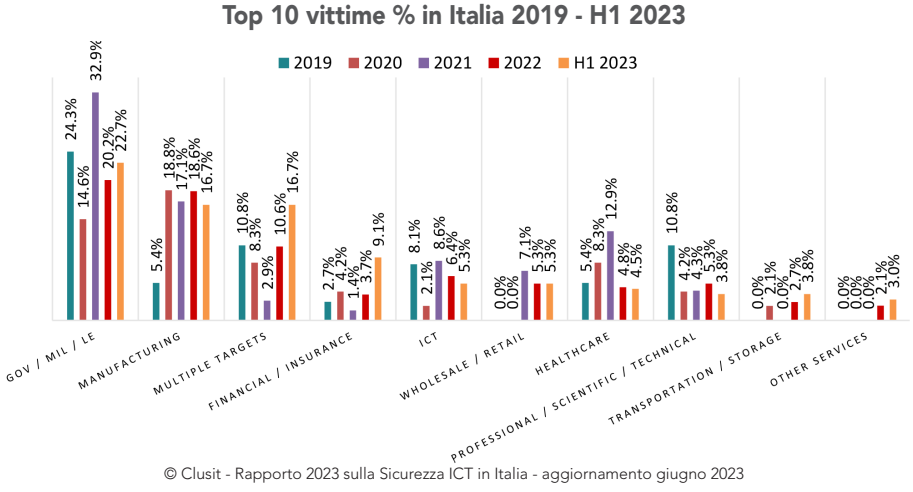


Fig. 27: *Top 10 vittime in Italia nel periodo 2019-H1 2023*

Al contrario, il posizionamento del settore **Healthcare** nel novero delle vittime in Italia si mantiene costante e, in controtendenza con il dato globale dove il mondo della sanità mantiene saldamente il triste primato del settore specifico più colpito, nel nostro Paese fortunatamente ha arrestato da qualche tempo la crescita in classifica. Punto di attenzione: in valore assoluto, all'aumentare del numero complessivo degli attacchi nel I semestre 2023, anche questo settore in Italia risulta più colpito che in passato, con un **incremento del 33% anno su anno**. Questo dato è coerente con quanto accade a livello mondo, dove la distribuzione tra le vittime sale dal 12% al 14%, con un **incremento superiore al 30% degli attacchi subiti**.

Distribuzione delle tecniche di attacco (2019 – H1 2023)

Anche l'analisi delle tecniche di attacco aiuta a comprendere le cause sottostanti l'elevata crescita degli attacchi subiti dalle nostre imprese e istituzioni.

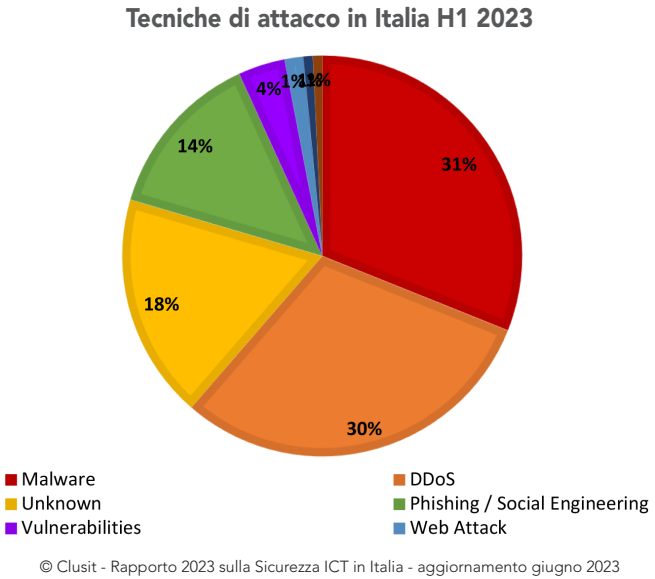


Fig. 28: *Tecniche di attacco in Italia nel primo semestre 2023*

Rispetto a quanto rilevato nel 2022, il **malware** (e in questa categoria il c.d. *ransomware*) continua a rappresentare la principale tecnica di attacco utilizzata dai criminali (**31%**), ma in modo molto meno consistente (era pari al 53% nel 2022) e di **4 punti percentuali inferiore al dato globale**.

In valore assoluto, il numero di attacchi malware non subisce un calo significativo, tuttavia la minore percentuale è indicativa del fatto che stiamo osservando, per la prima volta da quando è esploso il fenomeno del ransomware, un cambiamento rilevante nelle modalità e nelle finalità perseguite dagli attaccanti, che evidentemente riescono a ottenere con maggiore efficacia i loro scopi utilizzando tecniche diverse.
A riprova di questo fatto, sono invece i **DDoS** a registrare una notevole crescita, passando dal 4% del 2022 allo spaventoso **30%** del primo semestre 2023, una quota 5 volte superiore. L'incidenza di attacchi di questa tipologia in Italia è estremamente più elevata rispetto a quella registrata nel campione complessivo, che si ferma al 7,9%: **le vittime italiane hanno subito un numero maggiore di attacchi DDoS, tanto da registrare circa il 37% del totale di tali eventi** censito nel campione.
Gli attacchi DDoS sono una delle tecniche più utilizzate dagli hacktivist per raggiungere i loro obiettivi ed è quindi evidente, nel panorama italiano, la correlazione tra l'aumento di attacchi che sfruttano questa tecnica e la crescita della quota di incidenti riconducibile proprio alla tipologia "Hacktivism". Come noto, gli attacchi DDoS mirano a rendere inaccessibile/inutilizzabile un servizio online sovraccaricandone le risorse (di rete, di elaborazione, di memorizzazione, …). Gli hacktivist possono utilizzare questa tecnica per interrompere le attività di un'azienda o di un'istituzione, con lo scopo di attirare l'attenzione mediatica su una causa politica o sociale, esercitando così pressione sulla vittima e mettendone in luce la scarsa capacità di difesa.

Aumenta anche il dato degli attacchi di tipo phishing e ingegneria sociale, che – diversamente da quanto rilevato nel 2022 – in Italia risulta incidere in maniera maggiore rispetto al resto del mondo (**14% vs 8,6% globale**), indice di una forte necessità di sensibilizzazione e aumento della consapevolezza rispetto alle minacce cyber da parte degli utenti che hanno quotidianamente a che fare con i sistemi informatici.
Diminuisce la percentuale di incidenti basati su vulnerabilità note (**4%** vs 6% nel 2022), mentre compare una quota, seppur contenuta, di "web based attack" (**1,5%**). Sempre tenendo conto l'elevata quantità di situazioni dove non è stato possibile identificare la tecnica primaria dell'attacco (**Unknown, 18%** rispetto al 21% nel mondo), tali attacchi sono certamente presenti, ma ancora in quantità limitata.

Come già messo in luce nel 2022, anche in questi 6 mesi si conferma la pressoché assenza in Italia della categoria *Multiple Techniques,* che, da qualche anno nel nostro campione, include gli attacchi più avanzati. Ciò in parte conferma l'ipotesi precedentemente espressa per cui l'aumento degli attacchi in Italia sia con-causato da forti limiti nella capacità di difesa delle vittime.

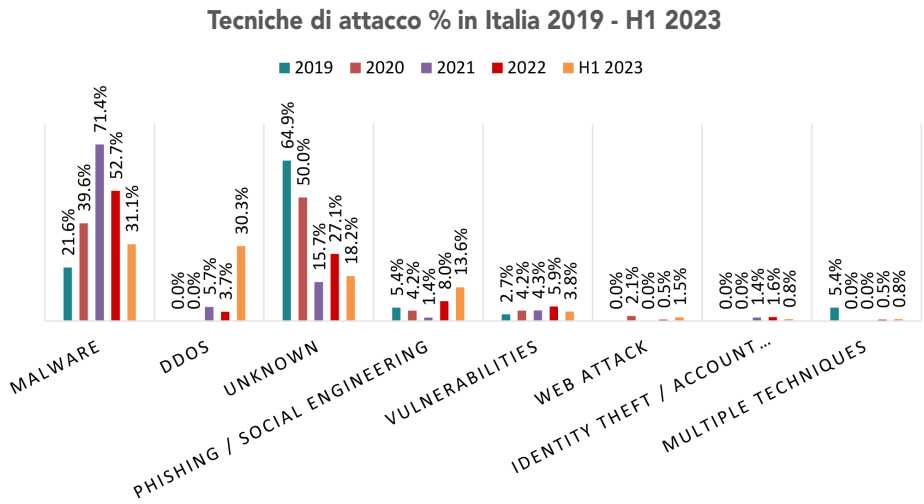


Fig. 29: *Tecniche di attacco in Italia nel periodo 2019-H1 2023*

Analisi della "Severity" degli attacchi

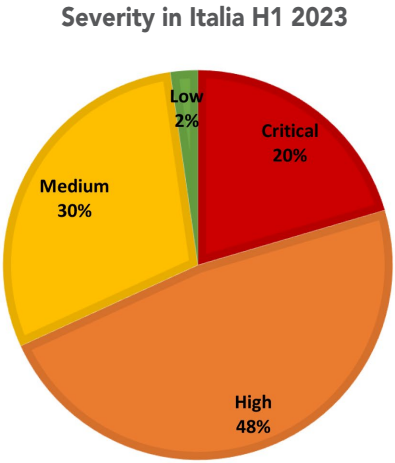


Fig. 30: *Severity degli attacchi in Italia nel primo semestre 2023*

Dal punto di vista della criticità degli attacchi, il dato italiano segue in questo semestre un andamento peculiare: a differenza di ciò che avviene a livello globale, infatti, gli incidenti di tipo "Critical" si fermano al **20%** (vs 40% globale), mentre la quota maggiore di attacchi fa riferimento a una severity "High" (**48%** in Italia vs 38% globale) e "Medium" (**30%** in Italia vs 21% globale). Completa il quadro un 2% di incidenti con criticità bassa.

In termini di severity, il quadro italiano nei primi 6 mesi del 2023 appare quindi più roseo rispetto al dato globale, con un numero minore di attacchi con severità massima.
Possiamo quindi concludere che in Italia siano aumentati gli attacchi "di disturbo", con severity limitata, che riescono però sempre più spesso ad andare a buon fine, e questo dato è coerente con la crescita dell'Hacktivism e degli attacchi di tipo DDoS, che hanno tipicamente queste caratteristiche. Si tratta comunque di attacchi che possono causare danni economici per le vittime che li subiscono, oltre che avere un effetto rilevante in termini di reputazione, poiché – come visto – vengono spesso messi in atto con scopo dimostrativo.

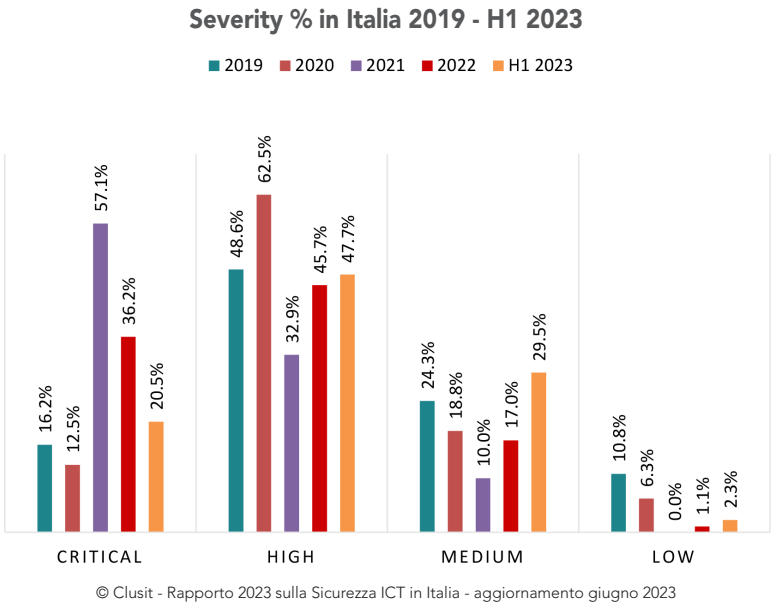


Fig. 31: *Severity degli attacchi in Italia nel periodo2019-H1 2023*

Guardando alla progressione storica, si nota un assestamento della severity "High", ma anche una diminuzione degli attacchi a massima criticità, che passano dal 36% del 2022 al 20% di questo semestre, in favore di un aumento degli incidenti con severità media (17% nel 2022 vs 29,5% del primo semestre 2023).

Possiamo sperare che la crescita sul mercato dei servizi di SOC e l'attenzione apportata dalle istituzioni, in primis l'Agenzia per la Cybersicurezza Nazionale, al tema della gestione degli incidenti e delle crisi, stiano sostenendo il riallineamento del dato italiano a quello internazionale.
D'altro canto, è sempre bene tenere a mente che gli eventi a maggiore gravità costituiscono ancora una percentuale estremamente rilevante (68% complessivo tra le Severity Critical e High), dato che ci ricorda che la strada da percorrere è ancora molto lunga e tortuosa.

Analisi degli attacchi alle organizzazioni governative e alle pubbliche amministrazioni

Sin dalla precedente edizione, il Rapporto comprende l'analisi verticale della situazione globale del settore delle organizzazioni governative e delle pubbliche amministrazioni, sia centrali che locali escluso il comparto difesa). Questo approfondimento è di grande importanza perché la situazione del settore pubblico si sta facendo particolarmente critica negli ultimi anni: da un lato, infatti, aumenta l'attenzione sulla sensibilità di tale settore, che proprio per la sua rilevanza sarà a breve direttamente interessato dalle misure di sicurezza previste dalla direttiva europea NIS2; dall'altro, si registra un significativo incremento degli attacchi, alla cui storica origine criminale si è andata sovrapponendo quest'anno una forte matrice politico-ideologica conseguente al conflitto russo-ucraino. Vediamo quindi nei grafici dei paragrafi seguenti la situazione del settore pubblico aggiornata agli eventi del primo semestre 2023, ricordando che per rendere confrontabili i valori dell'ultimo semestre con quelli degli anni precedenti, che sono espressi su base annuale, tutti i dati sono riportati non in valore assoluto ma normalizzati su base mensile o annuale, come indicato nei singoli grafici.

Analisi dei principali cyber attacchi noti a livello globale del 2018-2022 e del primo semestre 2023

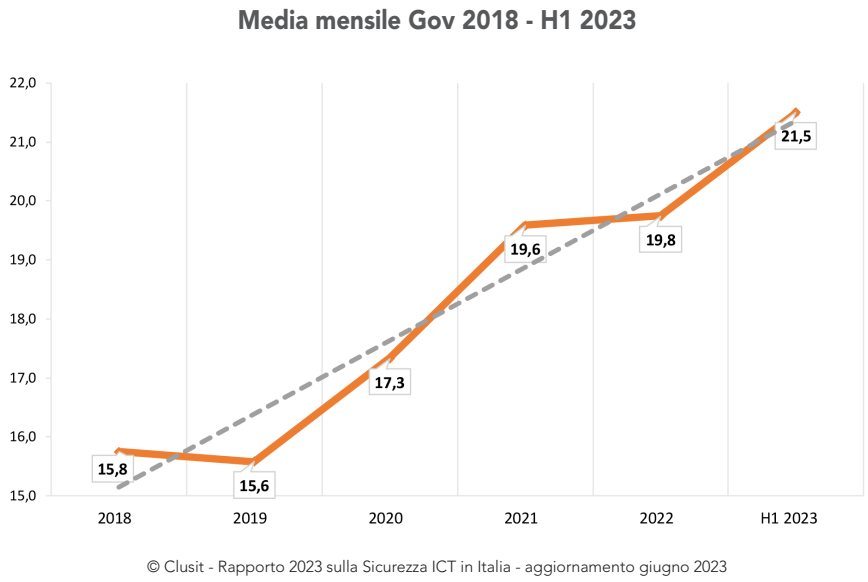


Fig. 32: *Media mensile degli attacchi al settore GOV (CENTRAL/LOCAL) nel periodo 2018- H12023*

Tra il 2018 e il primo semestre 2023, il campione ha incluso 1.185 attacchi noti di particolare gravità che hanno coinvolto realtà governative nel mondo. Dopo una crescita particolarmente significativa fra il 2019 e il 2021, il numero di attacchi gravi è rimasto pressoché costante nel 2022, per risalire poi significativamente nel primo semestre 2023. Nell'arco dei cinque anni si è comunque passati dai 15,8 attacchi per mese del 2018 ai 21,5 del primo semestre 2023, con un incremento complessivo del 36%.

Distribuzione degli attaccanti per tipologia (2019 – H1 2023)

La stragrande maggioranza degli attacchi condotti verso il settore pubblico è ancora relativa alla categoria **"Cybercrime"**, che tuttavia è scesa in questo primo semestre del 2023 dal 67% al 59% del totale: ha infatti improvvisamente preso quota la categoria **"Hacktivism"** la quale **ha quasi triplicato la sua presenza dallo scorso anno, passando dal 12% del 2022 al 30%** del primo semestre 2023.- Seguono, molto distaccate, **"Espionage/ Sabotage"** che è quasi dimezzata passando dal 13% al 8%, e **"Information Warfare"** crollata dall'8% al 3%.

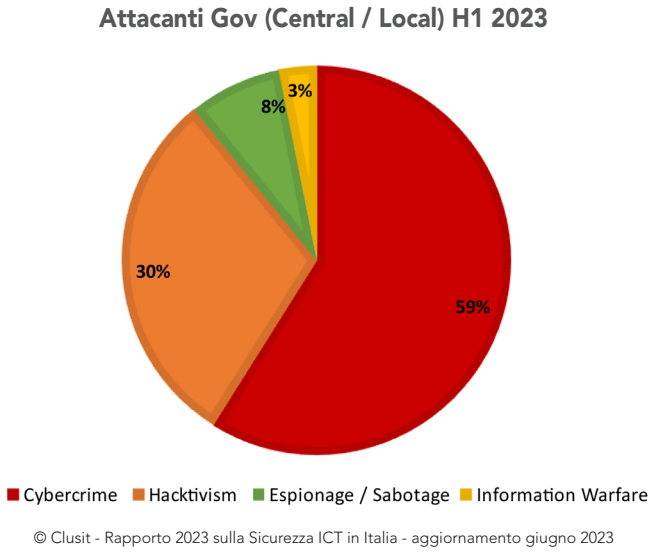
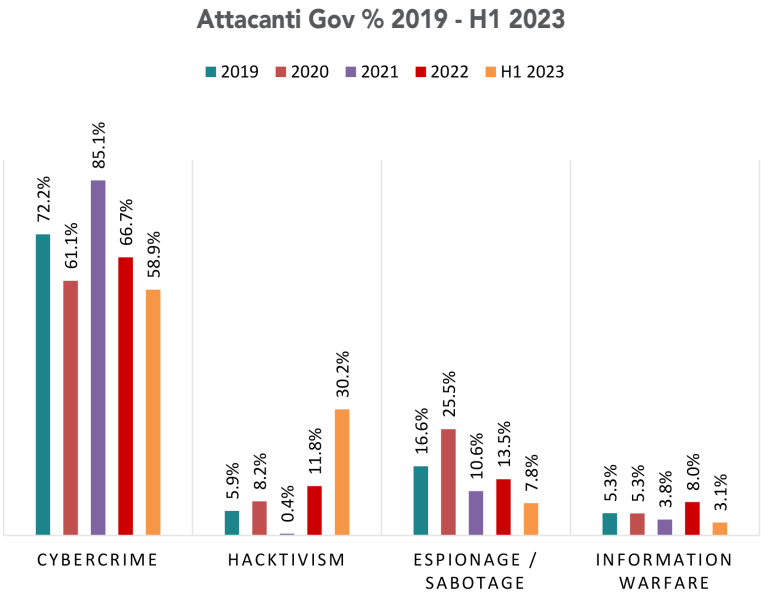


Fig. 33: *Distribuzione degli attaccanti al settore GOV (CENTRAL/LOCAL) nel primo semestre 2023*

In questi dati **si legge chiaramente l'influenza del conflitto russo-ucraino**, le cui tracce già erano evidenti durante il 2022, che tuttavia ha provocato nel primo semestre 2023 un ulteriore enorme incremento di attacchi ideologici e politici sferrati dagli attivisti contro organizzazioni governative appartenenti anche a Paesi non direttamente coinvolti nella guerra, con attacchi dimostrativi e di supporto verso l'una o l'altra parte.



© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia - aggiornamento giugno 2023

Fig. 34: *Distribuzione degli attaccanti per il settore GOV (CENTRAL / LOCAL) nel periodo 2019-H12023*

Distribuzione generale delle vittime per area geografica (2019 – H1 2023)

La distribuzione geografica delle vittime vede nuovamente il continente americano maggiormente sotto attacco, come storicamente sempre accaduto con l'unica eccezione del 2022 quando Europa e americhe si erano trovate perfettamente in parità. Nel primo semestre 2023 invece il vecchio continente scende dal 43% al 37% degli attacchi globali diretti verso il settore governativo, mentre il nuovo continente sale dal 43% al 48%. L'Asia rimane distaccatissima e costante all'11%, l'Oceania resta al 2% e il rimanente 1% è ancora costituito da attacchi diretti verso bersagli multipli.

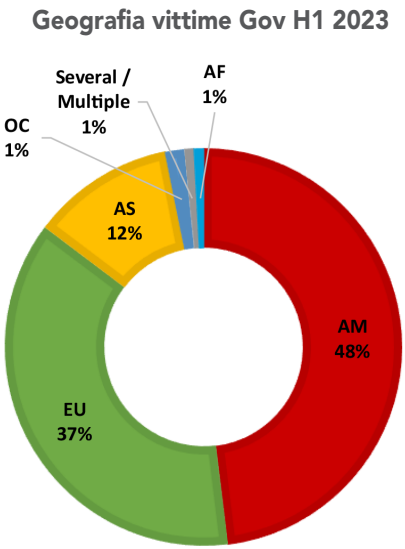


Fig. 35: *Distribuzione geografica delle vittime nel settore GOV (CENTRAL / LOCAL) nel primo semestre 2023*

È interessante notare, come si vede dal grafico in **Fig. 36**, che il primo semestre del 2023 appare proprio come un punto di svolta nella distribuzione geografica delle vittime, interrompendo quella che per le Americhe era stata una diminuzione continua negli ultimi anni, e per l'Europa una crescita continua. Quindi, almeno per quanto concerne le organizzazioni governative e le pubbliche amministrazioni, sembra che gli sviluppi recenti del conflitto rosso-ucraino abbiano nuovamente spostato gli attacchi dall'Europa al continente americano.

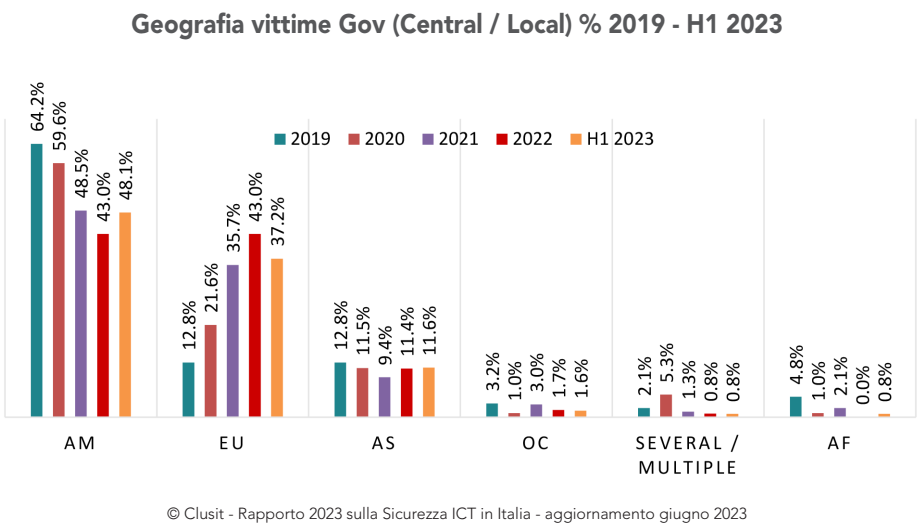


Fig. 36: *Distribuzione geografica delle vittime nel settore GOV (CENTRAL / LOCAL) nel periodo 2019-H1 2023*

Distribuzione delle tecniche di attacco (2019 – H1 2023)

Per quanto riguarda le tecniche utilizzate, la situazione è molto cambiata dallo scorso anno: nel primo semestre 2023, infatti, la modalità primaria di attacco è stata il Distributed Denial of Service, che ha quasi triplicato la sua presenza passando dal 12% del 2022 al 31% di questa prima metà anno. Al secondo posto troviamo il malware, sceso dal 34% del 2022 al 25% di quest'anno. Al terzo posto lo sfruttamento di vulnerabilità, che ha quasi raddoppiato la propria presenza passando dal 9% del 2022 al 17% di quest'anno. Gli attacchi per i quali la modalità non è nota o non è stata accertata sono così scesi dal secondo posto del 2022 al quarto del 2023, passando dal 27% al 12%. In discesa, e molto distaccati, risultano gli attacchi basati sul social engineering (3%).

Il dato più rilevante che si nota esaminando l'evoluzione storica delle tecniche d'attacco è la straordinaria crescita del DDoS in questo ultimo semestre, che prosegue una tendenza iniziata già lo scorso anno: ciò si inquadra perfettamente nel contesto geopolitico in corso, nel quale il conflitto russo-ucraino continua a provocare un'ondata di attacchi ideologici condotti principalmente verso organizzazioni governative mediante lo strumento del Denial of Service, tra i più efficaci per generare conseguenze mediaticamente rilevanti tramite l'interruzione di servizi di pubblica utilità. Contestualmente **sono aumentati anche gli attacchi basati sullo sfruttamento delle vulnerabilità e quelli basati sul web**, mentre sono diminuiti quelli "più sofisticati" basati su social engineering e identity theft.

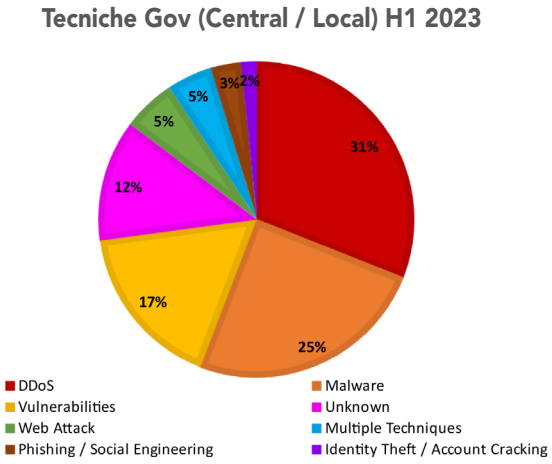


Fig. 37: *Distribuzione delle tecniche di attacco nel settore GOV (CENTRAL / LOCAL) nel primo semestre 2023*

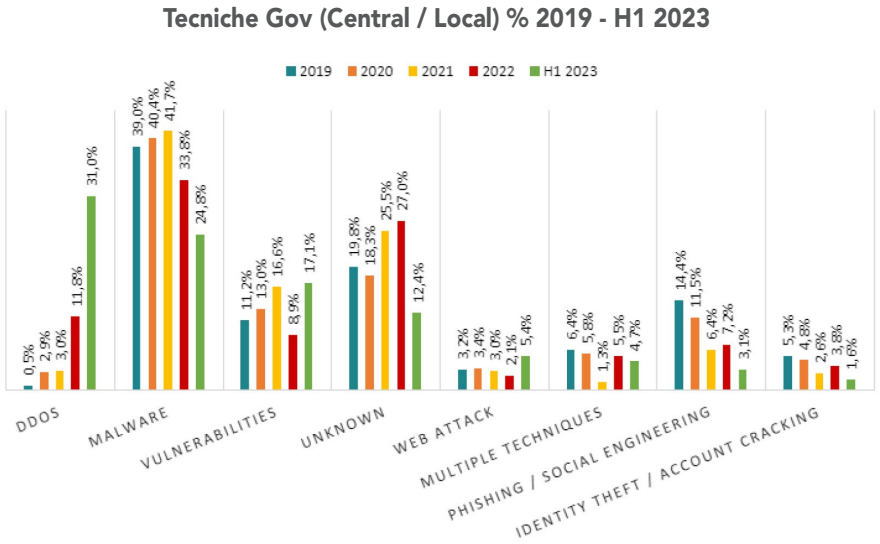


Fig. 38: *Distribuzione delle tecniche di attacco nel settore GOV (CENTRAL / LOCAL) nel periodo 2019-H12023*

Analisi della "Severity" degli attacchi (2019 – H1 2023)

Gli attacchi condotti verso il settore pubblico, come si vede dal grafico in Fig. 39, sono ancora caratterizzati come l'anno scorso da una Severity assai maggiore rispetto all'insieme di tutti gli attacchi: ben il 52% è infatti classificato come **critico**, contro il 40% del dato globale, e il 40% è classificato **alto** contro il 38% del dato globale. Si conferma quindi che **chi attacca il settore pubblico sia generalmente assai più preparato, motivato ed efficace nelle sue azioni, puntando a ottenere impatti decisamente più elevati della media**.

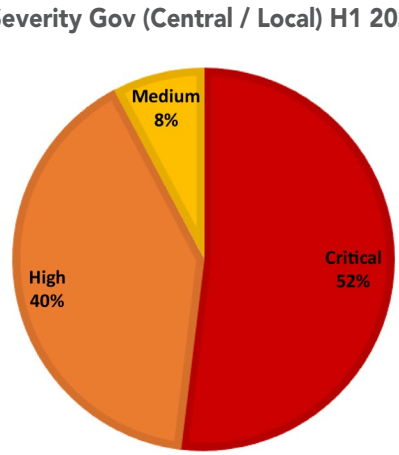


Fig. 39: *Distribuzione della Severity degli attacchi nel settore GOV (CENTRAL / LOCAL) nel primo semestre 2023*

Analizzando tuttavia il grafico evolutivo si nota una significativa ridistribuzione della Severity nel settore pubblico rispetto all'anno scorso, quando gli attacchi classificati come critici erano il 56% e quelli classificati come alti erano il 36% del totale. Questa diminuzione in percentuale degli attacchi critici è un fenomeno storicamente nuovo, e rappresenta un'inversione di tendenza anch'essa ascrivibile alla situazione conseguente al conflitto russo-ucraino ben leggibile dai grafici precedenti: in pratica l'**aumento massiccio degli attacchi dimostrativi e ideologici di bassa intensità basati sul DDoS** ha comportato la conseguente diminuzione media della criticità degli attacchi stessi.

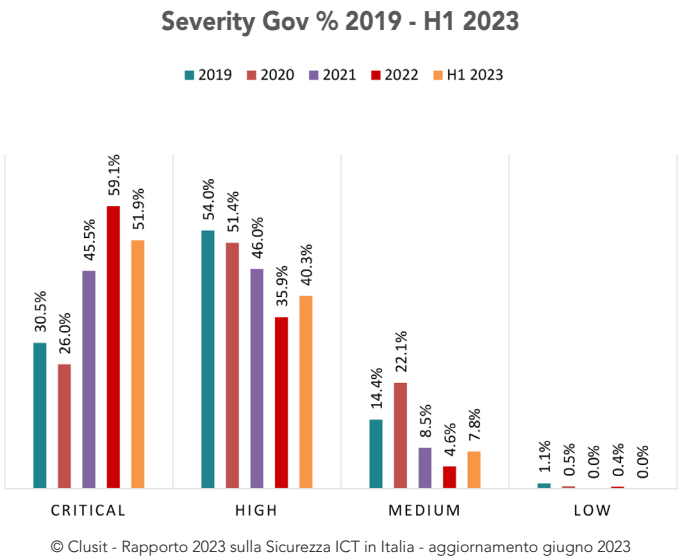


Fig. 40: *Distribuzione della Severity degli attacchi nel settore GOV (CENTRAL / LOCAL) nel periodo 2019-H12023*

Appendice metodologica

Le decisioni in ambito cybersecurity sono basate principalmente su analisi dei rischi, legate anche a valutazioni di scenario. Che si tratti di attivare o non attivare un servizio, implementare o non implementare un controllo, accettare o non accettare un rischio, a fine giornata il manager dovrà aver preso una decisione, e lo farà con i dati che ha a disposizione. Non decidere è comunque una decisione, di solito la peggiore, e un lusso che il manager non si può permettere. Quello che possiamo fare, come Clusit, è fornirgli i migliori dati che possiamo raccogliere, insieme agli strumenti per valutarne la qualità e i limiti.
L'analisi dei principali cyber attacchi noti a livello globale si scontra necessariamente con la disponibilità di un campione parziale e non necessariamente rappresentativo dello scenario complessivo di rischio di attacco. Per valutare il valore dei dati raccolti e delle analisi effettuate, è necessario chiedersi prima di tutto quali siano le modalità di raccolta e di analisi, e quali quindi i limiti dei risultati ottenuti.
I dati illustrati si riferiscono a incidenti riportati in fonti di informazione pubbliche. Da quando, nel 2012, è iniziata questa attività, il numero di fonti utilizzato è molto aumentato, e le modalità di ripulitura dei dati, ad esempio dalle duplicazioni, sono migliorate. L'utilizzo di fonti pubbliche introduce comunque un *bias* rispetto alla totalità degli incidenti occorsi e, quindi, all'esposizione ai rischi. In questa sezione cerchiamo di dare una maggiore visibilità a questi possibili bias, in modo che se ne possa tenere conto.

Per contro, quando un attacco arriva a essere pubblicato sulle fonti analizzate, di solito le caratteristiche descritte risultano essere abbastanza affidabili. Quando non lo sono, normalmente le parti interessate tendono a pubblicare o chiedere la pubblicazione di informazioni corrette.
Gli incidenti analizzati rappresentano certamente un campione significativo di quelli resi pubblici dalle fonti principali. Fra quelli resi pubblici, rimangono quindi esclusi incidenti riportati ad esempio da testate minori, locali o di Paesi del mondo non coperti dall'analisi. Nel corso degli anni, è aumentata l'attenzione alla copertura più ampia delle fonti italiane anche minori. In questo senso, possiamo avere quindi un bias verso la rappresentatività dei paesi occidentali maggiormente presenti (ad esempio, gli Stati Uniti) e verso l'Italia. Questo aspetto, se correttamente gestito, può essere più di aiuto che di svantaggio per i manager italiani.

Fra gli incidenti noti pubblicamente, rimangono esclusi quelli che non hanno avuto una rilevanza tale da essere inclusi nelle fonti analizzate. Si tratta per lo più di incidenti di lieve entità, o che interessano aziende di minori dimensioni e che non hanno particolarità tali da renderli di interesse per le fonti principali. Possono essere, ad esempio, attacchi malware di minore entità che, per chi deve gestire la sicurezza di un'organizzazione, aggiungono, probabilmente, poco rispetto alla valutazione della necessità di adottare una baseline di misure di sicurezza che è ormai da considerare indispensabile.
Ci sono poi incidenti che, pur essendo divenuti noti in contesti circoscritti, non hanno raggiunto le fonti pubbliche. Anche dove vi siano obblighi di notifica, questo non vuole dire infatti che tutti gli incidenti siano notificati (dipende da caratteristiche dell'incidente e dalla normativa locale e di settore), e soprattutto, le autorità in generale non rendono pubblici gli incidenti notificati. Lo stesso vale per le denunce alle autorità di polizia, alle assicurazioni, e per i dati raccolti dai fornitori di connettività e di servizi di gestione incidenti. Si tratta di dati interessanti, ma in generale disponibili solo a questi soggetti, e quindi molto frammentati. Alcuni li pubblicano a loro volta sotto forma di statistiche. Il Clusit collabora con le autorità e organizzazioni interessate a pubblicare questi dati all'interno del Rapporto, ma i dati rappresentano comunque viste diverse e più verticali su specifici ambiti, e quindi non sono integrati in questa analisi, ma pubblicati in altre parti del Rapporto, dando loro anche la giusta e specifica visibilità.

Nel campione di questa analisi sono certamente meglio rappresentati gli attacchi realizzati per finalità cyber criminali o di hacktivism rispetto a quelli derivanti da attività di cyber espionage, che tendono a essere condotti con grande cautela e pertanto emergono più difficilmente. Questo può essere un limite importante da considerare: gli attacchi che colpiscono la riservatezza dei dati sono sicuramente sottorappresentati perché, a meno che gli attaccanti per qualche motivo pubblichino l'informazione, le stesse organizzazioni colpite potrebbero non averne evidenza. Si tratta di *known unknown* rispetto ai quali è difficile avere dati statisticamente significativi. Anche venendone a conoscenza, le organizzazioni

colpite potrebbero avere interesse a non darne evidenza a nessuno. Un tema analogo è legato alle attività di information warfare, che possono essere condotte con altrettanta cautela, anche per non esporre gli strumenti utilizzati [2]. In questi casi, una delle parti potrebbe avere interesse a dare evidenza dell'attacco per motivi di propaganda, ma può essere difficile validare la veridicità di quanto affermato. Dove non vi siano sufficienti conferme sulle caratteristiche dell'attacco, o addirittura sul fatto stesso che l'attacco sia avvenuto, l'attacco non viene incluso nell'analisi.

Nel complesso, quindi, possiamo considerare i dati di questa analisi rappresentativi per la maggior parte degli attacchi di grandi dimensioni, con una sottostima difficile da quantificare in termini di attacchi banali o di lieve entità, e di attacchi, come quelli di cyber espionage, che possono facilmente non essere né rilevati né pubblicizzati.

In termini numerici, il campione analizzato è ormai piuttosto consistente, e si può quindi considerare rappresentativo di quanto reso pubblico. Le analisi fatte sul campione stesso danno quindi una rappresentazione chiara di quanto si sa, e possono essere utilizzate dai manager per avere quel quadro della situazione complessiva a livello globale che è sempre più necessario per definire le strategie di un'organizzazione in tema di cyber security.

[2] Salvo quando vengano esposti per errore, come nel caso di Stuxnet

Attività e segnalazioni della Polizia Postale e delle Comunicazioni nel primo semestre del 2023

Si elencano di seguito le principali attività svolte nel primo semestre del 2023 dalla Polizia Postale e delle Comunicazioni nell'ambito della prevenzione e del contrasto di una vasta ed eterogenea serie di attacchi informatici, diretti a colpire il patrimonio personale dei cittadini come l'integrità del tessuto economico-produttivo del Paese, la regolarità dei servizi pubblici essenziali come il mondo delle professioni, la sicurezza e la libertà personale di adulti e ragazzi, con particolare riferimento alla protezione dei bambini e delle persone più vulnerabili.

Centro Nazionale per il Contrasto alla Pedopornografia Online (C.N.C.P.O.)

Nel primo semestre 2023 il Centro Nazionale per il *Contrasto alla Pedopornografia Online (C.N.C.P.O.)* ha confermato il suo ruolo di punto di riferimento e di coordinamento nazionale dei Centri Operativi Sicurezza Cibernetica – COSC della Polizia Postale nel contrasto alla pedofilia e alla pornografia minorile online, oltre che a tutti gli altri reati e fenomeni che coinvolgono i minori nella rete internet.

Dall'analisi dei dati appare che il *trend* di flessione avviato nel 2022, relativo alla circolazione globale di materiale pedopornografico su circuiti internazionali, si stia man mano consolidando, mostrando come le limitazioni alla libertà individuale (*lockdown*), che avevano determinato un aumento dello scambio e della diffusione di contenuti di pornografia minorile in rete, si stia esaurendo.

In particolare, nell'ambito dell'attività di contrasto coordinata dal Centro, nel primo semestre dell'anno 2023, sono stati trattati complessivamente **1440 casi** di pedopornografia e adescamento di minori online, che hanno consentito di indagare **579 soggetti**, di cui **39 tratti in arresto** per reati connessi alla materia degli abusi tecnomediati in danno di minori.

Nell'ambito dell'attività di prevenzione svolta dal C.N.C.P.O. attraverso una continua e costante attività di monitoraggio della rete, nel periodo di riferimento, sono stati visionati **14.054 siti.** Al 30 giugno 2023 sono **2.675** i siti Internet inseriti in *black list* e oscurati, in quanto presentavano contenuti pedopornografici.

PRIMO SEMESTRE 2023 PEDOPORNOGRAFIA e ADESCAMENTO MINORI ONLINE					
Casi trattati	**Arrestati**	**Denunciati**	**Perquisizioni**	**Siti presenti in black list**	**Siti visionati**
1440	39	540	403	2675	14054

Adescamento online

Nel periodo di riferimento, le denunce relative ai casi di adescamento *online* mostrano un numero di casi stabile e costantemente più alto per le fasce di potenziali vittime che non superano i 13 anni. Giova ancora evidenziare come si tratti di bambini e ragazzi che non dovrebbero avere accesso ai *social* e che dovrebbero essere puntualmente sorvegliati dai genitori. I casi trattati sono stati complessivamente **184.**

PRIMO SEMESTRE 2023				
TOTALE		**Casi trattati vittime 0-9 anni**	**Casi trattati vittime 10-13 anni**	**Casi trattati vittime 14-17 anni**
Adescamento Online	184	20	106	58

Cyberbullismo

Nel periodo di riferimento sono stati trattati **164** di cyberbullismo.
Si registra, dunque, un andamento costante del fenomeno rispetto allo stesso periodo dell'anno precedente (160 casi nell'anno 2022); l'esiguo incremento di 4 casi, infatti, non rappresenta un elemento indicativo rispetto ad una variazione significativa del fenomeno, né può essere considerato prognostico in relazione all'andamento futuro dello stesso. Sono principalmente gli adolescenti a denunciare, talvolta anche in autonomia quando hanno compiuto i 14 anni, ma sono molti i casi in cui, secondo canali istituzionali e informali, vengono segnalati alla Polizia Postale e che coinvolgono bambini e ragazzi non ancora imputabili. La flessione del numero dei minori denunciati all'Autorità Giudiziaria per reati connessi al Cyberbullismo sembra comprovare l'idea che i casi interessino anche bambini e ragazzi più piccoli che per età non entrano nel circuito penale. La costante opera di sensibilizzazione svolta dalla Polizia Postale, presso le strutture scolastiche, e non solo, concorre a potenziale le strategie di autoprotezione delle vittime e mira a favorire maggiori livelli di consapevolezza negli adulti significativi, come strumento prioritario per prevenire e contenere il fenomeno.

CYBERBULLISMO	Primo semestre 2022	Primo semestre 2023
Casi trattati vittime 0-9 anni	11	5
Casi trattati vittime 10-13 anni	41	35
Casi trattati vittime 14-17 anni	108	124
TOTALE	**160**	**164**

Minori denunciati per Cyberbullismo	Primo semestre 2022	Primo semestre 2023
	74	56

Sextortion

Un fenomeno di elevato rischio per i minori, che interessa prioritariamente gli adolescenti, è la *sextortion*, che in passato era appannaggio del mondo degli adulti, ma che, da un paio d'anni, interessa in modo preoccupante ragazzi tra i 15 e i 17 anni. In una fase evolutiva nella quale la curiosità sessuale si intensifica, i ragazzi diventano oggetto delle attenzioni virtuali di sedicenti ragazze di bell'aspetto che, dopo uno scambio di messaggi sessualmente espliciti sui *social*, rivelano la loro identità *fake* e minacciano di pubblicare immagini sessuali private, se non si paga un riscatto. Si tratta di un fenomeno che viene poco denunciato e che però costituisce un elemento di forte minaccia nella vita di un giovane che può sentirsi in trappola tra la vergogna di essersi fidato di un contatto sconosciuto e di vedere pubblicate le immagini intime che lo riguardano e l'impossibilità di sopportare il giudizio negativo di genitori e coetanei.
Nel corso del primo semestre dell'anno sono stati trattati **66 casi,** la maggior parte dei quali nella fascia **14-17 anni,** più spesso in danno di vittime maschili.

PRIMO SEMESTRE 2023				
TOTALE		Casi trattati vittime 0-9 anni	Casi trattati vittime 10-13 anni	Casi trattati vittime 14-17 anni
Sextortion In danno di minori	66	1	10	55

C.N.C.P.O. – Attività di Polizia Giudiziaria

Si riportano di seguito, le attività investigative di maggior rilievo coordinate dal Centro Nazionale per il Contrasto alla Pedopornografia Online:

- Personale della Sezione Operativa per la Sicurezza Cibernetica della Polizia Postale e delle Comunicazioni di Bolzano, su impulso del CNCPO ha eseguito una misura di custodia cautelare in carcere nei confronti di un cittadino turco, responsabile di diffusione sui *social* di immagini, autoprodotte, a contenuto pedopornografico, che documentavano gli abusi commessi dall'uomo sul figlio di appena 2 anni.

- Il Centro Operativo per la Sicurezza Cibernetica della Polizia Postale e delle Comunicazioni di Palermo, congiuntamente a personale del CNCPO, ha tratto in arresto un 38enne per detenzione di ingente quantità di immagini e video di abusi sessuali su minori (10.000 *files*). L'uomo aveva precedenti specifici di polizia per i quali aveva già scontato una condanna. L'indagine nasce dalla segnalazione nell'ambito della cooperazione internazionale di polizia.

- ***Operazione "Shadow Man"***
  Il Centro Nazionale per il Contrasto alla Pedopornografia Online ha eseguito una custodia cautelare in carcere nei confronti di un cinquantenne produttore di materiale di pornografia minorile, da anni attivo in una comunità virtuale pedofila su TOR, ove si era distinto per il significativo contributo apportato, in termini di materiale pedopornografico, anche autoprodotto. L'operazione trae origine da complesse e lunghe indagini in modalità sotto copertura svolte sul *Darkweb* in collaborazione con Europol e la polizia britannica. L'uomo, conosciuto con lo pseudonimo di *Shadow*, per oltre un decennio era riuscito a eludere le indagini e rimanere anonimo, reiterando le condotte di violenza sessuale aggravata, commessa ai danni di minori di anni 10; di associazione per delinquere finalizzata alla diffusione di pratiche di pedofilia; di condivisione di notizie utili all'adescamento di minori e allo scambio, detenzione e diffusione di materiale pedopornografico. L'utente rappresentava un *high value target* internazionale nell'ambito delle indagini delle polizie di tutto il mondo impegnate in attività sotto copertura online nel contrasto alla pornografia minorile all'interno delle citate comunità pedofile virtuali.

- ***Operazione "Fast and Done"***
  Personale del Centro Nazionale per il Contrasto della Pedopornografia Online ha tratto in arresto un 45enne per detenzione e diffusione di materiale di pornografia minorile e violenza sessuale su minore. L'indagine trae origine da una segnalazione del collaterale australiano, relativa a un nuovo utente del *Dark Web*, verosimilmente italiano. Dall'esame dei *files* video raffiguranti abusi sessuali su un minore di 10 anni, si rilevava che la maggior parte di questi fossero autoprodotti. All'esito delle tempestive indagini, veniva identificato il responsabile, che veniva tratto in arresto in flagranza di reato, all'esito della perquisizione eseguita nei suoi confronti, per detenzione di oltre 20.000 *files*, oltre che per produzione e divulgazione di materiale pedopornografico e violenza sessuale su minore.

SEZIONE OPERATIVA

Reati contro la persona

Particolare attenzione è rivolta inoltre ai fenomeni del **revenge porn, con *113 casi trattati (di cui 16 in danno di minori), 43 persone denunciate*** e ***2 arrestate***, nonché delle **truffe romantiche,** con ***200 casi trattati (di cui 2 in danno di minori), 130 persone denunciate e 8 arrestate***. Si ritiene che molti sono i casi che rimangono sommersi e non denunciati in quanto caratterizzati da un forte coinvolgimento emotivo che provoca nella vittima un forte senso di vergogna nel raccontare quanto accaduto.
Sono stati **16** i casi di ***Codice Rosso*** che hanno visto la Polizia Postale impegnata attivamente nel contrasto dei reati contro la persona commessi attraverso la rete.

Reati contro la persona perpetrati OnLine*	GENNAIO GIUGNO 2023
Casi trattati	4877
Persone indagate	620
Persone arrestate	8

** Stalking / diffamazione online / minacce / revenge porn / molestie / sextortion / illecito trattamento dei dati / sostituzione di persona / hate speech / propositi suicidari*

Specifiche iniziative sono state rivolte all'attività di prevenzione e contrasto al fenomeno degli atti intimidatori nei confronti della categoria dei giornalisti e servizi di monitoraggio dei canali di diffusione, costituiti da siti web, piattaforme di digitali, profili e pagine presenti sui social network più noti (Facebook, Twitter, Instagram, Telegram, Pinterest e Youtube), finalizzati ad arginare la diffusione del linguaggio d'odio (hate speech).
In ultimo, ma comunque di primaria importanza, è stata l'attività rivolta all'individuazione di quelle persone che, sfruttando principalmente la cassa di risonanza che i social media offrono, hanno manifestato intenti suicidari in conseguenza dei quali sono state attivate tutte le procedure necessarie per la salvaguardia delle persone coinvolte con l'ausilio degli uffici di polizia competenti territorialmente. Nel periodo IN ESAME sono ***140***[1] le segnalazioni ricevute tramite il Commissariato di P.S. OnLine, canali di Cooperazione Internazionale di Polizia (Europol e Interpol), e social network e altrettanti gli interventi eseguiti sul territorio.

Sextortion

È un fenomeno che di solito colpisce gli adulti in modo violento e subdolo; fa leva su piccole fragilità ed esigenze personali, minacciando, nel giro di qualche click, la tranquillità delle persone.

[1] Di cui 20 rilevati dalle articolazioni territoriali della Polizia Postale e delle Comunicazioni.

Nel corso del periodo esaminato sono stati trattati **645** i casi di sextortion (di cui 66 in danno di minori), che hanno interessato in particolar modo vittime di maggiore età e più spesso di genere maschile. In taluni casi, l'azione criminosa ha generato effetti lesivi potenziati: il sentimento di vergogna che affligge la vittima trattiene la medesima a richiedere aiuto a familiari nei confronti dei quali si sentono colpevoli di aver ceduto e di essersi fidati di perfetti e "avvenenti" sconosciuti.
La sensazione di sentirsi in trappola che sperimentano le vittime è amplificata spesso dalla difficoltà che hanno nel pagare le somme di denaro richieste.

Sextortion	GENNAIO – GIUGNO 2023
Casi trattati	645
Persone indagate	70
Persone arrestate	2

ATTIVITÀ DI RILIEVO

Identificati e denunciati dalla Polizia Postale gli autori della diffamazione a mezzo internet ai danni della campionessa di nuoto sincronizzato Linda Cerruti (gennaio 2023)

Ad agosto dell'anno scorso, di rientro da una straordinaria prestazione atletica agli europei di nuoto sincronizzato che l'aveva portata a vincere otto medaglie, la campionessa Linda Cerruti aveva festeggiato postando sui social una foto in cui compariva in costume da bagno, in una classica posa del nuoto sincronizzato, esibendo le medaglie.
La foto, scattata sul molo di Noli (SV), città natale della campionessa, era stata ripresa da molte testate giornalistica e aveva attirato numerosissimi commenti, alcuni dei quali palesemente diffamatori e sessisti che l'atleta, amareggiata, aveva deciso di denunciare rivolgendosi alla Sezione Operativa per la Sicurezza Cibernetica della Polizia Postale di Savona. Le indagini, condotte anche dagli esperti del Centro Operativo per la Sicurezza Cibernetica di Genova e coordinate dalla Procura della Repubblica di Savona, con il supporto del Servizio Polizia Postale di Roma, hanno permesso di identificare 12 utenti della rete, ritenuti autori dei commenti diffamatori, più condivisi, tra questi un impiegato, cinquantenne, romano, un operaio veneto, due pensionati residenti in Lombardia, un quarantenne, dipendente pubblico, residente in Friuli Venezia Giulia e un trentenne, residente in Sardegna.
Con la partecipazione dei Centri Operativi per la Sicurezza Cibernetica della Polizia Postale della Lombardia, Piemonte, Emilia Romagna, Friuli Venezia Giulia, Veneto, Lazio, Umbria e Sardegna, sei internauti sono stati destinatari di una perquisizione informatica delegata dalla Procura della Repubblica di Savona, mentre gli altri sei sono stati convocati presso i Centri Operativi della propria città e dovranno rispondere del reato di diffamazione aggravata.

La polizia di stato arresta 8 persone responsabili di truffe romantiche. Identificate 32 vittime. Oltre 400mila euro sottratti (marzo 2023)

Il Centro Operativo per la Sicurezza Cibernetica della Polizia Postale di Roma ha arrestato otto persone in esecuzione di una ordinanza applicativa di misure cautelari emessa dal G.I.P. di Roma per truffa aggravata, riciclaggio e sostituzione di persona.

Le indagini della Polizia Postale coordinate dalla Procura della Repubblica di Roma hanno avuto l'obiettivo di contrastare il sempre più diffuso e odioso fenomeno delle cd. "truffe romantiche", reati contro il patrimonio commessi in danno di persone fragili, che i criminali ricercano e individuano sui social network, portando poi a termine il progetto criminale e la truffa sfruttando le debolezze e le vulnerabilità delle vittime.

I criminali utilizzano profili social fake spesso presentandosi come personaggi affascinanti e rassicuranti, con l'obiettivo di instaurare un rapporto con le vittime fino a indurle a credere ad una relazione sentimentale.

Guadagnata la fiducia e la confidenza delle vittime, i criminali fanno richieste di denaro, utilizzando le scuse più disparate; le richieste diventano sempre più frequenti e la vittima, imprigionata in una relazione a distanza, fatica a rendersi conto, e spesso ad accettare di essere vittima di una truffa.

Questa indagine prende le mosse dalla denuncia di una signora, contattata su Facebook da "Larry Brooks", sedicente ufficiale dell'esercito statunitense, di stanza in Siria, con la foto profilo raffigurante un affascinante uomo di mezza età. Tra i due si instaurava una vera e propria relazione sentimentale tanto che la vittima, credendo alla promessa di un futuro insieme, si convinceva a effettuare diversi bonifici per consentire all'uomo, di far fronte alle difficoltà economiche che gli impedivano di congedarsi e giungere finalmente in Italia. Per rendere più verosimile la truffa architettata, i criminali si spingevano a creare fittizie identità di studi legali che confermavano, utilizzando comunicazioni via mail, le esigenze ed urgenze economiche di "Larry Brooks".

I primi accertamenti effettuati in rete e sui flussi finanziari confermavano i sospetti che il profilo fake "Larry Brooks" avesse mietuto molte vittime, e truffato decine di donne; nel corso delle indagini emergevano ben 32 vittime accertate con un provento illecito di circa 400.000 euro nel periodo dal 2018 al 2021.

La lunga e complessa attività investigativa è stata condotta affiancando tecniche classiche di investigazione ad attività di analisi del traffico delle comunicazioni internet e dei flussi finanziari ed ha consentito di identificare nel Lazio gli odierni indagati.

Sui conti correnti riferibili al gruppo criminale sono transitate somme di denaro provento delle truffe, inviate direttamente dalle vittime, per poi essere incassate, o trasferite su conti nelle disponibilità dei complici, in molti casi con rimesse di denaro all'estero, per la condivisione dei proventi della truffa.

In relazione al quadro indiziario emerso, la Procura della Repubblica di Roma ha contestato il concorso in truffa, aggravata dall'aver approfittato delle condizioni di minorata difesa delle vittime e dalla transnazionalità del reato, nonché il reato di riciclaggio dei proventi del reato.

L'approccio delle vittime è risultato rispondere a un consolidato protocollo criminale; tuttavia i criminali hanno dimostrato di essere in grado di adattarsi alle diverse condizioni delle donne, riuscendo a far leva sui loro punti deboli sempre per conseguire l'obiettivo finale di ottenere l'invio di denaro.

Ad esempio, quando hanno scoperto che una delle vittime non aveva potuto coronare il proprio desiderio di maternità, hanno inserito nella storia la figura di "Elvis Brooks", figlio del sedicente militare, con il compito di instaurare una stretta relazione con la donna fino a spingersi al punto di chiamarla "mamma". In taluni casi per suscitare la compassione delle donne, il figlio veniva descritto come gravemente malato e bisognoso di costose cure.

Agli indagati è stato contestato anche il reato di sostituzione di persona; difatti "Larry Brooks" è persona realmente esistente negli USA, e la foto utilizzata nei profili falsi è di un avvocato statunitense che in relazione alle condotte descritte e infamanti ha presentato denuncia alle autorità USA.

"Sei arruolato, vieni a prendere le misure per la divisa" (marzo 2023)

La Polizia Postale ha denunciato per il reato di sostituzione di persona e detenzione abusiva d'armi un uomo di Frascati, di 54 anni, indiziato per aver raggirato un giovane disoccupato, promettendogli un posto di lavoro e per aver gettato discredito sulla Gendarmeria Vaticana.

L'indiziato, venuto a conoscenza delle aspirazioni del giovane disoccupato, si presentava falsamente come Ufficiale dell'Arma dei Carabinieri e millantando rapporti privilegiati con la Gendarmeria Vaticana, si proponeva quale intermediario per l'assunzione del giovane nel Corpo della Gendarmeria.

Il giovane e il padre si convincevano a versare una somma di denaro in cambio del fattivo interessamento; seguiva un fitto scambio di mail fasulle con la Gendarmeria Vaticana per trarre in inganno la vittima del reato, con tanto di compilazione di test selettivi di ingresso, indicazione del buon esito delle prove e addirittura riferimenti ad una futura convocazione presso la sede della Gendarmeria Vaticana per le *"prove della divisa"*.

Il giovane, convinto del buon esito delle selezioni, si presentava personalmente presso gli uffici della Gendarmeria Vaticana, scoprendo di essere caduto vittima di un truffatore.

La Gendarmeria Vaticana, resasi conto della truffa e preso atto del discredito in danno della prestigiosa Istituzione e del suo Comandante, segnalava i fatti al **Centro Operativo per la Sicurezza Cibernetica – Polizia Postale di Roma**, facendo scattare le indagini, coordinate dalla Procura della Repubblica di Roma, che consentivano, attraverso l'esame delle evidenze informatiche, di individuare e denunciare il sospetto autore.

Su delega della Procura si procedeva a perquisizione locale personale nei confronti del soggetto indagato, consentendo il rinvenimento e successivo sequestro di device e di materiale predisposto per simulare l'appartenenza ad un corpo di polizia, in particolare due pistole replica senza il previsto tappo rosso di sicurezza e due portatessere con placche metalliche riconducibili all'agenzia governativa americana FBI.

Associazione a delinquere finalizzata alla truffa e al riciclaggio: il centro operativo per la sicurezza cibernetica Umbria dà esecuzione a 18 decreti di perquisizione (maggio 2023).

Personale della Specialità, coordinato dalla Procura della Repubblica presso il Tribunale di Spoleto, ha dato esecuzione a 18 decreti di perquisizione nei confronti di altrettante persone, operative su tutto il territorio nazionale, indagate per i reati di truffa, ricettazione e riciclaggio.

Le complesse indagini, avviate a seguito della presentazione di numerose querele da parte delle vittime di truffe "romantiche" e di altri reati hanno consentito di delineare una rete criminale articolata su due livelli:

il primo livello, fortemente gerarchizzato e prevalentemente radicalizzato nei paesi dell'Africa centro occidentale, si occupava di creare falsi profili al fine di adescare ignare vittime;

il secondo livello, invece, costituito da decine di persone deputate al riciclaggio del denaro fraudolentemente ottenuto, aveva l'incarico di mettere a disposizione i propri conti ovvero di reclutare persone disposte a fornire, talvolta inconsapevolmente, il proprio conto corrente per far confluire le transazioni illecite in cambio di una percentuale già stabilita dal gruppo criminale.

Gli indagati, situati capillarmente sull'intero territorio nazionale, sono stati in grado di raggiungere vittime in svariati paesi europei ed extraeuropei, seguendo un modus operandi relativamente semplice.

In particolare, una volta ottenuto il contatto con la potenziale vittima su uno dei numerosi social network, la stessa veniva coinvolta in un legame affettivo virtuale tale
da convincerla a versare spontaneamente somme di denaro al suo "amato virtuale" per consentirgli di "risolvere" asseriti problemi. In caso di rifiuto, gli indagati erano arrivati persino a effettuare delle vere e proprie estorsioni, minacciando le vittime di pubblicare foto e video "intimi" o conseguenze legali per dei supposti comportamenti illeciti della vittima.

Successivamente, i proventi così ottenuti venivano smistati su diversi conti correnti ed utilizzati per l'acquisto di beni di varia natura, automobili, materiale edile, condizionatori ecc. che venivano poi spediti verso la Nigeria all'interno di alcuni container.

Le indagini informatiche eseguite su alcuni apparati mobili a disposizione dei correi hanno consentito di constatare l'esistenza di veri e propri gruppi su dei social network,
creati con utenze straniere, per mantenersi in contatto e con lo scopo di gestire le "vittime -clienti", di riciclare il denaro, nonché le percentuali da condividere in considerazione della tipologia "dell'affare".

L'incisivo impulso della magistratura nell'attività di indagine effettuata nei confronti dei compartecipi ubicati in diversi Paesi UE – extra UE e il decisivo intervento del Servizio Polizia Postale e delle Comunicazioni, anche tramite l'attivazione dei canali di cooperazione internazionale (Europol/Interpol), hanno permesso di scoprire un giro
d'affari di oltre un milione di euro in due anni.

Altrettanto preziosa è stata la collaborazione di Poste Italiane S.p.A. e di altri istituti di credito, che hanno, in tempi brevi, fornito i riscontri necessari per individuare la catena di trasferimenti di denaro originata dalle attività illecite compiute dalla struttura malavitosa.
Le indagini svolte dal Centro Operativo per la Sicurezza Cibernetica Umbria hanno portato all'individuazione e consequenziale esecuzione di 18 perquisizioni, coordinate dal Servizio Centrale di Polizia Postale e delle Comunicazioni e la collaborazione dei Centri Operativi della Campania, Emilia Romagna, Lazio, Liguria, Marche, Sicilia e Veneto, nelle province di Modena, Padova, Genova, Pesaro, Latina, Caserta, Campobasso, Palermo e il concorso del Reparto Prevenzione Crimine Veneto coinvolto dalla Direzione Centrale Anticrimine.

Estorsioni in Rete: utenti di siti di incontri minacciati e costretti a pagare da sedicenti sfruttatori. La Procura della Repubblica di Perugia emette sei decreti di perquisizione (giugno 2023)

Personale della specialità ha eseguito 6 decreti di perquisizione personale, locale e informatica, emessi dalla procura di Perugia nei confronti di altrettanti cittadini di nazionalità straniera, ma residenti in Italia, indagati per i reati di estorsione e minacce in danno di alcuni utenti di siti di incontro.
L'attività di indagine, effettuata dal Centro Operativo per la Sicurezza Cibernetica – Polizia Postale e delle Comunicazioni Umbria unitamente alla Squadra Mobile della Questura di Perugia è originata dalla denuncia di un uomo che, dopo aver contattato delle ragazze su un sito di incontri, è stato minacciato da ignoti soggetti, che hanno paventato mali ingiusti a lui e ai familiari e che lo hanno costretto a pagare – a più riprese – un importo complessivo superiore a 3000 euro.
Dagli approfondimenti investigativi è emerso che il "*modus operandi*" usato dagli autori delle minacce - operanti sull'intero territorio nazionale, è sempre stato lo stesso: dopo essersi presentati come "gestori" di alcune ragazze presenti sui siti d'incontri, hanno inviato ai fruitori, tramite applicativi di messaggistica istantanea, una serie di minacce con la scusa di aver fatto perdere del tempo – e quindi degli introiti – alle "loro" ragazze, denaro che avrebbe dovuto essere necessariamente ristorato dalle vittime per evitare il concretizzarsi delle minacce.
Gli investigatori della Squadra Mobile e della Polizia Postale perugina, a questo punto, hanno incrociato migliaia di dati, tra tabulati telefonici e file di log, che hanno portato all'individuazione di 6 soggetti, che potrebbero avere un diretto coinvolgimento nella vicenda.
L'attività di perquisizione locale, personale e informatica – eseguita nel capoluogo ligure – è stata coordinata dal Servizio Polizia Postale e delle Comunicazioni ed è stata effettuata in sinergia con il Centro Operativo per la Sicurezza Cibernetica – Polizia Postale e delle Comunicazioni Liguria e con la Squadra Mobile di Genova.
All'esito delle perquisizioni, gli operatori hanno sottoposto a sequestro numerosi supporti informatici che saranno oggetto di specifici accertamenti tecnici.

Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (C.N.A.I.P.I.C. e N.O.S.C.)

Prosegue, incessante, l'azione preventiva e di contrasto del Servizio Polizia Postale e delle Comunicazioni alle minacce cibernetiche che si affacciano con sempre maggior evidenza sullo scenario nazionale e internazionale.
Lo scenario geopolitico attuale è ormai caratterizzato da complesse dinamiche di competizione strategica, accelerate dalla crisi ucraina, nella cornice di strategie comunicative invasive e destabilizzanti.
La sicurezza nazionale e della comunità internazionale rappresenta una sfida che si evolve rapidamente in maniera sempre più complessa, considerato che lo sviluppo e la rapida diffusione di nuove tecnologie genera oggettive difficoltà anche per il crescente ricorso a campagne informative, o disinformative, che ampliano notevolmente il concetto di minaccia.
Ciò posto, il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC) del Servizio Polizia Postale e delle Comunicazioni, nell'esercizio della propria attività istituzionale di monitoraggio, ha rilevato - nella prima metà del 2023 - **un costante aumento delle attività ostili, di provenienza soprattutto estera**, collocabili all'interno di schemi di *crime as a service* come pure ricollegabili, anche indirettamente, ad una matrice statuale.
Durante questo periodo, molteplici indicatori hanno rilevato cambiamenti sostanziali nella strumentazione a supporto delle operazioni e nelle tecniche utilizzate dai gruppi offensivi, per supportare la frequenza e la portata (maggiormente invasiva) delle operazioni e ostacolare l'analisi forense.
Inoltre, in questo primo semestre, dall'analisi dei dati emersi dal versante nazionale, è cresciuta l'attività di contrasto generale alla minaccia cyber svolta dal **C.N.A.I.P.I.C.** contro campagne massive dirette verso infrastrutture critiche, sistemi finanziari e aziende operanti in settori strategici.

In quest'ambito, **si registra un aumento degli attacchi rilevati**, che - quanto a tipologia - utilizzano ancora prevalentemente, quali strumenti di azione, le campagne di *phishing*, la diffusione di *malware* distruttivi (specialmente *Ransomware*), attacchi Ddos, le campagne di disinformazione e *leak* di database.
Lo sfruttamento di vulnerabilità, anche note e non adeguatamente rimediate, costituisce inoltre uno dei veicoli di intrusione più ricorrenti, favorendo l'introduzione abusiva dell'attore ostile all'interno del perimetro, al tendenziale scopo di ottenere una persistenza silente
I target, maggiormente colpiti, riguardano il settore industriale - manifatturiero, che nelle rilevazioni precede immediatamente quello riguardante le piccole amministrazioni locali e le aziende di servizi e studi professionali.
Mediante la compiuta analisi dello scenario di attacco e dei rischi a esso collegati, sempre in dinamica evoluzione, il Servizio Polizia Postale e delle Comunicazioni, quale Organo del Ministero dell'Interno per la sicurezza delle telecomunicazioni, ha condiviso, a tutti gli attori istituzionali dell'ecosistema della cyber sicurezza nazionale, le evidenze informative

raccolte relative alle potenziali criticità in ambito cibernetico, che depongono per il mantenimento del più elevato grado di allertamento.
Anche in base ai riscontri appresi, è emersa la necessità di implementare ulteriormente l'attività informativa, ampliando ancor di più lo spettro di intervento, al fine di indirizzare l'azione (che si vuole sempre più sinergica) dei diversi attori coinvolti nella sicurezza verso gli spazi più nascosti e difficilmente penetrabili (*dark web)*. A tal fine, è risultata fondamentale l'attivazione dei canali di interlocuzione internazionali, già dedicati allo scenario descritto, come ad esempio Europol, Interpol e le agenzie di law enforcement dei paesi partner. Questi strumenti sono risultati essenziali, permettendo di elevare il livello di attenzione, specie al settore economico/finanziario, tradizionalmente oggetto di interesse da parte di compagini criminali con connotazione *state sponsored*.

Il risultato di questo sforzo si compendia in un **aumento delle richieste di cooperazione in ambito internazionale**, ricollegate anche al ruolo (sempre più consapevole) del CNAIPIC quale punto di Contatto nazionale della rete 24/7, ai sensi della Convenzione di Budapest sul cybercrime.
Appare, inoltre, importante ricordare l'attività preventiva svolta mediante la diffusione di dedicati alert, che sottendono indicatori di compromissione e avvisi di informazione di sicurezza alle infrastrutture informatiche dicasteriali, alle infrastrutture critiche nazionali e ai potenziali target di azioni ostili, individuati attraverso la permanente attività informativa assicurata dal Centro.
Cosicché l'attività del CNAIPIC e dei NOSC ha consentito, nel periodo di riferimento, di rilevare n. **5.775 attacchi**, nonché di diramare **n. 41.704 *alert***. Le indagini avviate esclusivamente dal Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche sono state n. 52, mentre n. 144 sono le persone indagate, con la collaborazione delle dipendenti articolazioni territoriali.

Queste ultime sono state costantemente sensibilizzate all'innalzamento delle attività di competenza, attraverso un adeguato e continuo coinvolgimento dei rispettivi Nuclei Operativi di Sicurezza Cibernetica (NOSC) e ciò al fine di garantire un adeguato flusso informativo per una tempestiva condivisione di ogni evidenza utile.

PRIMO SEMESTRE 2023	
Attacchi rilevati	5.775
Alert diramati	41.704
Indagini avviate dal CNAIPIC	52
Persone indagate	144
Richiesta di cooperazione internazionale in ambito Rete 24/7 High Tech Crime G8 (Convenzione Budapest)	47
Attacchi Ransomware	158

Da ultimo, va ricordato lo sforzo volto a costituire un sistema di sicurezza integrata, mediante l'intessitura di rapporti di partenariato, sia con componenti pubbliche che con *stakeholders* privati, che sfociano nella sottoscrizione di convenzioni e collaborazioni.
Lo scopo finale delle campagne di attacco più ricorrenti si conferma, oltre al danneggiamento informatico, quello dell'illecita sottrazione di codici e informazioni riservate, contenute all'interno dei sistemi critici. In questo quadro, l'attenzione del CNAIPIC si dirige anche alla disarticolazione dei mercati illegali sui quali i dai sottratti vengono reimmessi nel circuito criminale.

Operazione internazionale per la disarticolazione di Genesis Market, uno dei più grandi mercati neri virtuali del mondo, dedicato alla vendita di credenziali rubate.

Nell'aprile di quest'anno, nell'ambito di una più vasta indagine a livello internazionale, svoltasi simultaneamente in 16 Paesi, condotta dal FBI e dalla polizia olandese e coordinata da Europol ed Eurojust e diretta, per il territorio italiano, dalla Procura della Repubblica di Roma**,** la Polizia Postale ha messo a segno, su tutto il territorio nazionale, un'operazione di polizia informatica senza precedenti nel settore del contrasto ai mercati neri del web.
La piattaforma Genesis Market, uno dei più pericolosi mercati illeciti virtuali del mondo, specializzata nella vendita di credenziali di accesso e dati rubati, con un giro di affari di oltre 2 milioni di identità virtuali sottratte, è stata disattivata, con sequestri, eseguiti in tutta Europa, dei server sui quali poggiava l'infrastruttura informatica.

In Italia, risultavano coinvolte migliaia di credenziali, individuate dagli specialisti del Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (CNAIPIC) della Polizia Postale, sotto la direzione della Procura della Repubblica di Roma, e afferenti sia a spazi informatici della vita privata di comuni cittadini (email, social network, account di e-commerce, ecc.), sia, in maniera ancor più allarmante, password in grado di garantire l'accesso illecito a spazi informatici istituzionali della pubblica

amministrazione, nonché appartenenti a banche e grandi imprese nazionali, erogatrici di servizi pubblici essenziali.
Sul solo territorio italiano, sono stati emessi dalla Procura della Repubblica di Roma nr. 37 decreti di perquisizione personale, locale e informatica, che il CNAIPIC e i Centri Operativi per la Sicurezza Cibernetica di Campania Basilicata e Molise, Lazio, Lombardia, Puglia, Emilia Romagna, Calabria, Veneto, Sicilia Occidentale, Abruzzo, Friuli Venezia Giulia, Liguria, Toscana, Trentino-Alto Adige ed Umbria, hanno eseguito nei confronti di altrettanti clienti della piattaforma, i quali avevano acquistato nel corso del tempo migliaia di credenziali di accesso.

Operazione ENEL Distribuzione

Nei mesi scorsi, Enel Distribuzione ha denunciato una violazione di sicurezza (data breach) riguardante decine di migliaia di anagrafiche di clienti del mercato libero di energia. I dati venivano sottratti attraverso la creazione (ed il successivo accesso abusivo) ad account "usa e getta" sul portale E-Distribuzione del gruppo Enel.
Dall'analisi dei file di log è stato possibile accertare responsabilità penali da parte di soggetti riconducibili ad alcune società di call-center, operanti sul territorio campano, nonché agenti di commercio del settore energetico nelle regioni della Puglia e della Sicilia.
Le successive attività di perquisizione, disposte dalla Procura di Napoli, a carico dei soggetti campani individuati, ha portato all'arresto di nr.3 soggetti dediti al procacciamento illecito dei dati sensibili tramite accesso abusivo e alla denuncia a piede libero di vari personaggi, per il trattamento illecito dei dati stessi.

FINANCIAL CYBERCRIME

Prosegue l'esponenziale crescita del *financial cybercrime*, che si conferma anche nel primo semestre del corrente anno sempre più come una delle forme predominanti e preminenti del crimine informatico, con una tendenza che permane a livello globale.
Molteplici e in continua evoluzione risultano le tecniche utilizzate dalle organizzazioni criminali, attivate in danno dei cittadini, delle piccole e medie imprese (che costituiscono il tessuto economico portante del Paese), nonché, sovente, in danno delle più grandi e importanti aziende.
Persistono i più tradizionali *modus operandi,* tipici del crimine finanziario di interesse della Polizia Postale e delle Comunicazioni. In primo luogo il c.d. *"phishing"*[2] che consente il furto dei dati sensibili per l'accesso ai sistemi di *home banking*, funzionale a illecite operazioni bancarie: lo scopo di tali tecniche di attacco è, infatti, quello di entrare in possesso delle credenziali finanziarie delle vittime, per poter poi operare dai conti correnti online; con le carte di credito/debito attraverso prelievi; con bonifici o con l'acquisto di beni online.

[2] Realizzabile anche nelle varianti del c.d. ***"smishing"*** (allorché non si utilizzi la classica email, ma il "veicolo" utilizzato per ingannare la vittima sia un messaggio telefonico) e del c.d. ***"vishing"*** (qualora si ricorra ad un contatto diretto a voce).

Al riguardo giova rammentare come l'innalzamento delle procedure di sicurezza attivate dalle banche (anche con la doppia verifica sul telefono del titolare, quale presupposto necessario per realizzare l'operazione in frode) abbia indotto i criminali ad attuare la tecnica cosiddetta del "*sim swap*", ancora largamente diffusa: sussistendo, infatti, la necessità di acquisire i codici autorizzativi, i criminali riescono a ottenere un duplicato della SIM della vittima (grazie al *dealer* compiacente o attraverso l'utilizzo di documenti falsi) ove ricevono gli OTP necessari al perfezionamento delle operazioni fraudolente.
Analogamente, si registra una consistente operatività della tecnica criminale del c.d. "*man in the middle*", del BEC *(business e-mail compromised)* e del *chef executive officer fraud* (CEO *Fraud*): dinamiche delinquenziali che rappresentano a tutt'oggi le principali tipologie di frode maggiormente diffuse in danno di piccole e grandi aziende.

- BEC *(Business e-mail compromised)* che consiste nel**:**
  - Intercettare le comunicazioni fra aziende o anche privati (attraverso un accesso abusivo ad una delle caselle di posta elettronica delle potenziali vittime), intercettare eventuali richieste di pagamento, sostituirsi ad una delle parti e dirottare i bonifici modificando fatture o comunicando nuove coordinate bancarie;
  - Alterare in modo impercettibile una mail, traendo in inganno la controparte e anche in questo caso dirottando bonifici su altri conti.

È tipico anche l'utilizzo della tecnica denominata "spoofing", che consente un mascheramento dei dati reali di chi sta operando il crimine.

- CEO *(Chef Executive Officer)*
  In questo caso i criminali, dopo un attento studio sulle fonti aperte (legate soprattutto agli spostamenti ufficiali dei CEO di grandi aziende per la partecipazione degli stessi a eventi finanziari di grande rilievo), avendo cura di creare un indirizzo mail quasi identico a quello del capo dell'azienda, o utilizzandone uno reale (previa illecita disponibilità delle credenziali di accesso), contattano un dirigente aziendale con potere dispositivo e lo traggono in inganno con un atteggiamento strettamente confidenziale, convincendolo a fare uno o più bonifici per un'operazione finanziaria riservata ed urgente. Spesso tali strategie criminali prevedono l'intervento di una figura con il ruolo di un avvocato specializzato nei contratti internazionali, nonché la formazione di documenti completamente falsi che supportano la strategia dell'inganno posta in essere.

L'attività di questa Specialità nel settore del *financial cybercrime* è svolta a 360°, tanto in ambito preventivo (con campagne mirate di informazione rivolte sia alle *law enforcement* non specializzati in materia di *cybercrime*, che al pubblico, anche attraverso i *social* ufficiali) quanto in ambito repressivo.

LE FRODI INFORMATICHE E MONETICA Primo semestre 2023	
Frodi Informatiche (Ril. nazionale)	5.354
Persone indagate	388
Somme sottratte	€ 21.536.551

Nella prevenzione e nel contrasto al *financial* cybercrime, la cooperazione internazionale assume un ruolo assolutamente strategico, atteso che la transnazionalità delle condotte illecite connota costantemente l'indagine giudiziaria di specifico settore.
Ordinariamente, infatti, è all'estero che si consuma, almeno parzialmente, la condotta criminosa e tanto le tracce informatiche (sovente abilmente manipolate attraverso i più vari strumenti di anonimizzazione), quanto le tracce finanziarie (conti correnti e strumenti finanziari, sistemi di pagamento elettronico, corrieri di denaro, criptovalute, ecc.), frequentemente, riconducono fuori dal territorio nazionale; per tale motivo, nei casi di prontezza di reazione delle vittime e, quindi, nell'immediatezza dei fatti, grazie alla richiamata cooperazione è possibile conseguire buoni risultati in termini di recupero delle somme distratte e di identificazione degli autori.
Nel particolare contesto operativo, fondamentale è l'apporto della piattaforma OF2CEN (*On Line Fraud Cyber Centre and Expert Network*), realizzata appositamente al fine di prevenire e contrastare le aggressioni criminali ai servizi di home banking e monetica, con la quale viene svolta un'accurata analisi delle frodi di interesse della Specialità: una struttura informatica frutto di specifiche convenzioni con le principali banche, con ABI e con gran parte del mondo bancario che consente di intervenire in tempi ristretti sulle segnalazioni oggetto di investigazione.
Nell'ottica di una proficua azione di contrasto, che come sopra rilevato non può prescindere da strategie di intervento operativo realizzate in sinergia con altri paesi, è da segnalare la costante, consueta, partecipazione, a vari tavoli di lavoro internazionali, con particolare riferimento a quello denominato EMMA (European Money Mule Action), giunto ormai alla sua nona edizione, le cui ultime risultanze saranno condivise da tutti i paesi aderenti alla fine dell'anno corrente.
Insieme alla Polizia Postale, aderiscono forze di polizia di altri 26 stati europei e l'agenzia Europol: in un periodo di tempo concertato vengono avviate operazioni in sinergia, anche con indagini congiunte, dando esecuzione a mirati provvedimenti delle Autorità Giudiziarie, identificando i titolari dei conti correnti con risultati investigativi di notevole rilievo.
Il 2023, inoltre, è stato caratterizzato dal sempre più crescente interesse, da parte delle organizzazioni criminali, per le c.d. criptovalute. Le evidenze offerte dalle più recenti investigazioni offrono, infatti, il riscontro ad un innalzamento dei livelli di impiego di tali valute digitali, con conseguente sempre maggiore capacità di gestione dei sistemi di *blockchain* su cui registrare le transazioni perfezionate con "criptovalute".

Tali transazioni si caratterizzano per una maggiore difficoltà di tracciamento, (costituendo per tale motivo utile strumento attraverso cui perfezionare l'efficace riciclaggio dei proventi illeciti) rendendo più complesse le investigazioni per la conseguente necessità di impegnare professionalità con elevati livelli di competenze in grado di utilizzare sofisticati *software* di analisi, che agevolano l'esplorazione dei citati sistemi di *blockchain*. A ciò si aggiunga che sebbene le transazioni in argomento, al netto delle richiamate difficoltà, siano tracciabili,[3] l'utilizzo di alcune particolari monete digitali - create per essere, nel loro funzionamento, totalmente anonime (su tutte le cripto valute "monero" e "dash") - rende impossibile acquisire informazioni utili alle investigazioni.

Per tutte le richiamate ragioni, appare più che verosimile che l'abilità tecnica richiesta per movimentare capitali ingenti attraverso il ricorso a criptovalute sarà sempre più rapidamente acquisita anche dalle organizzazioni criminali di stampo mafioso, le quali, nella recente storia, si sono caratterizzate per aver assicurato alle giovani generazioni di affiliati accresciuti livelli di professionalità e specializzazioni funzionali al successo dell'impresa criminosa.[4]

Sul tema, deve segnalarsi inoltre la circostanza di un sempre maggior utilizzo delle criptovalute anche da parte dei cittadini i quali, anche con bassa scolarizzazione informatica, sono sempre più attratti dagli investimenti in moneta digitale con la speranza di realizzare veloci e importanti guadagni esponendosi anche a furti e frodi attraverso attacchi di phishing o attraverso finte piattaforme di trading online.

Proprio per tale motivo, nell'ambito del panorama delittuoso di interesse è da segnalare la forte espansione delle truffe attuate tramite proposte di investimenti di capitali *online* (il c.d. *trading online*). Le evidenze più recenti riportano, infatti, una decisa crescita delle denunce e, conseguentemente dei capitali investiti sottratti alle vittime, con un coinvolgimento di soggetti passivi del reato non più circoscritto a persone vulnerabili come gli anziani, ma esteso a diverse tipologie di "investitori", segno della sempre maggiore capacità organizzativa della sottesa struttura criminale, ramificata per lo più all'estero.

---

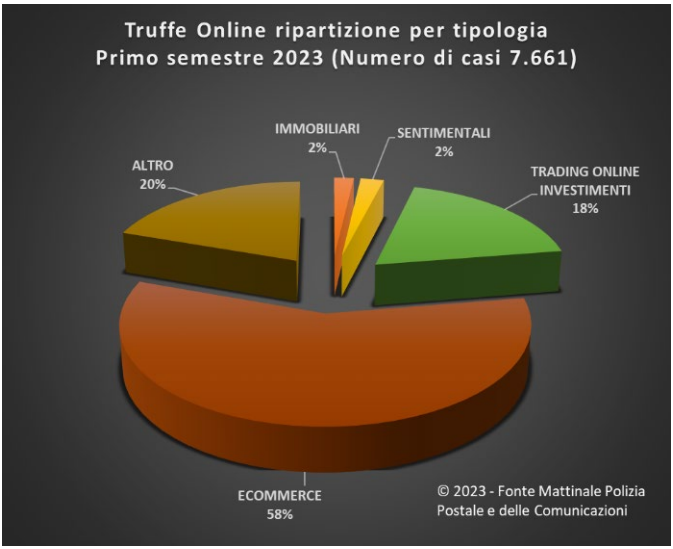
[3] Ogni utente e ciascun portafoglio virtuale (*wallet*) è, infatti identificato nella *blockchain* da un codice univoco alfanumerico. Seppure tale caratteristica ne determina la natura pseudo-anonima rimane tuttavia astrattamente possibile riuscire a collegare un indirizzo *wallet* all'IP con cui è stato gestito. Diventa quindi possibile, ad esempio, associare un *wallet* ad una area geografica, elemento utile all'identificazione del possessore.

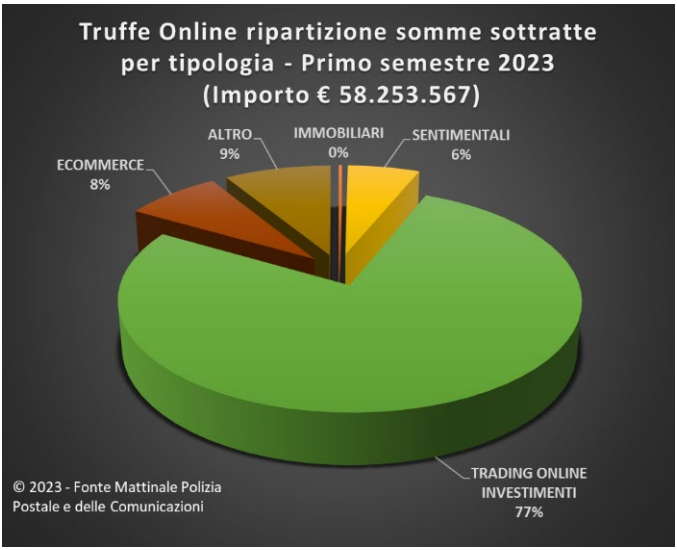
[4] La circostanza che le **criptovalute** si caratterizzino per una elevata volatilità (in un mercato che, peraltro, è attivo senza soluzione di continuità 365 giorni all'anno H24), potenziale ostacolo al loro utilizzo nell'azione di riciclaggio può essere agevolmente superata attraverso la conversione delle più utilizzate criptovalute in stablecoin: crypto asset con valore stabile ancorato o ad una valuta fiat (generalmente il dollaro USA, esempio THETER, BUSD o USDC) o al prezzo dell'oro (suscettibile di ben minori fluttuazioni: come ad esempio la criptovaluta DIGIX GOLD).

TRUFFE ONLINE

Report relativo alle truffe online
Periodo: 01/01/2023 – 30/06/2023

		IMPORTI SOTTRATTI	
IMMOBILIARI	**CASI TOTALI 7.661**	158.974 €	**PERSONE INDAGATE 1.853**
SENTIMENTALI ROMANCE SCAM		3.460.589 €	
TRADING ONLINE		44.905.283 €	
E COMMERCE		4.606.297 €	
ALTRO		5.122.424 €	
		TOTALE 58.253.567 €	





Tra le nuove minacce che potrebbero modificare lo scenario della contraffazione e della violazione dei diritti di proprietà intellettuale - e più in generale delle condotte delittuose che attualmente si perfezionano in rete - si inserisce l'ideazione del c.d. "metaverso".

Spesso definito superficialmente come il naturale sviluppo dei social media, si caratterizza per esserne un potenziamento con funzionalità e destinatari virtualmente infiniti. Seppur ancora oggi si trovi nella sua fase iniziale di sviluppo, l'evoluzione della tecnologia computeristica sta rapidamente trasformando le primordiali "realtà virtuali" che, da ambienti virtuali immersivi, mutano sempre più in una rivisitazione della tecnologia della rete internet, capace di sostituire tutti gli apparati mobili esistenti, generando nuove tecnologie e mutando il comportamento dell'uomo: non "semplicemente" una rete di computer, server e altri dispositivi elettronici attraverso cui gli utenti, una volta online, comunicano tra di loro, interagiscono, visitano siti, fanno acquisti, ma una vera e propria "realtà alternativa" dove gli utenti, attraverso i loro avatar, interagiscono tra di loro, fanno attività, acquisti e partecipano a eventi in un mondo che imita quello fisico e nel quale accedono usando tecnologie come la realtà virtuale (VR), la realtà aumentata (AR), l'IA, i social media e la valuta digitale. In tale nuovo scenario internet è incorporato nell'esperienza umana quotidiana: si realizza una trasposizione della realtà fisica in una dimensione virtuale e la navigazione si trasforma in vita (apparente).
Naturalmente una tale svolta tecnologica non è esente da problemi, il metaverso, infatti, potrebbe acuire criticità già esistenti nell'era digitale. Fra le diverse distonie potenzialmente ipotizzabili, si potranno manifestare significativi problemi riguardo alla tutela dei dati e delle

informazioni sia private che aziendali: gli utenti, infatti, potrebbero esporsi con sconosciuti sentendosi "al sicuro", mettendo a rischio i loro asset nella vita reale e permettendo ai malintenzionati di appropriarsi di tantissime informazioni sensibili quali, ad esempio, documenti personali, dettagli bancari, informazioni sul nucleo familiare e altri dettagli riservati. A questi temi andranno ad aggiungersi molte delle questioni attinenti alla tutela della proprietà intellettuale: il metaverso, infatti, favorirà il c.d. *immersive commerce,* uno shopping immersivo che può ben rappresentare il futuro dell'e-commerce in una realtà potenziata da una "esperienza sensoriale", con veri e propri negozi virtuali dove i clienti-avatar potranno fare acquisti digitali. Tutto ciò rappresenterà opportunità e rischi per titolari di diritti di proprietà intellettuale e industriale, così come per fornitori di contenuti. Opportunità per i titolari di poter immaginare una presenza strategica nel nuovo ecosistema, ma rischi relativi a pirateria o contraffazione (in caso di marchi) e difficoltà in tema di prova di illecito sfruttamento.
Proprio in virtù di un tale possibile scenario, è parso necessario avviare uno studio approfondito - che sarà realizzato attraverso un Gruppo di Lavoro appositamente costituito in seno al Servizio Polizia Postale - delle potenziali evoluzioni del metaverso e dell'impatto che potrà avere in termini di diffusione delle condotte delittuose che ben potrebbero trovare in tale "ambiente" nuove e proficue opportunità.

Di seguito, un dettaglio delle **operazioni più significative** portate a termine dalla Specialità nell'azione di contrasto ai richiamati fenomeni delittuosi nel primo semestre del 2023.

Operazione "Ghost Money"

In data 18 maggio 2023, i Centri Operativi per la Sicurezza Cibernetica (COSC) di Roma e di Torino, hanno dato esecuzione a provvedimenti di custodia cautelare, emessi dal G.I.P. di Roma nei confronti di 6 indagati per truffa aggravata, frodi informatiche, riciclaggio e auto riciclaggio.
Le indagini condotte da personale del COSC di Roma, sono state avviate a seguito di frodi realizzate con la tecnica del SIM SWAP attraverso la quale il sodalizio criminale riusciva a carpire le credenziali dell'home banking inviate al numero telefonico delle vittime, che venivano così private dei propri fondi. Le perquisizioni e l'analisi dei dispositivi sequestrati ha consentito di far emergere un complesso sistema di frodi informatiche (di cospicui importi compresi tra i 2 e 4 milioni).
L'evoluzione investigativa ha consentito di smascherare il contesto criminale che ha colpito diversi istituti di credito mediante falsi mandati di pagamento SEPA, sfruttando le vulnerabilità dell'architettura dei sistemi informatici, e riciclando i proventi attraverso l'utilizzo di società intestate fittiziamente a c.d. "*teste di legno*".

Operazione "Grandi Firme"

In data 29 giugno 2023, personale dei Centri Operativi per la Sicurezza Cibernetica (COSC) di Catania e Napoli, coordinati dal Servizio Polizia Postale e delle Comunica-

zioni, hanno dato esecuzione a decreti di perquisizione locale e personale, emessi dalla Procura Distrettuale di Catania, nei confronti di 11 soggetti, di cui 7 residenti a Catania e 4 a Napoli, indagati per associazione a delinquere finalizzata all'introduzione nello Stato e commercio di prodotti con segni falsi.
L'operazione di polizia giudiziaria nasce dagli sviluppi delle evidenze acquisite all'esito di altre perquisizioni effettuate in data 10 novembre 2022, nel contesto dell'operazione "Gotha IPTV" tesa a contrastare la diffusione di palinsesti televisivi ad accesso condizionato.
L'analisi del materiale sequestrato nel corso della richiamata operazione di PG consentiva, infatti, di acquisire chiari riscontri indiziari circa il coinvolgimento di ulteriori soggetti coinvolti nell'illecito commercio, realizzato attraverso social media e servizi di messaggistica crittografata, di capi di abbigliamento, scarpe e accessori vari contraffatti, riportanti i marchi di famose aziende di moda.
All'esito delle perquisizioni il personale operante ha rinvenuto un ingente quantitativo di merce contraffatta e diversi apparati cellulari utilizzati per le illecite condotte.

Cyberterrorismo

Nell'ambito della prevenzione e del contrasto alla diffusione di contenuti terroristici online e, in particolare, dei fenomeni di radicalizzazione sul web, il personale della Polizia Postale e delle Comunicazioni effettua costantemente il monitoraggio del web e svolge attività investigative, sia d'iniziativa che su specifica segnalazione (anche grazie a quelle che giungono dai cittadini tramite il portale del Commissariato di P.S. Online), al fine di individuare i contenuti illeciti presenti all'interno degli spazi e dei servizi di comunicazione online di ogni genere.
In particolare, il personale del settore Cyberterrorismo svolge attività informativa e investigativa nell'ambito della prevenzione e del contrasto alla diffusione di contenuti terroristici online ed, in particolare, dei fenomeni di radicalizzazione sul web.
Il target operativo di tale settore, dunque, si concretizza nella prevenzione e repressione dei reati che utilizzano la dimensione virtuale per fini terroristici, minando l'ordine e la sicurezza pubblica per ragioni riconducibili sia a forme di fondamentalismo religioso, sia a forme di estremismo politico ideologico, anche in contesti internazionali.

In ambito di cooperazione internazionale per la prevenzione e contrasto del cyber terrorismo si rappresenta che la I Sezione della III Divisione del Servizio Polizia Postale e delle Comunicazioni costituisce il punto di contatto italiano della rete Europol IRU - Internet Referral Unit, coordinata dal Centro ECTC di Europol (European Counter Terrorism Center) – per il monitoraggio dei contenuti terroristi online, e partecipa insieme agli operatori di polizia di altri paesi anche agli action day che in tale ambito vengono promossi con notevoli risultati operativi.
E invero, il continuo e vertiginoso incremento dell'utilizzo delle piattaforme di comunicazione online, social network e applicazioni di messaggistica istantanea, ha determinato parallelamente un considerevole incremento, ad una platea pressoché illimitata, di qualsiasi

tipo di contenuti propagandistici riconducibili al terrorismo, sia di matrice islamista, sia formazioni di estrema destra (neonazismo, neofascismo, tifoserie strutturate, suprematismo), formazioni di estrema sinistra (movimenti di lotta armata, anarchici, insurrezionalisti, antagonisti), formazioni separatiste.
In tale ambito, si rende necessario garantire sia l'esecuzione di una costante attività di monitoraggio investigativo della rete e dei canali di messaggistica istantanea, per l'identificazione e il deferimento all'Autorità Giudiziaria dei responsabili della diffusione dei contenuti illeciti, sia un costante scambio informativo con la Direzione Centrale della Polizia di Prevenzione e con le Agenzie di Intelligence, competenti in materia di contrasto al terrorismo.
Nell'ambito del contrasto al fenomeno del c.d. cyberterrorismo e in generale, dell'estremismo in rete gli investigatori della Sezione Cyberterrorismo hanno concorso alla prevenzione e al contrasto dei fenomeni di eversione e terrorismo, sia a livello nazionale che internazionale, posti in essere attraverso l'utilizzo di strumenti informatici e di comunicazione telematica.
L'attività, funzionale al contrasto del proselitismo e alla prevenzione dei fenomeni di radicalizzazione estremista religiosa e dell'eversione di estrema destra e antagonista, ha permesso di sviluppare una dedicata attività informativa in contesti di interesse, per oltre **91.000** spazi web oggetto di approfondimento investigativi; tra questi oltre **220** risorse digitali sono state oscurate poiché caratterizzati da un contenuto illecito.
L'attività di monitoraggio del web effettuata dalla Specialità ha permesso di riscontrare in primis come la diffusione di contenuti propagandistici jihadisti, nel corso del tempo, abbia subito un sensibile peggioramento qualitativo, determinato sia dal ridimensionamento del Califfato sul territorio, sia dalle perdite di tecnici e social media manager cui era devoluto l'incarico di gestire la propaganda, nonché per l'utilizzo sempre più frequente dell'Intelligenza Artificiale sulle principali piattaforme web, per la scansione (e rimozione) dei contenuti pubblicati dagli utenti.

Tra le numerose attività investigative svolte nel corso del 2023 dalla Polizia Postale, degna di nota è quella che ha permesso di identificate e denunciate due promotori del gruppo no-vax denominato "guerrieri ViVi", e di oscurare alcuni canali di comunicazione in rete.
In particolare, all'esito di un primo filone investigativo che già nel 2022 aveva consentito di denunciare ventiquattro appartenenti al gruppo no vax - no green pass denominato "guerrieri Vivi", il Centro Operativo per la Sicurezza Cibernetica di Genova ha eseguito nello scorso mese di gennaio alcune perquisizioni a Brescia, Verona e Matera, delegate dalla D.D.A. della Procura della Repubblica di Genova, a carico di tre soggetti di cui due indiziate di essere promotori del sodalizio nell'ambito di un procedimento per violazione degli artt. 1 e 2 c. 1 e 2 della l. n. 17/1982 (associazione segreta) e degli artt. 110 - 414 c. 1 n.1 e c.3, in relazione all'art. 340 c.p. (istigazione all'interruzione di un servizio di pubblica necessità).
Ed invero, il Centro Operativo per la Sicurezza Cibernetica della Liguria ha identificato i capi dell'organizzazione dopo mesi di serrate indagini informatiche che hanno consentito di setacciare centinaia di chat su numerosi social e documenti postati in rete, scardinando

l'anonimato che gli autori ritenevano di avere conseguito grazie all'utilizzo di reti VPN e del sistema di messaggistica Telegram.
L'attività di proselitismo e istigazione a delinquere del gruppo no-vax ha quotidianamente preso di mira rappresentanti istituzionali e appartenenti all'ordine dei medici attraverso commenti "violenti", postandoli in maniera coordinata e ripetitiva sui profili social delle vittime, soprattutto di chi esprimeva opinioni a favore dei vaccini, imbrattando con scritte in vernice rossa le sedi di alcune Asl, di hub vaccinali, ospedali, ordini dei medici, scuole, sedi di alcuni sindacati e testate giornalistiche.
Con la conclusione delle restrizioni legate alla pandemia, il gruppo no vax, dichiaratamente ossessionato da ogni presunta forma di controllo, non ha interrotto la propria attività di proselitismo e si è orientato verso gli argomenti dei sistemi di pagamento e di identità digitale, dei cambiamenti climatici, del 5G, "attaccando" in rete, con lo stesso modus operandi, talvolta anche con minacce, chi esprimeva opinioni a favore dello sviluppo di tali tecnologie o tematiche.
Gli attacchi venivano coordinati su gruppi Telegram creati ad hoc e sugli stessi gruppi venivano poi pubblicizzate le incursioni, con immagini o screenshot di quanto vandalizzato.
Sono state create anche alcune challenge con cui i promotori invitavano gli adepti a compiere azioni illecite, come posizionare striscioni o adesivi ritraenti il logo del gruppo su sedi Istituzionali, in una sorta di gara che prevedeva un premio in bitcoin da assegnare all'autore dell'azione più eclatante.
Le perquisizioni eseguite dagli investigatori del Centro Operativo per la Sicurezza Cibernetica di Genova, con l'ausilio degli Uffici di Milano, Venezia, Campania, Basilicata e Molise, e il coordinamento del Servizio Polizia Postale e delle Comunicazioni di Roma, presso le residenze degli indagati, i loro luoghi di lavoro e un maneggio in provincia di Brescia presso cui si incontravano, hanno consentito di acquisire evidenze informatiche di conferma dell'attuale operatività dei "ViVi" e di procedere al sequestro preventivo dei loro mezzi di comunicazione e propaganda in rete, emesso dal GIP del Tribunale di Genova.
Il carattere transnazionale delle attività di contrasto alla diffusione dei contenuti terroristici online, sia per la natura internazionale del fenomeno che per la stessa struttura della rete, comporta un'imprescindibile attivazione di strumenti di cooperazione sovranazionale che possano apportare un indiscusso valore aggiunto alle attività di prevenzione messe in atto dalle diverse Forze di Polizia nazionali.
Nel contesto delle attività investigative che sono state avviate grazie alla cooperazione internazionale, appare opportuno evidenziare quella che, il 26 gennaio, a seguito di attivazione da parte del Servizio Centrale Operativo e del Servizio per la Cooperazione Internazionale di Polizia-Gruppo ENFAST-Divisione SIReNE, ha permesso al personale del Servizio di Polizia Postale e delle Comunicazioni Roma, unitamente alla Squadra Mobile di Rimini, di eseguire un Mandato di Arresto Europeo emesso dalla Germania per omicidio volontario, nei confronti di un trentenne di nazionalità turca, incensurato in Italia, ricercato su tutto il territorio Schengen, che veniva rintracciato presso una struttura ricettiva di questo centro.
In particolare, fin dalla giornata del 25 gennaio erano stati effettuati dalla Squadra Mobile

accertamenti di natura tecnica e dinamica, a riscontro dell'attività svolta dal Servizio di Polizia Postale e delle Comunicazioni, che aveva proceduto allo sviluppo della labile traccia informatica relativa ad un dato telematico anonimo e alle successive attività di OSINT, individuandone la posizione in zona Marina Centro, accertamenti a seguito dei quali, si giungeva all'individuazione certa dello stesso.
Il turco, sottoposto a perquisizione presso l'hotel dove aveva preso alloggio con false generalità, veniva trovato in possesso di una pistola calibro 9x19 marca "Glock", con doppio caricatore e nr. 14 cartucce 9x19 con ogiva blindata, catalogabili come munizionamento "da guerra". All'esito degli immediati accertamenti svolti, l'arma era da ritenersi clandestina in quanto non censita sul catalogo Nazionale delle Armi, risultando altresì oggetto di segnalazione della Polizia Tedesca, per fatti accaduti su qual territorio. Venivano trovati anche documenti d'identità falsi, alcuni smartphone e altro materiale di interesse investigativo.
Il soggetto quindi è stato tratto in arresto, oltre che per il MAE anche per la flagranza di reato riguardo alla detenzione e porto dell'arma clandestina, nonché del munizionamento da guerra e per il possesso dei documenti falsi. Al termine delle incombenze di rito è stato associato presso la casa circondariale di Rimini a disposizione delle Autorità Giudiziarie procedenti.

Appare opportuno evidenziare anche un'ulteriore attività investigativa, parimenti avviata dalla Polizia Postale, nell'ambito dello scambio informativo all'interno della rete di uffici dell'European Network Fugitive Active Search Teams (E.N.F.A.S.T.), a seguito della segnalazione pervenuta dalla Direzione Centrale della Polizia Criminale - Servizio Cooperazione Internazionale di Polizia -Divisione S.I.Re.N.E., inoltrata dal collaterale ufficio tedesco.
Nel dettaglio, in data 11.02.2023, personale della Squadra Mobile della Questura e del Centro Operativo per la Sicurezza Cibernetica di Palermo ha tratto in arresto un cittadino straniero di 26 anni, ricercato in Italia e in ambito Schengen poiché destinatario di un mandato d'arresto europeo emesso dalla Germania, per i reati di tentato omicidio in concorso e istigazione a delinquere. Lo stesso era anche ricercato in Italia poiché destinatario di un ordine di carcerazione emesso dalla Procura della Repubblica presso il Tribunale di Ferrara, dovendo espiare la pena definitiva di anni 9 e giorni 1 di reclusione per reati di spaccio di stupefacenti, detenzione di armi clandestine, furto aggravato, resistenza e minacce a P.U.
In particolare, gli approfondimenti informatici condotti nell'immediato dal Servizio Polizia Postale e delle Comunicazioni, effettuati sulle connessioni internet all'account social del ricercato, hanno permesso di localizzare il ricercato nella zona del centro storico palermitano.
La prosecuzione degli accertamenti investigativi condotti da personale del C.O.S.C. e della sezione omicidi della Squadra Mobile di Palermo, anche attraverso una complessa attività di O.C.P., ha consentito la sua compiuta identificazione, nonostante utilizzasse documenti falsi e numerazioni telefoniche intestate ad altri connazionali.
Appreso che il ricercato necessita di trattamenti medici di emodialisi per una grave malattia, sono state condotte in meno di 24 ore accurate ricerche dagli operatori delle strutture investigative, presso le strutture sanitarie del capoluogo siciliano, deputate al trattamento

di tale patologia. Pertanto lo stesso è stato individuato, nonostante le false generalità dichiarate, presso il reparto di nefrologia di un ospedale di Palermo e tratto in arresto e condotto, dopo le formalità di rito, presso la Casa Circondariale "A. Lorusso" Pagliarelli di Palermo.
Tra le numerose attività investigative effettuate nell'ambito del cd. cyberterrorismo appare opportuno evidenziare l'operazione "Alchimia" che ha permesso l'identificazione di diversi minori che sperimentavano miscele esplosive con sostanze chimiche acquistate su internet, i cui effetti venivano documentati con la pubblicazione di foto e video sui social.
In particolare, grazie ad una complessa attività di polizia giudiziaria, condotta tra ottobre 2022 e febbraio 2023, gli investigatori del Centro Operativo per la Sicurezza Cibernetica di Milano hanno individuato alcuni spazi Telegram utilizzati da adolescenti per condividere le loro esperienze su armi ed esplosivi.
Gli internauti, tutti minorenni e residenti in diverse aree geografiche del territorio italiano, erano accomunati dalla passione per le armi. A tal proposito, qualcuno ha affermato *"I miei genitori sono contrari alle armi allora me le fabbrico io oppure me le prendo da qualche parte [...] Ci ho sparato con una glock vera... [...] Te lo dico perché le modifico da quando avevo 14 anni [...]"*.
Nelle chat, infatti, affermavano di andare in giro con coltelli e a volte persino con pistole (a salve o da softair), incuranti di possibili controlli da parte delle forze dell'ordine, come riscontrato in altre frasi del seguente tenore: *"Io avevo una glock però poi ci sono andato a scuola perché lo avevo visto in un film americano [...] io sono andato con un multitool con coltello, rischiato molto di andare al minorile [...] Io portavo quello a scatto nel giubbino"*.
Spesso pubblicavano anche foto e video che mostravano armi da taglio, da sparo e da softair, esposte in posa o durante l'effettivo utilizzo.
Nelle loro discussioni su Telegram richiedevano informazioni e consigli su come confezionare molotov, esplosivi e detonatori, pubblicando anche foto degli ordigni realizzati, scrivendo *"avete mai fatto una molotov? io si [...] martedì provo a fare del napalm [...] Qualcuno ha un video Tutorial per un detonatore? [...] buon pomeriggio, ecco a voi un piccolo dispositivo. [...]"*.
Al termine dell'indagine, coordinata dal Tribunale per i Minorenni di Milano, nella mattinata del 28 giugno scorso la Polizia Postale, in collaborazione con le DIGOS e con l'ausilio di unità cinofile specializzate della Polizia di Stato, ha eseguito 8 perquisizioni nelle città di Avellino, Lecce, Milano, Pisa, Sassari, Nuoro e Treviso.
Si rappresenta, infine, che il 24 luglio 2023 è stato pubblicato in Gazzetta Ufficiale il decreto legislativo n. 107, in vigore dal 26 agosto u.s., per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2021/784, relativo al contrasto della diffusione di contenuti terroristici online.
Si segnala come il quadro normativo unionale e la normativa attuativa, determinano per il Servizio Polizia Postale e delle Comunicazioni, Organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione, l'attribuzione di importanti competenze ed un ruolo cardine nel nuovo scenario nazionale e internazionale relativo al contrasto della diffusione di contenuti terroristici online.
E invero, la Polizia Postale e delle Comunicazioni assumerà specifiche competenze nelle

procedure di emissione degli ordini di rimozione, nell'emissione delle decisioni di cui all'art. 5 par. 4 del Regolamento, nonché nella fase sanzionatoria.
In particolare, con riferimento all'emissione degli ordini di rimozione, la Polizia Postale fornirà il necessario supporto tecnico ai punti di contatto delle Autorità competenti nell'assolvimento dei propri compiti, al fine di ottimizzare le complesse e rapide procedure di rimozione dei contenuti terroristici online, previste dal Regolamento (UE) 2021/784.
Ed ancora, la Polizia Postale avrà il compito di portare a conoscenza l'ordine di rimozione, adottato con decreto motivato dell'Autorità competente, ai titolari delle piattaforme di comunicazioni online, destinatari del provvedimento stesso.

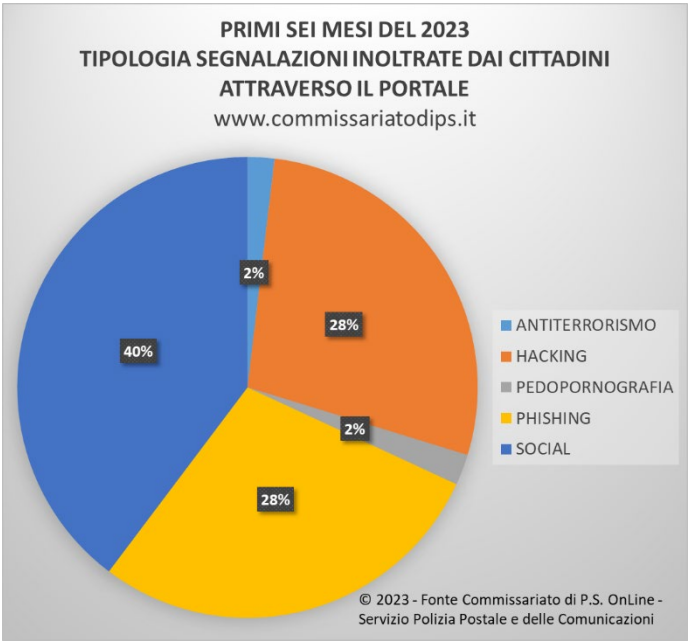
Inoltre, la Polizia Postale è l'Autorità competente:
- emettere la decisione circa la valutazione se le piattaforme siano "esposte a contenuti terroristici" (ad esempio, per aver già ricevuto due o più ordini di rimozione definitivi nei 12 mesi precedenti);
- sorvegliare l'attuazione delle misure specifiche imposte ai titolari delle piattaforme online esposte a contenuti terroristici;
- emettere le ulteriori decisioni nei confronti del prestatore di servizi hosting che non abbia adottato misure specifiche adeguate a contrastare l'uso improprio dei suoi servizi per la diffusione al pubblico di contenuti terroristici.

Per l'adempimento delle incombenze imposte dal Regolamento europeo e dalla normativa nazionale di recepimento, la Polizia Postale curerà l'utilizzo dello strumento informatico denominato PERCI, con il coordinamento svolto dall'EU-IRU di Europol, e dovrà occuparsi delle segnalazioni ai fornitori di servizi hosting delle risorse web con contenuti illeciti di carattere terroristico di volta in volta interessati dalla segnalazione, previa attività di deconfliction, in raccordo con la Direzione Centrale della Polizia di Prevenzione.

Commissariato di P.S. online

L'uso crescente delle nuove tecnologie ha reso necessario lo sviluppo e il potenziamento di nuovi strumenti di comunicazione che consentissero alla Polizia di Stato di mettersi in contatto diretto con gli utenti del *web*.
In tale ottica il portale del Commissariato di P.S. online ha permesso al cittadino, abituato ormai a utilizzare la rete internet per svolgere le principali attività quotidiane, di rivolgersi agli operatori della Polizia Postale in qualsiasi momento e in qualunque luogo si venisse a trovare.
Attraverso questo strumento l'utente ha la possibilità di esprimere il proprio disagio per un torto subito, segnalare comportamenti che giudica illeciti e chiedere aiuto per superare difficoltà e problematiche, anche nei casi in cui potrebbe essere fonte di disagio rappresentarle di persona.
La facilità con cui il cittadino riesce a interagire con la piattaforma dedicata rende possibile raccogliere le segnalazioni di quegli utenti che, mossi da spirito altruistico e di

collaborazione, si rivolgono alla Polizia Postale e delle Comunicazioni in un'ottica di sicurezza partecipata - nella sua declinazione online - fornendo utili evidenze su fenomeni emergenti potenzialmente lesivi, così contribuendo, in termini di efficace prevenzione, a evitare che altri internauti possano cadere nelle trappole della Rete: grazie al servizio online dedicato all'inoltro di segnalazioni e alla richiesta di informazioni accessibile dal portale, infatti, gli operatori della Specialità, possono orientare l'analisi rispetto a condotte delittuose anche emergenti ed elaborare idonee strategie di contrasto.
L'analisi delle 39.020 segnalazioni ricevute nel primo semestre 2023, ha evidenziato la necessità di potenziare le attività di informazione e prevenzione sulle tematiche della sicurezza informatica, introducendo sezioni di approfondimento e attivando mirate collaborazioni che rendessero facilmente fruibile ed efficace la comunicazione con il cittadino.



In tale ottica sono stati incrementati gli spazi web, con l'attivazione di nuovi profili social (Twitter e Linkedin in aggiunta alle già presenti pagine facebook) ed è stata arricchita l'area riservata agli approfondimenti e alla pubblicazione di "avvisi per gli utenti", un efficace strumento di autotutela messo a disposizione degli internauti per riconoscere le truffe del momento e non cadere nei raggiri.

Tra i fenomeni emergenti nel primo semestre del 2023 si evidenzia l'uso frequente dello *spoofing*[5] per il compimento di truffe che mirano a rendere credibili richieste di trasferimento di denaro fraudolente; l'aumento, conseguente all'elevato numero di account social rubati, di richieste estorsive e di false comunicazioni di assistenza da parte dei *social network* per il recupero di account rubati; l'uso dello *smishing*[6] per segnalare fraudolentemente presunti accessi anomali e richieste di autorizzazione sul conto corrente.
In continua crescita il numero delle segnalazioni di estorsioni a sfondo sessuale e delle truffe sugli acquisti online che colpiscono parimenti acquirente e venditore.
La tipologia di segnalazioni che ha subito l'incremento maggiore è la richiesta di aiuto: utenti che manifestano intenzioni autolesioniste a seguito di patite situazioni di disagio. Sono complessivamente 120 i casi trattati, che comprendono anche le richieste ricevute dalle redazioni di note trasmissioni televisive, per i quali spesso si è reso necessario attivare l'intervento diretto di pattuglie presenti sul territorio.

COMMISSARIATO P.S. ONLINE Primo semestre 2023	
Segnalazioni pervenute	39.020
Informazioni richieste	10.485
Visite al sito[7] www.commissariatops.it	1.216.353
Accessi al sito[8] www.commissariatodips.it	23.781.956

Campagne preventive di sensibilizzazione

Nella propria *mission* istituzionale, la Polizia Postale e delle Comunicazioni, affianca all'attività di contrasto un'importante opera di prevenzione che si esplica, oltre che attraverso il costante monitoraggio della rete, nella pianificazione e realizzazione di campagne di sensibilizzazione, rivolte principalmente ai bambini e agli adolescenti, per accrescere la loro consapevolezza nei confronti dei rischi e delle insidie della rete, che consenta loro un corretto utilizzo delle nuove tecnologie.

[5] Particolare tipologia di attacco che consente di nascondere la propria identità per risultare affidabile alla vittima designata al fine di ottenere accesso a informazioni riservate e dati sensibili.

[6] Tecnica di phishing attraverso l'uso di sms.

[7] Numero delle volte che il sito è stati visitato.

[8] Numero di pagine del sito visionate.

L'impegno profuso dagli operatori della Polizia Postale nel dialogo con le nuove generazioni, con la collaborazione delle istituzioni scolastiche, costituisce un elemento cardine nell'attività di prevenzione di specifiche fenomenologie delittuose, il cui concreto verificarsi è impedito, talvolta, proprio in virtù delle segnalazioni avvenute nel corso degli incontri. Il coinvolgimento diretto dei ragazzi su tematiche potenzialmente sensibili si dimostra sempre più una formula vincente ed efficace nell'importante percorso dell'attività di prevenzione.

Tra le iniziative più significative, si evidenzia "Una vita da Social", campagna educativa itinerante, giunta oramai alla sua X edizione, realizzata attraverso l'utilizzo di un'aula multimediale e interattiva, installata a bordo di un *truck* che attraversa numerose località italiane ed estere per affrontare insieme a studenti, docenti e genitori i temi della cybersicurezza e dell'uso dei *social network*. Questo progetto ha raggiunto, nel primo semestre del 2023, un totale di 163.715 ragazzi.

Lo scorso 2 febbraio presso l'Auditorium Parco della Musica a Roma, alla presenza di più di 3000 studenti, è stato proiettato il docu-film "SENZA RETE", prodotto in collaborazione con la RAI, in cui vengono raccontate storie e testimonianze di ragazzi vittime di bullismo e *cyber-bullismo*, alcune delle quali con tragico epilogo.

Il 7 febbraio, si è celebrato il "SAFER INTERNET DAY", un evento seguito da più di 470.000 studenti attraverso la diretta *streaming*, unitamente al progetto #CUORICONNESSI, nato dalla collaborazione tra Unieuro e Polizia di Stato contro il cyberbullismo, con l'obiettivo di responsabilizzare i ragazzi, soprattutto delle scuole di primo e secondo grado, sull'uso consapevole di internet. In occasione dell'evento, è stato promosso il quarto volume di "#CUORICONNESSI – cyberbullismo, bullismo e storie di vita online, la realtà delle parole", in cui i giovani si mettono a nudo trovando il coraggio di raccontare le proprie storie.

Analisi dei principali attacchi noti del primo semestre 2023 verso il settore Manufacturing a livello globale e in Italia

Presentiamo qui alcune informazioni a complemento dei dati del rapporto Clusit 2023 con la situazione degli attacchi andati a buon fine e di pubblico dominio verso il settore **Manufacturing** nel primo semestre dell'anno in corso e il confronto con gli anni precedenti (2018-22).
Nel rapporto sono presentati i dati globali, separando poi gli attacchi globali da quelli verso il nostro paese.
Nelle tabelle, la prima a livello globale e la seconda in Italia, sono indicati sia il totale di attacchi verso il settore MFG che gli attacchi totali dell'anno/periodo in corso e, successivamente, la percentuale di attacchi verso il settore rispetto al totale.

A livello Global

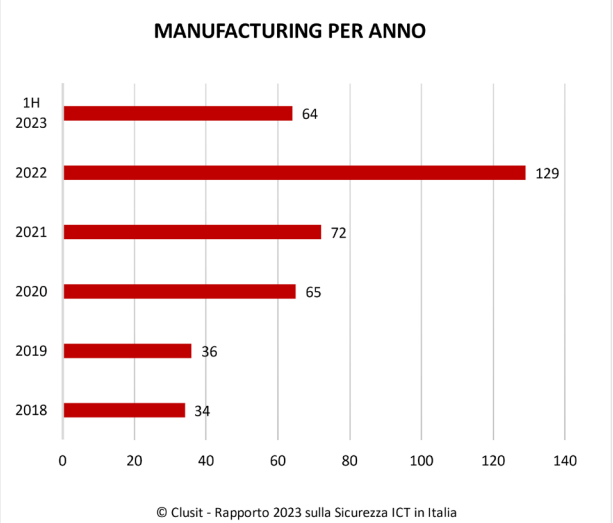
ATTACCANTI	2018	2019	2020	2021	2022	1H 2023	TOTALE
Cybercrime	21	24	58	68	116	62	349
Hacktivism	0	0	0	0	4	1	5
Espionage / Sabotage	10	12	6	4	9	1	42
Information Warfare	3	0	1	0	0	0	4
Totale attacchi MFG per anno	34	36	65	72	129	64	400
Totale attacchi per anno	1554	1667	1874	2049	2489	1377	11010
% attacchi MFG su Totale dell'anno	2,2%	2,2%	3,5%	3,5%	5,2%	4,6%	3,6%
% Crescita MFG anno su anno	0,0%	5,9%	80,6%	10,8%	79,2%		

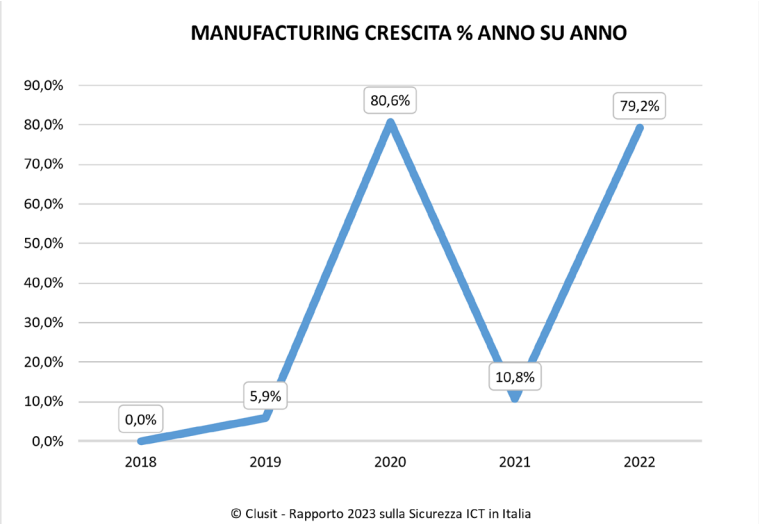
A livello Italia

ATTACCANTI	2018	2019	2020	2021	2022	1H 2023	TOTALE
Cybercrime	0	0	8	12	35	22	77
Espionage / Sabotage	2	2	1	0	0	0	5
Information Warfare	0	0	0	0	0	0	0
Hacktivism	0	0	0	0	0	0	0
Totale per anno	2	2	9	12	35	22	82
Totale attacchi per anno	1554	1667	1874	2049	2489	1377	11010
% attacchi MFG su Totale dell'anno	0,1%	0,1%	0,5%	0,6%	1,4%	1,6%	
% Crescita MFG anno su anno	0,0%	0,0%	350,0%	33,3%	191,7%		

Infine, è stata calcolata la percentuale di crescita anno su anno, portando a 0% il 2018: i numeri (visibili anche nel secondo grafico) indicano di quanto sono cresciuti gli attacchi rispetto all'anno precedente.
Nei grafici, invece, oltre all'andamento totale degli attacchi verso il settore e la crescita anno su anno, sono indicati per ogni categoria (attaccante, tecnica, geografia delle vittime e severity degli attacchi) un confronto tra la situazione del 2022, quella del primo semestre 2023 e i trend 2018-1H23.

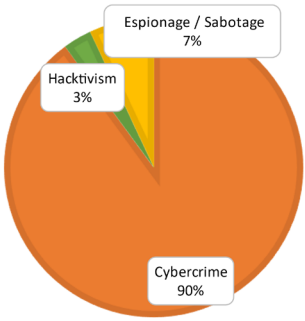
Riassumendo la situazione: gli attacchi verso il settore Manufacturing sono cresciuti, con un raddoppio tra il 2019 e il 2021, fino ad arrivare al loro massimo storico nel 2022 (+79% rispetto al 2021). Come vediamo il 2023 è in linea con il 2022. Infatti nel primo semestre 2023 gli attacchi hanno sostanzialmente raggiunto il totale registrato negli anni 2020/2021 e la metà di quelli del 2022, quindi il trend di crescita pare essere confermato.


MANUFACTURING PER ANNO
1H 2023
64
2022
129
2021
72
2020
65
2019
36
2018
34
0
20
40
60
80
100
120
140
© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia


MANUFACTURING CRESCITA % ANNO SU ANNO
90,0%
80,0%
70,0%
60,0%
50,0%
40,0%
30,0%
20,0%
10,0%
0,0%
0,0%
5,9%
80,6%
10,8%
79,2%
2018
2019
2020
2021
2022
© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia

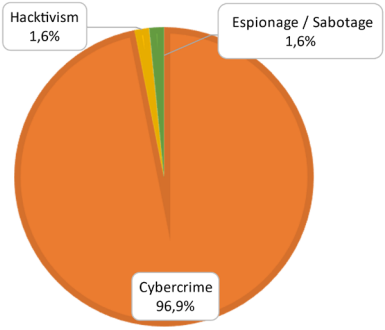
Il Cybercrime si conferma la minaccia principale per questo settore con oltre il 90% dei casi (in Italia si verifica nel 100% !)

MANUFACTURING PER ATTACCANTE 2022



© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia

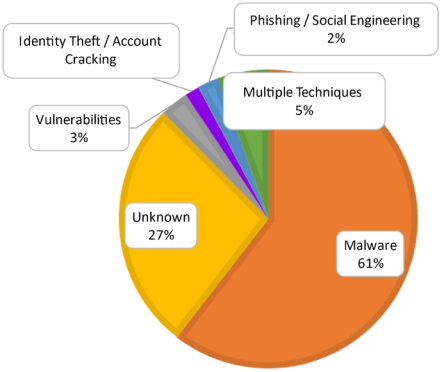
MANUFACTURING PER ATTACCANTE 1H 2023



© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia

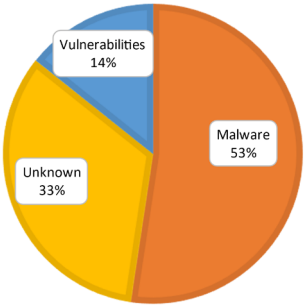
Il Malware (nello specifico ransomware) che rimane oltre il 50% anche nel 2023, Data Breach (indicati come tecnica "unknown") e Vulnerabilità (in particolare 0-day) sono le tecniche di attacco più sfruttate. Da notare il trend in aumento dello sfruttamento delle Vulnerabilità nel 2023.

MANUFACTURING PER TECNICA 2022



© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia

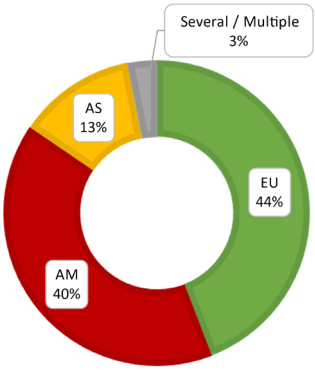
MANUFACTURING PER TECNICA 1H 2023



© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia

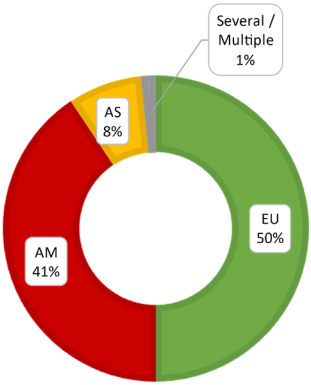
L'Europa è il continente più attaccato, arrivando a coprire il 50% degli attacchi verso il settore nei primi 6 mesi del 2023. Segue l'America, una minoranza di attacchi verso l'Asia e pochissimi verso location multiple. (Da valutare meglio la consistenza dei numeri relativi ad attacchi nel "Rest Of the World", ovvero Asia, Oceania, Africa che risultano poco rappresentativi).

MANUFACTURING PER GEOGRAFIA 2022



© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia

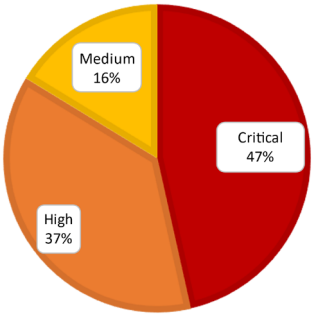
MANUFACTURING PER GEOGRAFIA 1H 2023



© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia

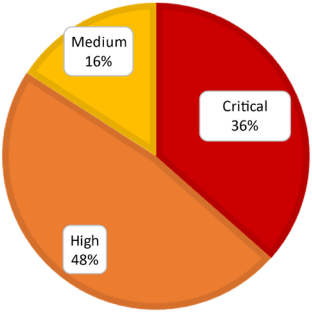
Gli attacchi con impatti critici erano quasi la metà nel 2022 (47%) e sono momentaneamente scesi al 36% nel 2023 (vedremo poi cosa succede alla fine dell'anno).

MANUFACTURING PER SEVERITY 2022



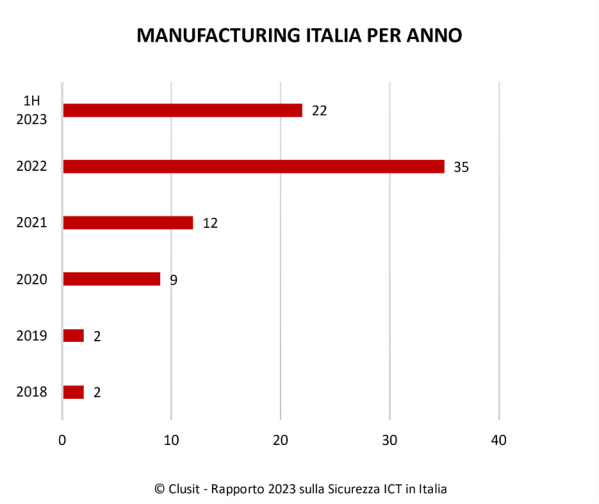
© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia

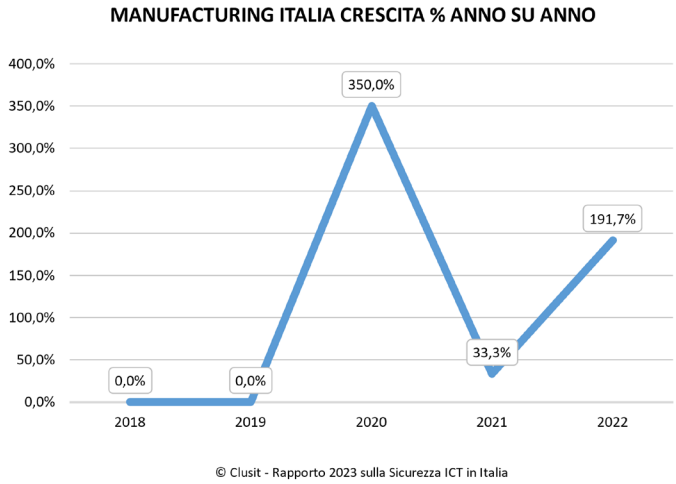
MANUFACTURING PER SEVERITY 1H 2023



© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia

Per quanto riguarda l'Italia invece: nel 2022 gli attacchi verso il settore sono cresciuti in maniera allarmante (+192%), triplicati rispetto all'anno precedente.



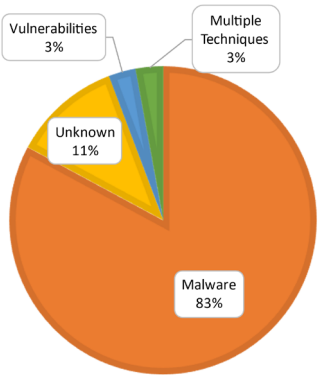


Nel primo semestre 2023 sebbene in numeri assoluti gli attacchi siano inferiori a quelli dell'anno precedente, in termini percentuali rispetto ai numeri globali, rappresentano l'1,6% del totale degli attacchi (contro l'1,4% del 2022). Irrilevanti in passato, crescita con picchi nel 2020 (+350%) e 2022 (+191%). Primo semestre 2023 in linea con 2022, e pari alla somma del periodo 2018-2021

Il cybercrime (al 100% del totale) è l'unica motivazione degli attacchi verso il settore nel nostro paese fin dal 2021 e le tecniche utilizzate seguono i trend globali, con il Malware/Ransomware con percentuali elevate sempre confermate.

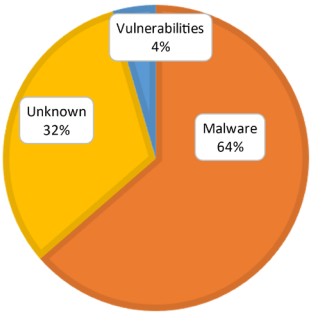
Come già visto a livello globale, Tecnica principalmente utilizzata (83%) è Malware/Ransomware, poi «Data Breach» (Unknown), a seguire poche Vulnerabilità (0-Days) sfruttate.

MANUFACTURING ITALIA TECNICHE 2022



© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia

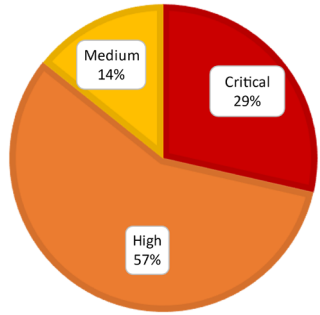
MANUFACTURING ITALIA TECNICHE 1H 2023



© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia

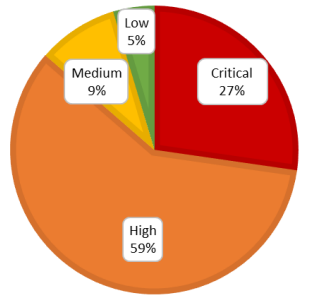
Un aspetto interessante, e anche una conferma, è che nel primo semestre 2023, così come nel 2022, quasi un terzo degli attacchi verso le aziende del settore manifatturiero hanno avuto impatti critici.

MANUFACTURING ITALIA PER SEVERITY 2022



© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia

MANUFACTURING ITALIA PER SEVERITY 1H 2023



© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia

Alcuni dati dal Report Dragos ICS/OT CyberSecurity Year in Review 2022

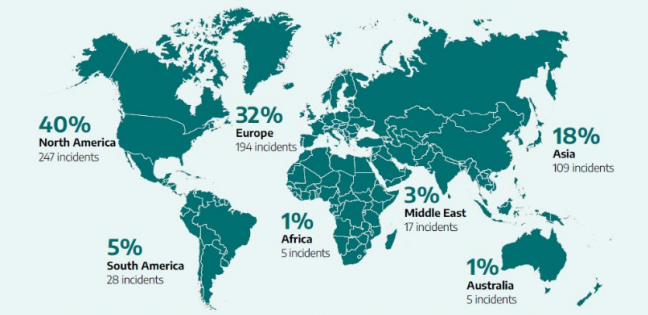
Volendo confrontare i dati del rapporto CLUSIT con altre fonti a livello internazionale, possiamo approfondire l'aspetto del Malware/Ransomware con alcune informazioni contenute nel Report Dragos ICS/OT CyberSecurity Year in Review 2022.
Da questo report possiamo constatare che il Ransomware ha colpito Impianti e sistemi ICS/OT con un aumento del 98% rispetto all'anno precedente, e vediamo anche un aumento del 35% dei gruppi criminali che utilizzano questa tecnica con l'obiettivo di colpire i sistemi di fabbrica.

Nel rapporto Dragos abbiamo anche una suddivisione per settore e sotto-settore industriale.
Il 72% degli attacchi con impatto MFG sono stati in 104 Settori industriali, quali:

- 10% Metalli
- 9% Automotive
- 9% Alimentari
- 6% Elettronica e Semiconduttori.
- 5% materiali edilizia
- 5% costruttori macchine
- 5% plastica
- 4% Farmaceutici
- 3% Oil & Gas

Infine la suddivisione degli attacchi ransomware a livello geografico vede i seguenti numeri:

- 40+5 = 45% Americhe (Nord e Sud)
- 32% Europa (stimiamo 3-4% Italia)
- 18+3+1+1 = 23% MEA/Asia/Oceania



Globally, 40 percent of the ransomware attacks targeted industrial organizations and infrastructures in North America, for a total of 247 incidents; Europe is second with 32 percent or 194 incidents; Asia with 18 percent or 109 incidents; South America with 5 percent; the Middle East with 3 percent; Australia and Africa each had 1 percent. North America remains one of the most highly targeted regions by ransomware.

DRAGOS
SAFEGUARDING CIVILIZATION

Alcuni dati dal Microsoft Digital Defense Report (Oct.2023)

Valutando il livello di esposizione a Vulnerabilità, censite come CVE (Common Vulnerability Exposure) riguardo a sistemi OT/IoT/IIoT, abbiamo alcuni dati che qui riportiamo:

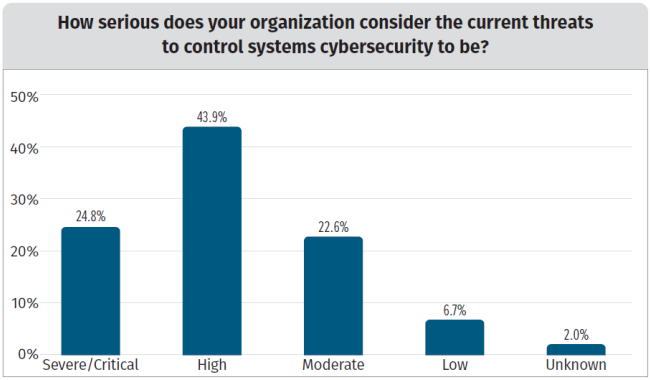
- del 78% dei device IoT con Vulnerabilità conosciute, abbiamo il 46%, quasi la metà, senza possibilità di patch (ovvero il 36% in assoluto)
- 25% dei dispositivi OT usa software non supportato (senza possibilità di patch)
- 96% delle applicazioni usa componenti software Open Source
- Registrato un +742% dal 2010 degli attacchi su software Open Source
- 57% dei firmware device OT risulta esposto a più di 10 CVE conosciute.

Volendo approfondire alcuni dati riferiti a Device ICS/OT vulnerabili e non vulnerabili (PLC ecc.), possiamo notare che: del 78% IoT con Vulnerabilità conosciute, abbiamo visto che il 46%, quasi la metà, è senza possibilità di patch (ovvero il 36%) ed il 32% potrebbe ricevere patch (il 25%)
Inoltre, fortunatamente, secondo questo studio il 22% risulta non vulnerabile: 15% senza CVE conosciute e il 7% con patch applicate.

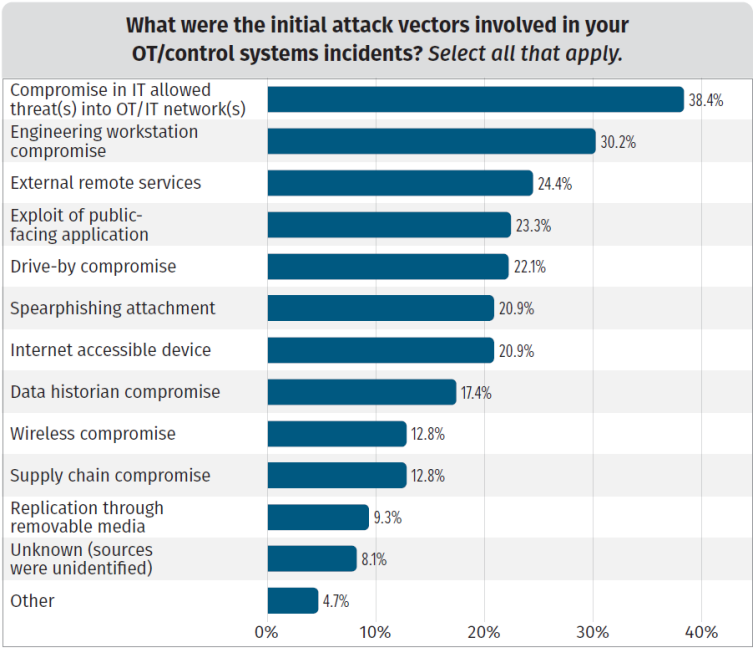
Alcuni dati dal SANS ICS/OT CyberSecurity Survey (Sept.2023)

Dal periodico Survey di SANS veniamo a conoscenza che per il 2022-2023 sono stati intervistati 701 CISO che gestiscono oltre 1.760 Impianti industriali/Utility. Di questi abbiamo 70 CISO Europei (10%) con 245 Impianti (14%) in oltre 60 categorie industriali. Possiamo stimare che ci siano circa una decina di CISO Italiani con 20-30 impianti sul nostro territorio.

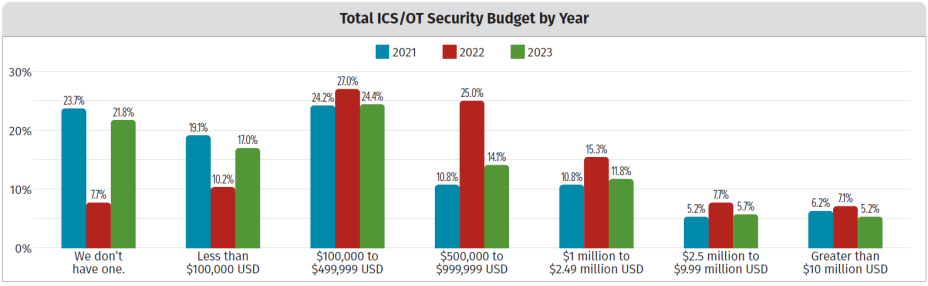
Con riferimento alla pericolosità delle minacce percepite riferite ai sistemi ICS/OT abbiamo il seguente diagramma:



Con riferimento ai vettori iniziali dai quali parte l'attacco all'infrastruttura OT, ecco le risposte:



Infine abbiamo un'analisi dell'andamento del budget a disposizione dei CISO per la protezione dell'infrastruttura OT, in cui risulta una (preoccupante) contrazione generalizzata dei budget.

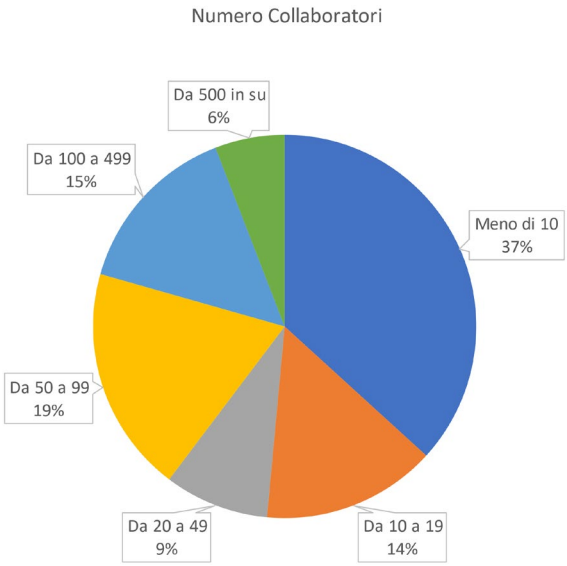


La Cybersecurity nelle piccole e medie imprese
Una survey realizzata in Lombardia con focus nelle province di Varese e Como

Introduzione

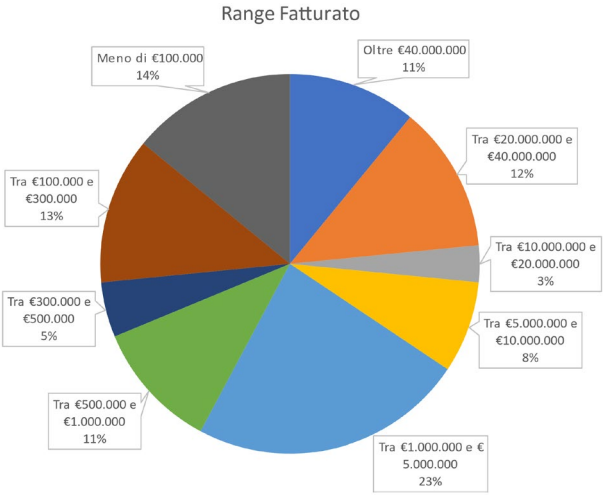
Tra i mesi di Luglio e Settembre 2023, con la collaborazione di Reti S.p.A., abbiamo riproposto ad un nuovo campione di aziende il questionario cybersecurity per PMI che era già stato somministrato a circa un centinaio di aziende tra Novembre 2022 e Gennaio 2023, i cui risultati sono stati pubblicati nell'edizione di Marzo 2023 di questo Rapporto.
Il campione, in questo caso, è leggermente più piccolo (circa 70 aziende) ma comunque significativo , soprattutto considerando che la gran parte dei dati confermano dei trend già largamente visibili nei dati di sei mesi fa.
Presentiamo qui di seguito l'intero dataset dei risultati, raggruppando le domande fatte al campione per temi omogenei.

Struttura dell'azienda

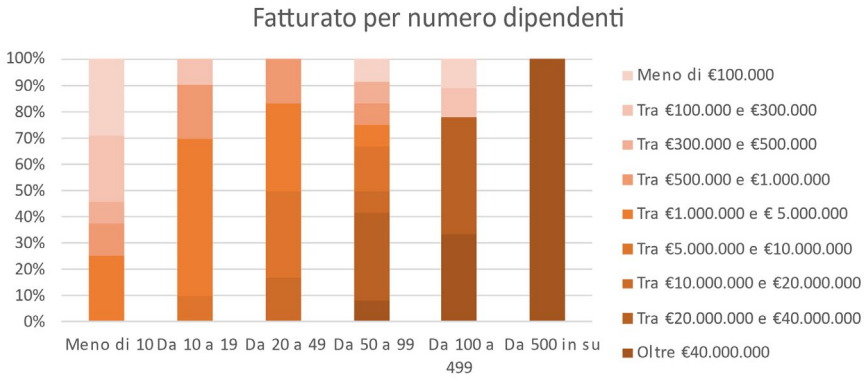


Abbiamo richiesto alle aziende alcuni dati dimensionali, quali ad esempio il numero di collaboratori (a qualunque titolo) ed il fatturato, diviso per fasce.

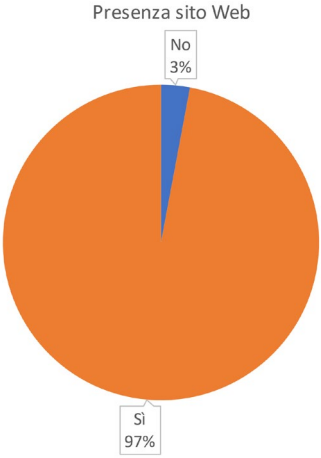
I dati evidenziano una situazione eterogenea tra le aziende coinvolte nel sondaggio in termini di dimensioni e fatturato. È evidente una vasta gamma di variazioni nelle dimensioni delle aziende partecipanti, con alcune aziende che impiegano un numero significativo di dipendenti e altre che sono notevolmente più piccole in termini di forza lavoro.

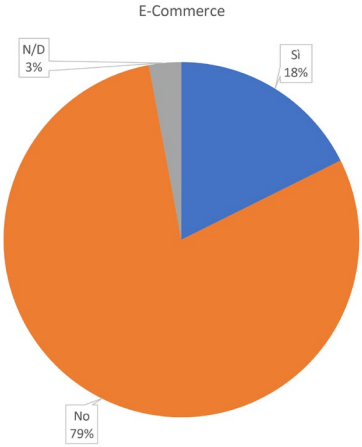


La dimensione prevalente delle aziende coinvolte è comunque quella con meno di 10 dipendenti; La dimensione media nei dati è di 18 collaboratori.
Il fatturato è parimenti molto diverso, ma appare una buona correlazione tra la dimensione e il fatturato, al netto di alcune risposte forse frutto di errori o di omissioni deliberate.



Digital Footprint

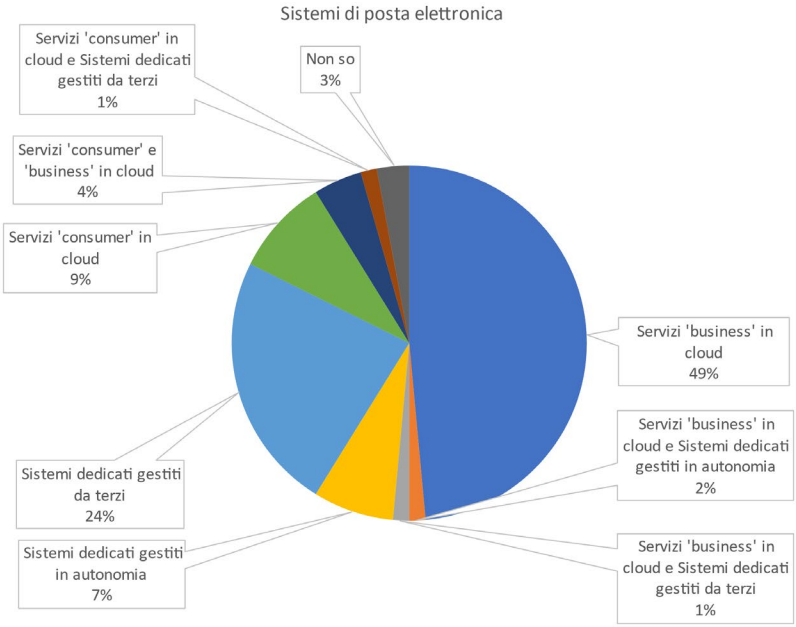




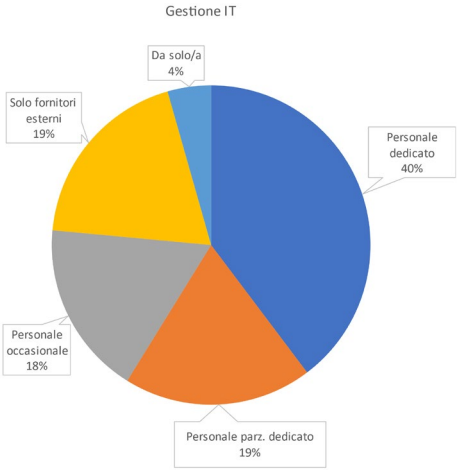
La presenza digitale delle aziende intervistate appare molto completa, con quasi la totalità delle aziende che dichiara di avere un proprio sito Web.

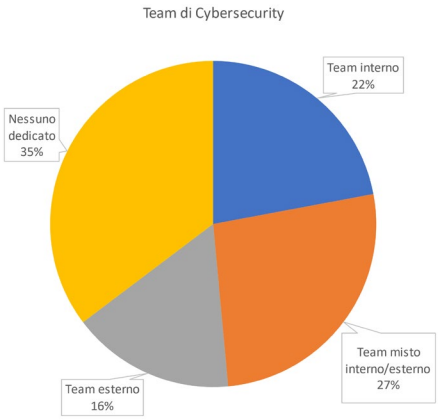
È anche interessante che quasi il 20% delle aziende dichiari di disporre di un sito di e-commerce, il che farebbe pensare che siano aziende più sensibili ai temi della cybersecurity. Vista l'esiguità del campione che risulterebbe, non si ritiene però che i dati relativi siano particolarmente indicativi di una realtà diffusa, e non si è proceduto ad un'analisi incrociata.

Per quanto riguarda la posta elettronica, si registra ormai la prevalenza dei sistemi in cloud, con solo un complessivo 31% che dichiara di usare e-mail su sistemi dedicati. Desta qualche preoccupazione la presenza di numerose realtà che si fanno bastare dei servizi di livello "consumer", cosa che non depone a favore di una forte maturità tecnologica di queste aziende, anche se in molti casi si tratta di realtà di piccole o piccolissime dimensioni. Ricordiamo comunque che un servizio di livello professionale è comunque raccomandabile, poiché dotato in genere di accorgimenti dei quali, invece, una casella (magari gratuita) rivolta al consumatore finale non dispone.



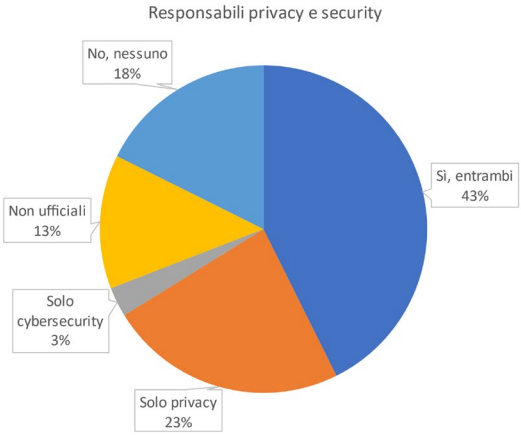
Organizzazione IT, privacy e security





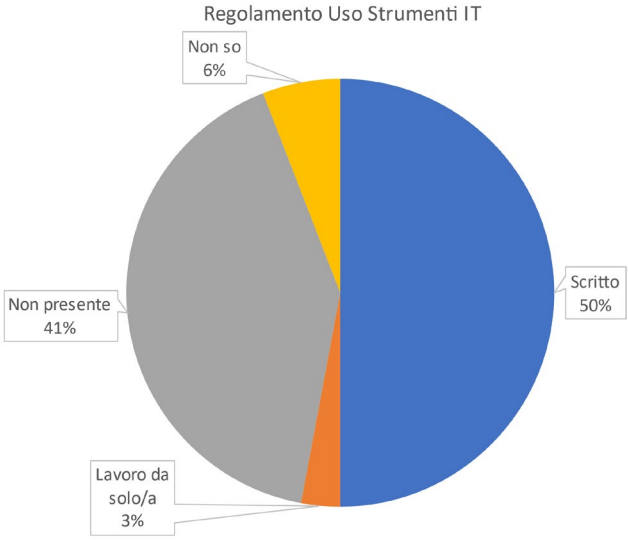
L'organizzazione delle aziende intervistate in merito all'IT ed alla cybersecurity evidenzia chiaramente il diverso livello di maturità delle aziende stesse rispetto alla problematica.
Nel caso del team IT, in buona parte esiste personale dedicato, con soltanto un quinto circa delle aziende che si appoggia esclusivamente a fornitori esterni. Questo peraltro è comprensibile, vista la piccola dimensione media delle aziende nel campione.
Per quanto riguarda la cybersecurity, troviamo invece persone dedicate interne solo in poco più del 20% del totale, mentre, per contro, in più di un terzo del campione troviamo che non vi è alcuna persona identificata, nemmeno esterna. In questi casi dobbiamo supporre che se ne occupino, in caso sia necessario, persone tolte ad altri compiti; con quali competenze e con quale livello di preparazione, non è dato sapere.

È indicativo che in questi casi non vi sia nemmeno l'indicazione di un team esterno, ovvero si è costretti a pensare che l'azienda non abbia nemmeno identificato a priori un fornitore al quale rivolgersi nel momento del bisogno, anche se è banale osservare che i momenti difficili che seguono, ad esempio, alla constatazione di un data breach, non sono quelli più adatti a scegliere con serenità ed accortezza un fornitore per un tema così delicato.



Anche se la presenza di un responsabile cybersecurity dedicato è molto rara, conforta in parte il fatto che in quasi la metà del campione si sia almeno identificata una persona le cui responsabilità includano questo tema. Per quello che si diceva poc'anzi, tuttavia, si è portati a pensare che questa sfortunata persona nella maggior parte dei casi lavori pressoché nell'assenza di qualsiasi supporto dell'organizzazione. In alternativa, come spesso l'evidenza aneddotica potrebbe portare a pensare, il ruolo potrebbe essere solo nominale e di fatto non ricoperto.

La diversa maturità del tema "privacy" viene qui evidenziata dalla presenza invece di una persona responsabile del tema nella gran parte delle organizzazioni; per il 18% che proprio non ne dispone, i dati indicano che si tratta delle realtà più piccole, per le quali è forse difficile trovare le risorse necessarie, anche in termini di tempo.

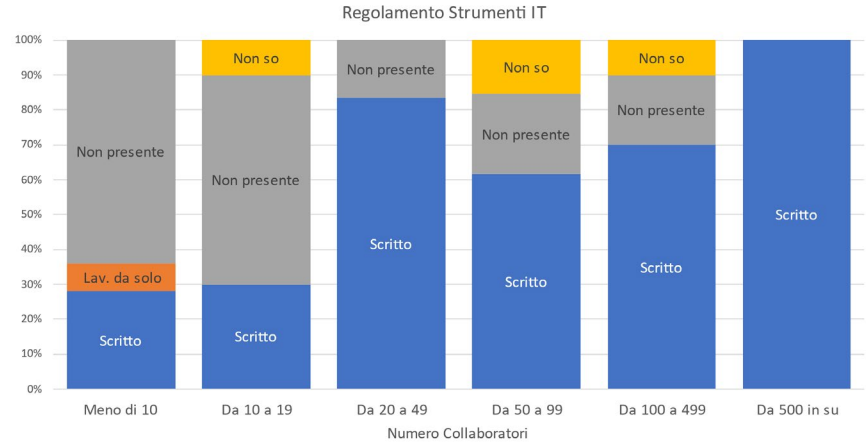


Un tema di security, ma fortemente legato all'ambito privacy, è quello della presenza o no di un regolamento per l'uso da parte del personale della strumentazione IT data in consegna dall'azienda.
Questo regolamento fa parte delle misure fortemente raccomandate anche dall'Autorità Garante per la Protezione dei Dati Personali, e fa quindi comunemente parte della "dotazione minima" anche in ambito privacy. Qualsiasi azienda, anche minima, che doti i propri collaboratori (anche uno solo) di mezzi informatici dovrebbe avere questo regolamento e renderlo ben noto ai suddetti collaboratori.

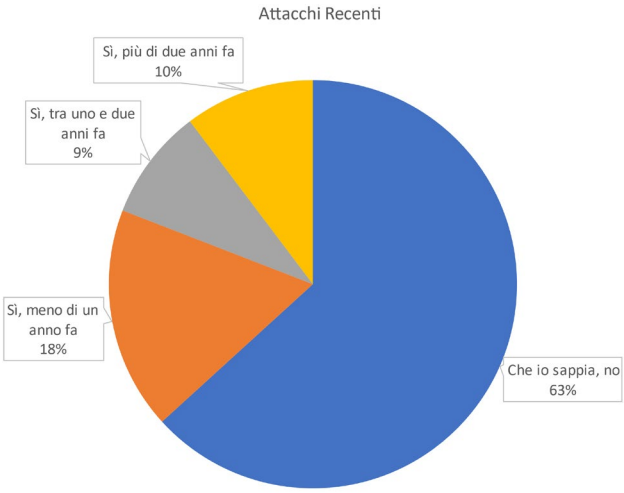
Vediamo invece che, tralasciando le ditte individuali, in quasi metà del campione il documento non è presente, indicando ancora una volta una sottovalutazione del problema da parte di buona parte degli intervistati.

Ma quali sono queste aziende? Lo si può capire bene dal grafico che incrocia la presenza di questo Regolamento con la dimensione aziendale, dal quale appare evidente la correlazione della preparazione con il numero di collaboratori. Nessuna azienda con più di 500 collaboratori ne è priva, mentre nelle aziende con meno di 20 persone meno di un terzo lo adotta,

nonostante si tratti di una misura largamente conosciuta e diffusa, e che non richiede alcuna spesa tecnica.



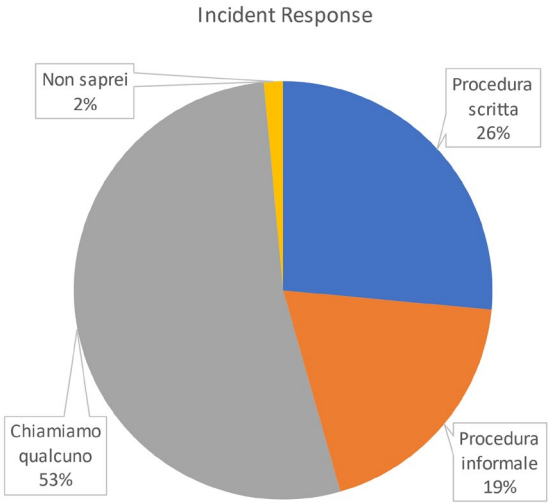
Attacchi recenti e risposta agli incidenti



Nel campione degli intervistati troviamo che la parte interessata da un incidente di cybersecurity in un tempo relativamente recente è del 37%.

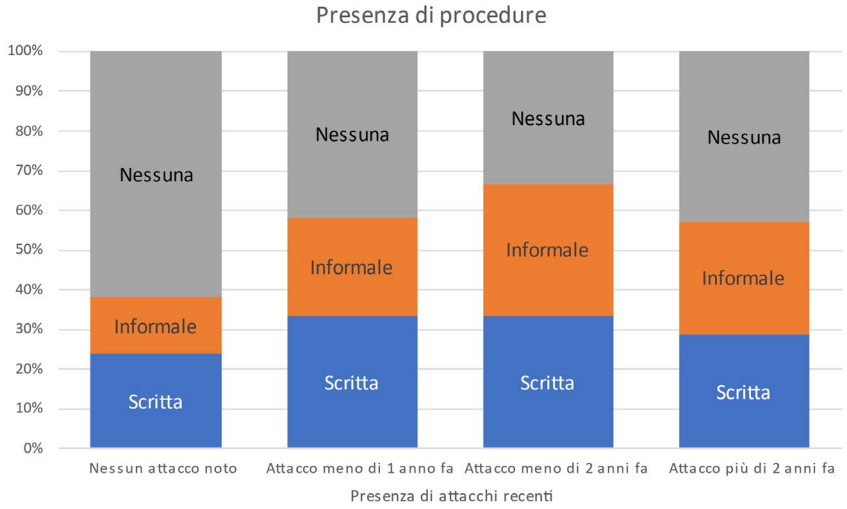
Si potrebbe osservare che è una quota comunque minoritaria, ma è più opportuno invece notare che Il numero di imprese colpite è in rapida crescita: nel Rapporto Clusit di Marzo 2023 presentavamo i risultati della precedente edizione di questa survey, trovando che le imprese colpite erano il 28%.

Il numero di imprese interessate da un incidente è quindi cresciuto di poco più del 32% in sei mesi, cosa che non ci deve lasciare tranquilli.

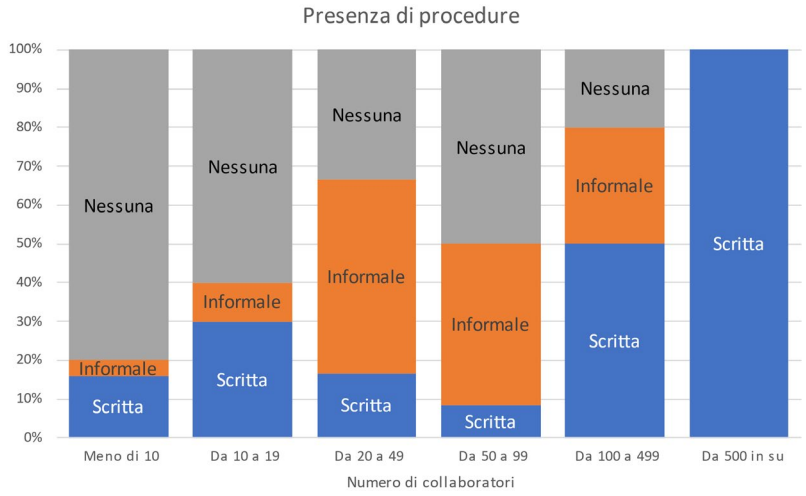


A fronte di questa rapida crescita del numero di aziende colpite, vediamo che il numero di aziende che proprio non si preparano risulta diminuito dal 60% di Marzo 2023 al 53% di oggi, e che il numero di aziende che hanno una procedura scritta è aumentato dal 16% al 26%.
Per capire qualcosa in più del fenomeno possiamo correlare questo stesso insieme di dati, relativo alla preparazione agli incidenti, con la distanza temporale dell'incidente.
Potremmo aspettarci che tutte le aziende colpite tendano ad adottare una procedura formale, anche se magari con una certa latenza; intuitivamente, insomma, potremmo aspettarci una crescita nel tempo delle procedure scritte, al crescere della distanza dell'evento.

Non si assiste invece a nulla di tutto ciò: vediamo forse una piccola differenza tra chi non è mai stato colpito e chi invece lo è stato, ma nessuna correlazione significativa in merito al tempo.

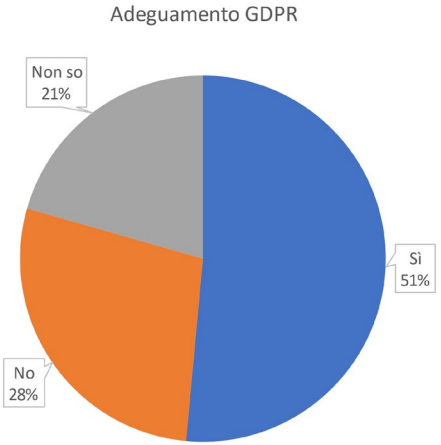


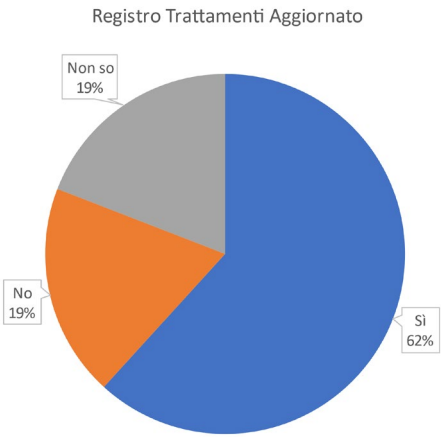
Siamo quindi portati a sospettare che il motivo della differenza nei dati sia un altro. Incrociando il dato precedente con il numero dei collaboratori dell'azienda, troviamo invece, ancora una volta, una evidente correlazione, indicando che molto probabilmente il fattore più pesante è quello dimensionale.



In sintesi, le aziende più preparate sono comunque quelle più grandi, mentre quelle sotto una certa soglia continuano a mostrare difficoltà.

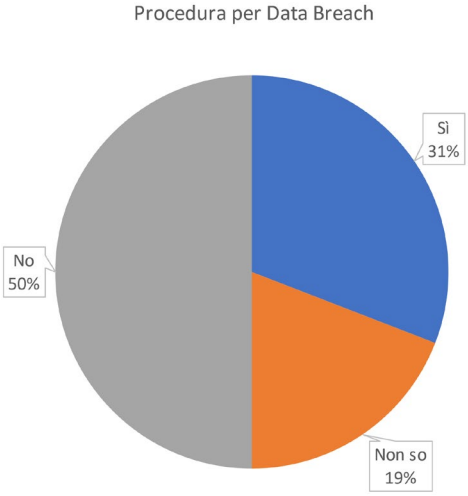
Situazione privacy





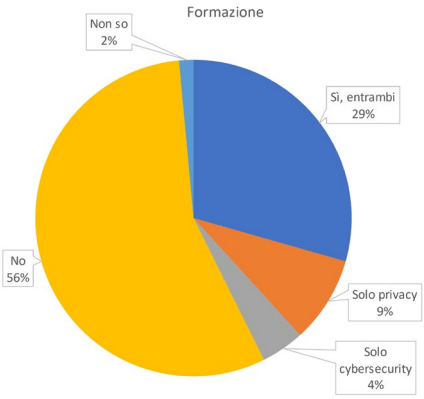
La situazione in ambito privacy risulta abbastanza sotto controllo, con una quota di più di metà del campione che riporta di avere svolto un progetto di adeguamento al GDPR, e quasi due terzi del campione con un registro dei trattamenti aggiornato.

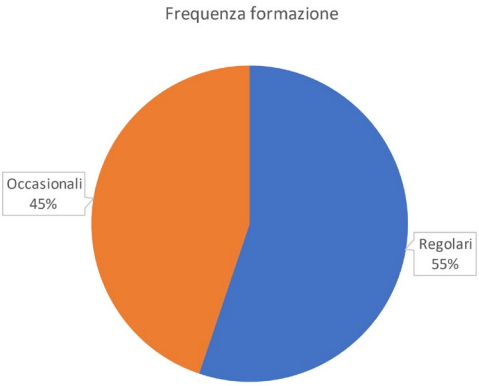
Per quanto si sia ancora lontani da situazioni ottimali, i numeri riflettono una sensibilità al tema ormai diffusa ed anche un adeguamento ben avviato, sebbene in ritardo.



Meno confortante è il dato sulla presenza di una procedura relativa alla gestione dei data breach, confermando ancora una volta – benché sia superfluo – che le aziende difettano gravemente nelle misure preventive.

Formazione

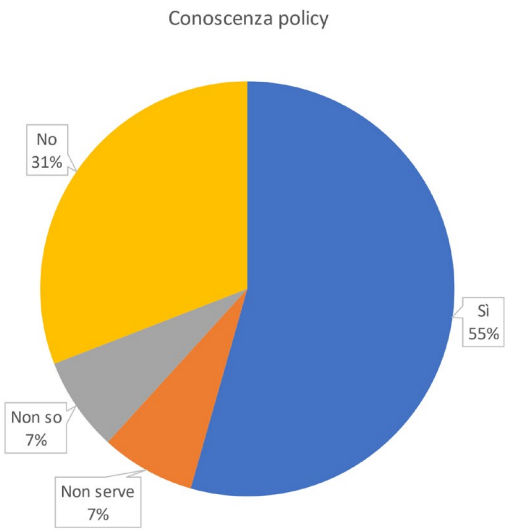




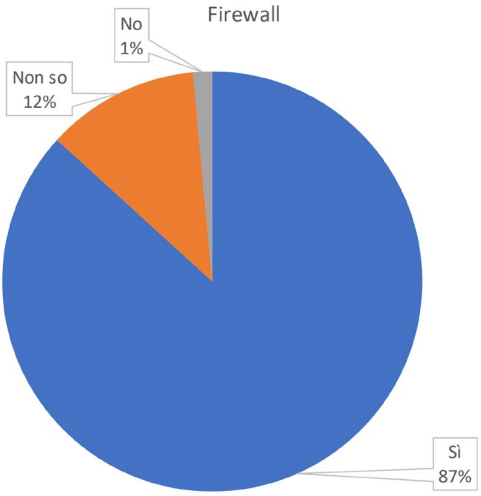
Il panorama della formazione è invece abbastanza triste, solo leggermente meno sconfortante in ambito privacy.

Di fatto solo un terzo delle aziende fa formazione in ambito cybersecurity, e di queste solo poco più di metà lo fa in modo regolare, per cui possiamo concludere che solo circa in un'azienda su sei viene dedicata sufficiente attenzione a questo tema, sebbene sia cruciale. Ricordiamo che le persone sono la prima linea di difesa, ed anche l'ultima.

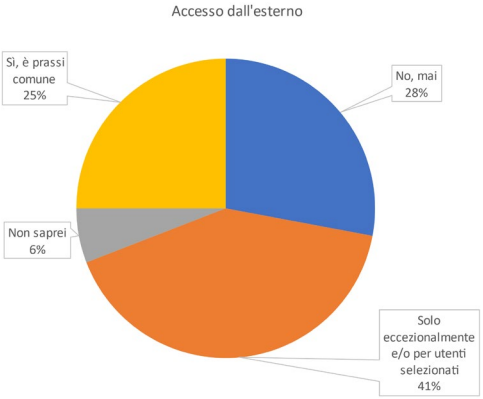
Appaiono quindi ottimistiche le risposte di più di metà degli intervistati, che riportano un'opinione positiva sulla conoscenza da parte delle persone delle policy di sicurezza.

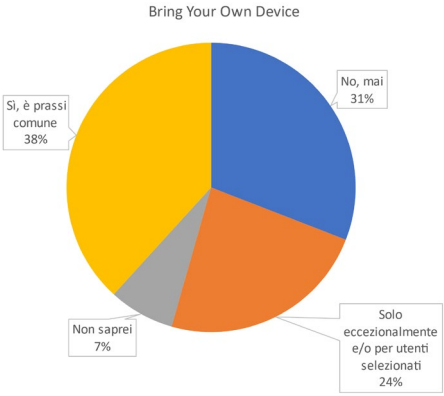


Contromisure comuni



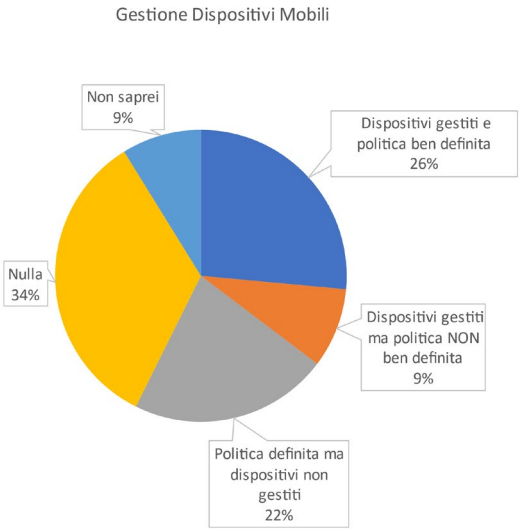
Relativamente ad alcune contromisure di sicurezza molto comuni, vediamo che la protezione di rete è stata ben acquisita, e la gran parte delle reti aziendali è protetta da un firewall.



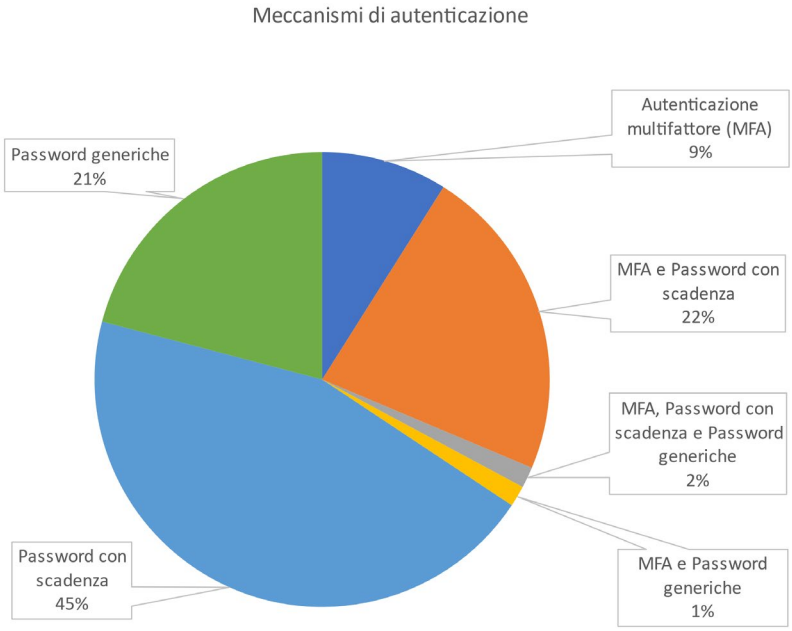


Più contraddittori invece i dati relativi all'accesso alla rete da parte di dispositivi non controllati: se l'accesso dall'esterno (via Internet e simili) è impossibile o comunque molto raro per la grande maggioranza delle aziende, la prassi di consentire l'uso di dispositivi personali all'interno della rete vanifica in buona parte l'efficacia della prima contromisura.

L'uso di un dispositivo non controllato all'interno della rete, infatti, è poco sicuro tanto quanto l'accesso via Internet, se non addirittura peggiore.
A quanto osservato poc'anzi si può aggiungere che il tema della gestione dei dispositivi, soprattutto quelli mobili, appare ancora poco percepito, come si può facilmente evincere dal grafico seguente.



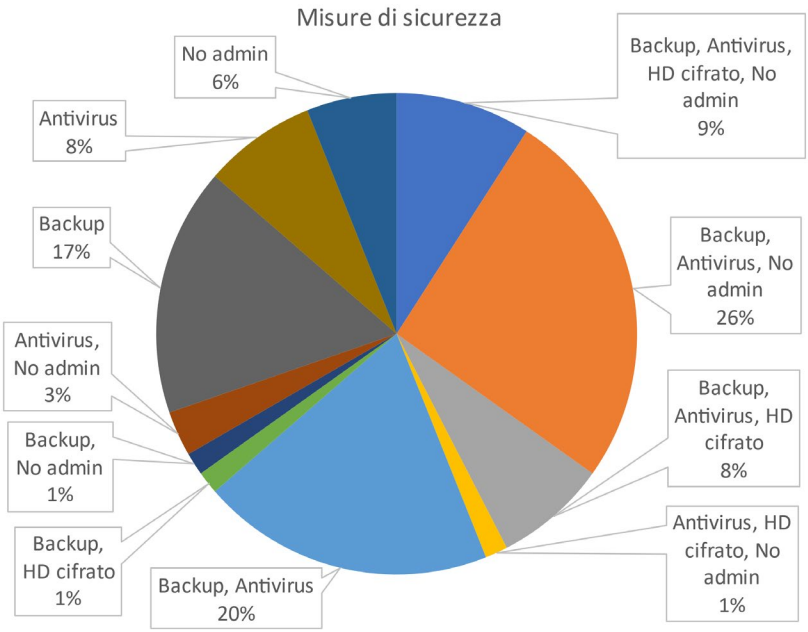
Oggi gli strumenti di gestione del parco di dispositivi mobili (laptop, smartphone, ecc.) sono diffusi e poco costosi, e perciò risulta molto consigliabile la loro adozione, naturalmente insieme ad una ragionevole politica che magari contemperi la possibilità di usare dispositivi propri per l'accesso a dati e sistemi aziendali, con le necessità di protezione dell'azienda.



Anche per quanto riguarda l'autenticazione si registra una notevole immaturità ed una sottovalutazione del problema, che non è più giustificata a fronte della disponibilità di numerosi meccanismi di autenticazione forte, come ad esempio le password monouso via app sullo smartphone, la biometria, e così via, anche a prezzi che rasentano lo zero.

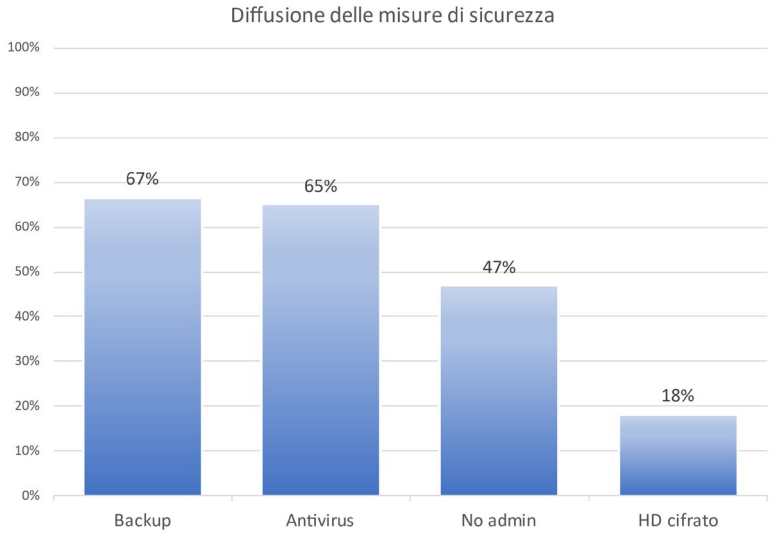
La penultima domanda cercava di misurare la presenza nelle aziende di quattro misure tecnologiche, molto mature e diffuse, e dal costo ormai assai limitato o addirittura nullo:

- backup centralizzato ("Backup");
- antivirus gestito sui dispositivi dell'azienda ("Antivirus");
- configurazione dei dispositivi personali (laptop, smartphone, ecc.) in modo che l'utente non abbia credenziali di amministrazione ("No admin");
- protezione dei dati salvati sui laptop mediante crittografia ("HD cifrato").



Il grafico sopra riporta la diffusione delle varie combinazioni di queste misure, grafico dal quale possiamo vedere che solo il 9% del campione adotta tutte e 4 le misure, e che meno di metà delle aziende ne adotta almeno 3.

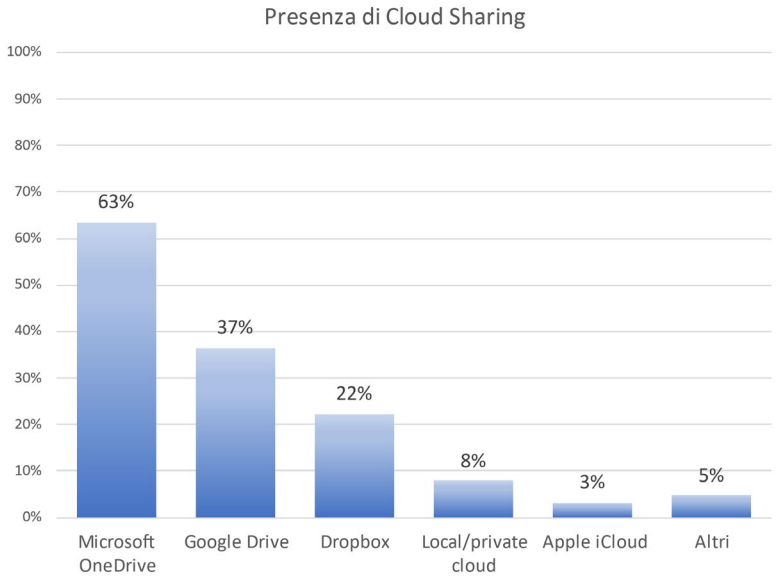
Nel grafico della pagina seguente si può notare come le misure più diffuse siano il backup e l'antivirus, ma anch'esse presenti solo in 2/3 circa del campione. La misura meno adottata è la crittografia dell'hard disk, nonostante sia pressoché gratuita (è inclusa nel prezzo di quasi tutti i sistemi operativi e di quasi tutti gli antivirus) e sia l'unica salvaguardia in caso di furto o smarrimento del dispositivo.



Per concludere, si è indagato sulla diffusione di alcune tecnologie di "Cloud Sharing", che possono essere un ottimo metodo di salvaguardare i propri dati in un ambiente controllato (purché ovviamente ci si fidi del fornitore), ed una linea di difesa, se ben usate, anche contro malware di vari tipi. Queste tecnologie hanno anche il pregio di essere quasi sempre gratuite, per un periodo iniziale e/o per un volume di dati compreso nel prezzo di alcuni servizi.

In questo caso non si è fatta distinzione tra la versione "consumer" e quella "aziendale" di questi servizi, per motivi di semplicità della domanda.

Come si può vedere nel grafico, i meccanismi più diffusi sono quelli proposti dai vendor principali, anche se è interessante notare la presenza di un 8% di tecnologie di "private cloud" realizzate, per lo più, mediante NAS locali dal costo limitato, ma comunque efficaci.



Algoritmi predittivi e approccio risk-based nella gestione delle vulnerabilità: il contributo del catalogo KEV

[A cura di Alfredo Di Gennaro, Giuseppe Massa e Pier Paolo Glave – Cisco]

L'articolo analizza il contributo del catalogo Known Exploit Vulnerabilities (KEV) gestito dal Cybersecurity & Infrastructure Security Agency (CISA), come fattore decisionale, all'interno di una strategia di gestione delle vulnerabilità basata sul rischio. La ricerca evidenzia che solo il 3,2% delle CVE pubbliche rappresenta un rischio reale e spiega perché sia opportuno focalizzarsi in via prioritaria proprio sulla gestione e la mitigazione di questo numero ristretto di vulnerabilità.
In questo contesto si esplorano i dati raccolti da Cisco e dal Cyentia Institute per approfondire diversi aspetti del catalogo KEV, come appunto le vulnerabilità oggetto di exploit attivo, la mancata inclusione di alcune di loro tra le CVE ad alta severity, la rappresentatività dei vendor e le azioni di remediation effettivamente portate avanti dai team di sicurezza e IT operation.

Introduzione

Il Known Exploited Vulnerabilities (KEV) è un catalogo gestito dal U.S. Cybersecurity and Infrastructure Security Agency (CISA) per tenere traccia delle vulnerabilità hw/sw in base al loro effettivo sfruttamento per fini malevoli.
In questo articolo approfondiremo le logiche con cui è stato costruito il catalogo del CISA e il valore che esso fornisce nel processo decisionale, partendo dalle ricerche compiute dal Cyentia Institute che, in collaborazione con Cisco, ha recentemente rilasciato la nona edizione della pubblicazione "Prioritization to Prediction" (P2P), che analizza, appunto, le problematiche legate alla gestione delle vulnerabilità[1] mettendo in relazione i suoi dati con quelli del catalogo KEV.
In particolare, vedremo come il KEV possa essere considerato una delle più significative sorgenti di informazioni in un programma di Vulnerability Management Basato sul Rischio (RBVM) ed analizzeremo i risultati più importati della ricerca del Cyentia Institute, che sono qui di seguito anticipati:

- il catalogo KEV contiene una frazione molto esigua delle vulnerabilità note: solo lo 0.5% di tutte le vulnerabilità pubblicate dal MITRE nella lista dei CVE;
- il numero di vulnerabilità individuate dal CISA è in continua crescita;
- il KEV è in generale più critico in termini di pericolosità rispetto al CVSS: circa il 33% delle vulnerabilità del KEV è classificato come critico mentre solo il 15% di tutte le vulnerabilità tracciate nel CVE sono classificate con il massimo livello di severità;

[1] https://www.cyentia.com/prioritization-to-prediction-v9/

- pressoché tutte le organizzazioni (98.3%) sono state impattate da almeno una delle vulnerabilità presente nel KEV;
- il KEV offre buone informazioni in merito all'exploitation di una CVE ma non può essere considerato esaustivo: il 94% delle CVE che presentano una "exploitation activity" non sono contenute nel KEV.

Il Catalogo KEV

Il Catalogo KEV è stato pubblicato dal CISA, la prima volta, il 3 Novembre, 2021 contestualmente alla "Binding Operational Directive 22-01" emessa dal Department of Homeland Security degli Stati Uniti d'America.
Il catalogo nasce con l'obiettivo di indicare "esplicitamente" a tutte le agenzie federali americane le vulnerabilità più pericolose e quindi da prioritizzare nel processo di remediation ed i tempi massimi per mettere in sicurezza i sistemi affetti.
Il CISA include una data vulnerabilità all'interno del catalogo KEV seguendo un processo che si basa su tre criteri:

1. La vulnerabilità deve avere ottenuto dal MITRE un "Common Vulnerabilities and Exposures (CVE) ID", e tale CVE ID deve essere pubblico (non riservato). Questo al fine di poter mettere in correlazione i due sistemi di catalogazione.
2. Deve esistere l'evidenza di tentativi di "active exploitation" indipendentemente dal fatto che siano essi andati a buon fine o no.
3. Deve essere stata rilasciata una procedura chiara e definita per effettuare la remediation del sistema affetto dalla vulnerabilità.

Oltre a ciò, come già accennato, il CISA considera importante i tempi entro i quali è necessario effettuare le azioni di remediation e la disponibilità delle precise azioni da intraprendere per gestire la vulnerabilità. Considera, quindi, rischiosa la pubblicazione di informazioni su exploit "efficaci" se non si dispone di alcuna possibilità di contrastarli.

Nel suo giorno di prima pubblicazione, il catalogo KEV conteneva 287 CVE presenti nell'hardware o software di 84 produttori; da allora le sue dimensioni si sono più che triplicate, raggiungendo, il 1° luglio 2023, le 965 vulnerabilità in prodotti di 199 vendor.
Ciò potrebbe far pensare ad una crescita lineare del catalogo con l'aggiunta di 34 CVE per mese e quindi circa una al giorno, ma in realtà le cose non sono andate proprio così. Con riferimento alla Figura 1, si nota che le CVE sono state aggiunte al catalogo KVE a blocchi e in periodi diversi inframezzati da periodi lunghi anche 26 giorni senza aggiunte, seguiti poi da rilasci consistenti anche di 95 CVE in un solo giorno (Figura 1).

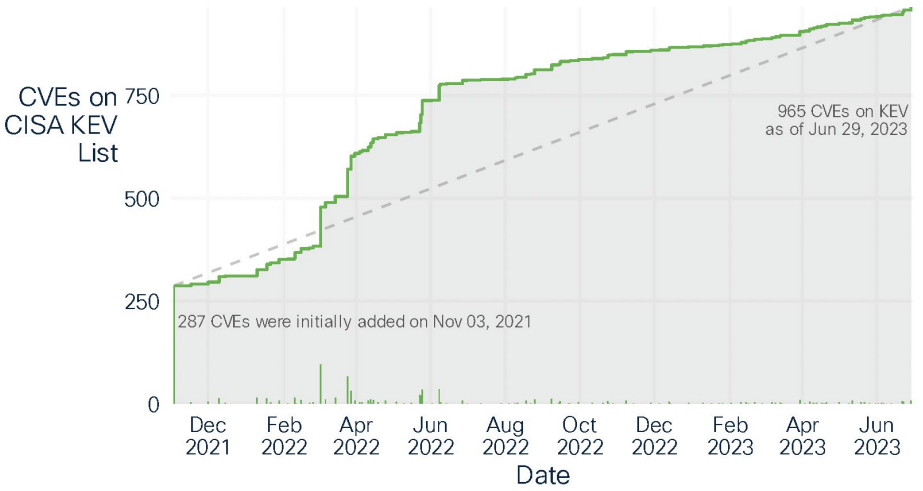


Figura 1: *Crescita del Catalogo KVE negli anni*

Si può poi notare come, in poco più di un anno, da dicembre 2021 a dicembre 2023 la lista delle KEV sia pressoché triplicata, passando da 250 a 750 CVE, il che potrebbe apparire preoccupante, ma vale la pena sottolineare che a giugno 2023 le 965 vulnerabilità individuate erano solo pari a circa lo 0.5% delle oltre 200 mila CVE pubblicate dal MITRE.
Questo dato potrebbe essere visto allora come un fattore positivo: dopo tutto, se dovessimo preoccuparci esclusivamente di una CVE su 200, lo stesso incremento di 3 volte in un anno non apparirebbe significativo.
Per trovare una chiave di lettura corretta va sottolineato che il CISA sostiene di avere evidenza che tali vulnerabilità siano di fatto soggette ad "active exploitation", ma non dice da nessuna parte che queste siano le "uniche" vulnerabilità sotto attacco.

Confronto KEV - Cyentia Exploit Intelligence Service

Per capire il valore e la rappresentatività del catalogo KVE, correliamo allora i dati del CISA con quelli di altre ricerche e fonti usate da soluzioni commerciali in ambito Risk-Based Vulnerability Management, in particolare con quelli del "Cyentia Exploit Intelligence Service", messi a paragone con i cataloghi CVE, KVE in **Figura 2**.

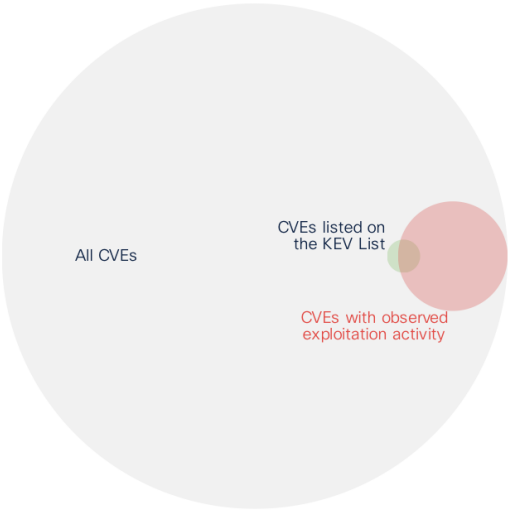


Figura 2: *Correlazione tra dati su Vulnerabilità note e Vulnerabilità sfruttate*

Il Cerchio rosa, relativo ai dati del Cyentia Institute, indica che secondo loro, circa il 5% di tutte le vulnerabilità pubblicate dal MITRE hanno una qualche forma di "exploitation activity". Il cerchio verde, 10 volte più piccolo, rappresenta il catalogo KEV, con appena lo 0.5% delle vulnerabilità CVE incluse.
La sovrapposizione tra i 2 dati interessa i 2/3 del catalogo KEV, cioè la maggioranza dei dati del KEV trova riscontro nei dati del Cyentia Institute, a riprova dell'affidabilità dei dati del CISA e del valore della "K" nell'acronimo KEV: ***In pratica, ciò significa che correggere o proteggere le vulnerabilità indicate nel catalogo KEV dovrebbe essere la priorità n. 1 per tutti.***
Ma che dire di quella vasta striscia di rosa dei dati del Cyentia Institute che non si sovrappone al KEV?
Secondo l'Istituto, circa il 94% delle vulnerabilità sfruttate non è presente nel catalogo del CISA.
Questa discrepanza è dovuta principalmente alle differenze nelle metodologie di raccolta dei dati. In particolare, il fatto che il catalogo KEV sia relativamente recente fa sì che esso dia un maggiore peso alle vulnerabilità più nuove. Di fatto, i dati del Cyentia Institute indicano che esistono molte vulnerabilità più vecchie, che sono tuttora oggetto di exploit attivo: queste ultime è meno probabile che compaiano nel KEV.

Il KEV si concentra su vulnerabilità che sono attivamente sfruttate in natura, ma vale la pena dare una rapida occhiata anche alla effettiva disponibilità di codice e procedure per l'exploit della vulnerabilità.

Questo è importante perché una ricerca precedente, sempre del Cyentia Institute, ha mostrato un **aumento di 15 volte dell'attività di sfruttamento per le vulnerabilità con codice exploit pubblico**.
La Figura 3 è simile alla precedente Figura 2, tranne che ora sovrappone ai tre dati precedenti i dati sulle CVE per le quali è pubblico il codice per l'exploit.

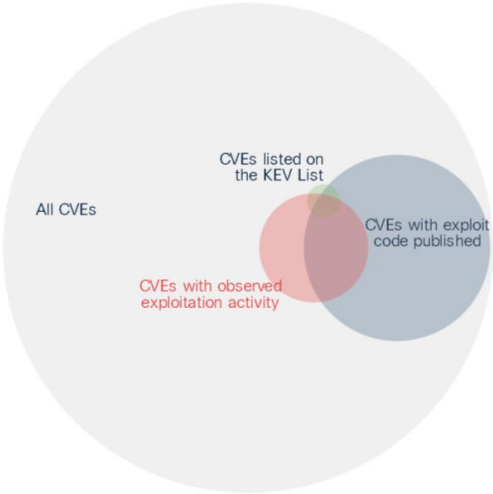


Figura 3: *Correlazione tra dati su vulnerabilità note e vulnerabilità sfruttate e presenza di codice*

Il 68% circa delle vulnerabilità' incluse nel catalogo KEV hanno a disposizione codici di exploit, il che testimonia quanto sopra affermato in termini di affidabilità del catalogo KEV. La cosa interessante è che il grande divario che abbiamo visto prima tra Cyentia Institute e KEV non è così pronunciato qui. Circa il 55% dei CVE per indicati dall'Istituto ha il codice dell'exploit disponibile pubblicamente. L'implicazione qui è che, indipendentemente da come viene misurato lo sfruttamento, la probabilità che esista un codice di exploit disponibile al pubblico è più o meno la stessa.
Quindi il KEV è un buon punto di partenza ma non può rappresentare il punto finale di una strategia di gestione delle vulnerabilità basata sul rischio.

Abbiamo ipotizzato che un limite del catalogo CISA KEV potrebbe essere quello della polarizzazione sull'età recente della vulnerabilità.

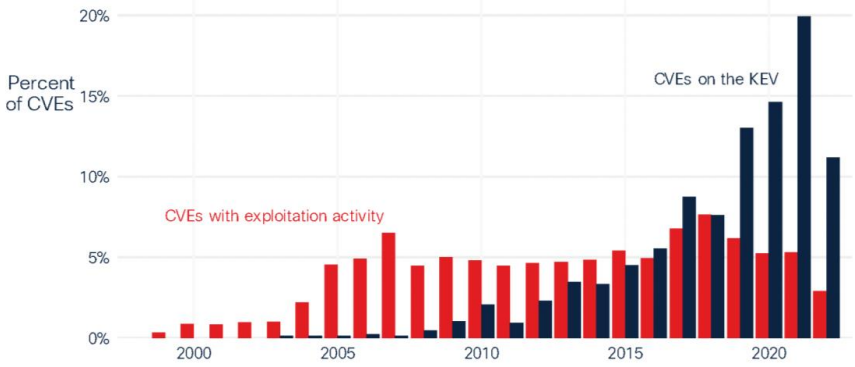


Figura 4: *Distribuzione delle CVEs per data di pubblicazione e con codice di sfruttamento*

La **Figura 4** mostra la distribuzione delle CVE **per data di pubblicazione**, rappresentando queste due serie:
- le vulnerabilità nel KEV (barre blu);
- le vulnerabilità per cui Cyentia Institute ha evidenza di exploit (barre rosse) avvenuti negli scorsi 90 giorni.

Il grafico mette in evidenza, quindi, come Il KEV sia sbilanciato verso le vulnerabilità più recenti, essendo solo il 5% note prima del 2012 e ben l'81% immediatamente antecedente la nascita del catalogo steso, e allo stesso tempo fornisce una distribuzione molto più uniforme di ciò che gli aggressori stanno utilizzando in questo momento. Sebbene alcuni dei CVE siano datati, e quindi teoricamente meno presenti in rete o risolvibili da tempo, sono semplicemente troppo buoni per essere ignorati dagli aggressori.

Conclusione: **il KEV è limitato per la sua polarizzazione sulle vulnerabilità più recenti. Se si dà priorità alle vulnerabilità basandosi solo sul catalogo KEV, si rischia di trascurare alcuni vecchi problemi che gli hacker considerano ancora vantaggiosi.**

Catalogo KEV e distribuzione per vendor

I processi di risoluzione e protezione delle vulnerabilità sono, solitamente "product-specific" e quindi importante analizzare il punto di vista del CISA KVE rispetto alla distribuzione per Produttore e ai dati sulle CVE realmente sfruttati a disposizione del Cyentia Institute.

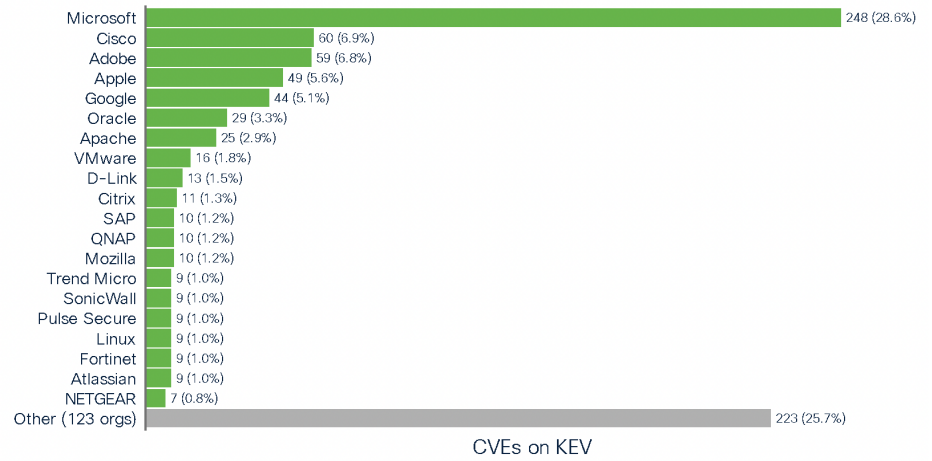


Figura 5: *Distribuzione percentuale delle vulnerabilità del catalogo KEV per produttore*

La **Figura 5** fornisce una ripartizione dei primi 20 fornitori presenti sul KEV (più un grosso gruppo di "altri produttori" con percentuali di sotto dello 0,8%.
Sembrerebbe, da una prima lettura veloce, che i prodotti Microsoft presentino più vulnerabilità sul KEV rispetto a qualsiasi altro fornitore. Ma, se leggiamo i dati in maniera più attenta, ciò non significa che i prodotti Microsoft siano intrinsecamente più vulnerabili di altri, ma significa che ci sono più exploit "noti" contro prodotti Microsoft, e questo è dovuto ai tantissimi prodotti Microsoft disponibili e al loro enorme numero di clienti e non ultimo, anche agli sforzi di Microsoft nel tracciare e segnalare gli exploit. Inoltre, i CVE di Microsoft rispondono bene al criterio adottato dal CISA di "includere solo i CVEs che abbiano a disposizione una patch o una procedura di remediation".
Considerata quindi questa importante presenza di Microsoft nel catalogo, vale la pena chiedersi se questa importanza sia sproporzionata se messa in relazione alla sua presenza tra tutti i CVE realmente sfruttati in base ai dati del Cyentia Institute.

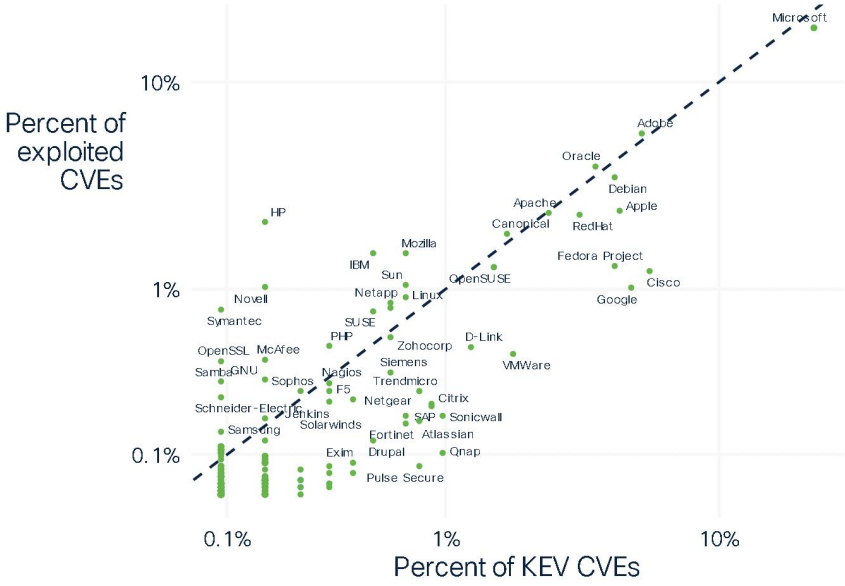


Figura 6: *Distribuzione CVE per vendor nel KEV rispetto alle CVE realmente sfruttate*

I fornitori sopra e a sinistra della diagonale hanno una proporzione inferiore di CVE sul KEV rispetto alla loro presenza nella popolazione generale di CVE sfruttati, mentre quelli sotto e a destra della diagonale sono sovrarappresentati sul KEV.
Quindi, Microsoft è in realtà un po' sovrarappresentata nel KEV: rappresenta il 22,2% del KEV ma è il 18,2% di tutti i CVE sfruttati. HP è un caso interessante in quanto rappresenta lo 0,1% dei CVE KEV ma il 2,1% di tutti i CVE sfruttati, ma tale dato potrebbe essere dovuto alla citata polarizzazione dei dati KEV. Anche Google, Cisco e Fedora pur essendo ai primi posti del KEV risultano sovrarappresentati. Probabilmente non esiste una stessa ragione per tutti e tre questi produttori, ma sicuramente la loro ampia presenza sul mercato potrebbe essere il motivo principale.
Conclusione: ***Alcuni fornitori sono sovrarappresentati nel catalogo KEV se si tiene conto del numero totale di vulnerabilità sfruttate.***

Proprietà delle vulnerabilità nel catalogo KEV

Andiamo ora ad analizzare le **proprietà** delle vulnerabilità, per scoprire se alcune caratteristiche aumentano o diminuiscono la probabilità che una certa vulnerabilità compaia nel catalogo KEV.
Occorre considerare che categorizzare e contestualizzare le vulnerabilità è impegnativo. Esistono molte fonti di dati diverse, molte delle quali hanno formati complessi e difficili da analizzare (ad esempio, le descrizioni in testo libero e la natura gerarchica dei CWE). Questi dati un po' confusi rendono difficile individuare quali caratteristiche possono influenzare la popolazione del catalogo KVE.
Considereremo comunque due proprietà ampiamente usate dai team di Security:
- il punteggio dato dal Common Vulnerability Scoring System (CVSS);
- il testo della descrizione della vulnerabilità.

Ricordiamo prima di tutto che il CVSS è il metodo per fornire un indice di severità di una vulnerabilità, gestito da Forum of Incident Response and Security Teams (FIRST), una no-profit americana, il cui scopo è fornire aiuto e strumenti ai gruppi di Incident response di tutto il mondo.
CVSS si ottiene componendo tre gruppi di parametri: Base, Temporali e Ambientali. Il gruppo Base considera le caratteristiche di una vulnerabilità che non cambiano con il tempo e con il contesto organizzativo, quali il vettore di attacco, la complessità, i privilegi richiesti, l'impatto sull'integrità. Il cosiddetto "CVSS score", che va da 0 a 10, si ricava principalmente da queste caratteristiche della metrica Base e rappresenta un indice di severità. Per fare un esempio, la presenza di un exploit kit facile da trovare e da usare tenderà a far aumentare il punteggio CVSS di una vulnerabilità, mentre la disponibilità di una patch ufficiale da parte del vendor tenderà a farlo scendere.
I parametri temporali sono quelli che cambiano nel tempo a causa delle attività degli attaccanti nel produrre codici di exploit e dei produttori nello sviluppare patch software.
Le metriche ambientali si applicano all'ambiente specifico, e tengo in conto, ad esempio, gli aspetti di confidenzialità in cui esiste una vulnerabilità. Questi parametri modificano la metrica base e sono, per definizione, specifici per ciascuna impresa.

L'analisi del Cyentia Institute, considera CVSS versione 3 e i risultati sono riassunti in **figura 7** dove sono messi a confronto tre diagrammi a barre:
- Il primo (Everything) è relativo alla distribuzione complessiva del punteggio CVSS (in ascissa), tra tutte le vulnerabilità CVE.
- Il secondo (Exploited) considera la distribuzione dei CVSS per le solo vulnerabilità che sappiamo essere oggetto di exploit in campo.
- Il terzo (KEV) illustra la distribuzione dei CVSS solo per le vulnerabilità presenti nel catalogo KEV.

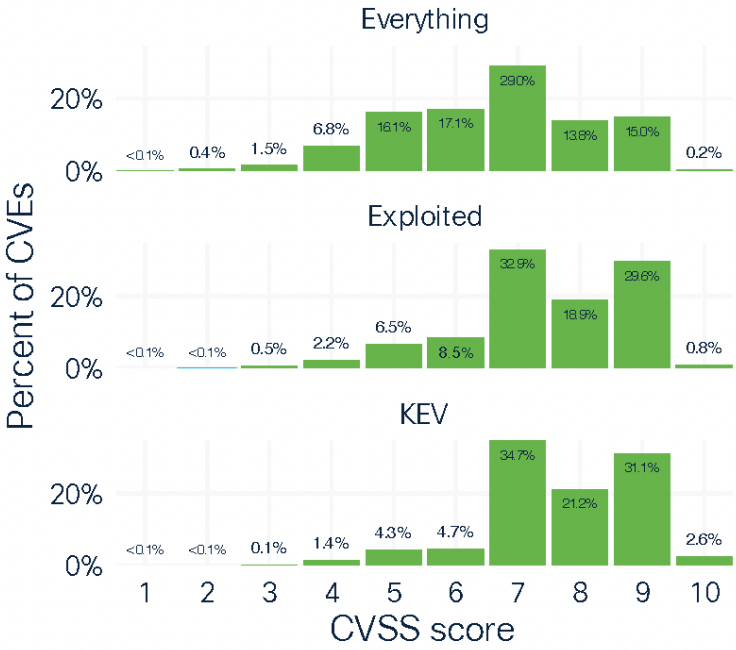


Figura 7: *Distribuzione del CVSS per tutte le CVE, per quelle sfruttate e per quelle KEV*

Come vediamo, il secondo e il terzo grafico hanno una distribuzione molto simile, con un leggero spostamento della percentuali più numerose di CVE verso CVSS più alti, nel grafico relativo al KEV.
La conclusione, piuttosto ovvia, è che le vulnerabilità di cui si vedono exploit in campo hanno un punteggio CVSS più alto della media, e ancora leggermente più alto, nel caso di quelle nel catalogo KEV.
Questo ha perfettamente senso, dato che il punteggio CVSS indica quanto sia facile sfruttare una vulnerabilità in campo.

Nella prossima (e ultima) analisi, andiamo invece a considerare le **descrizioni** associate alle vulnerabilità CVE presenti nel catalogo KEV.
Per rendere lo studio più facilmente leggibile, il Cyentia Institute ha processato le stringhe delle descrizioni CVE con un sistema di analisi del linguaggio naturale (NLP), in modo da estrarre alcune parole chiave, come "SQL injection", "Denial of Service" e simili.
Il risultato è visualizzato nella figura 8 dove, ancora una volta, il confronto è tra quello che è presente nel KEV e quelle CVE che vengono viste dal Cyentia Institute come oggetto di exploit attivo.

La chiave per interpretare il grafico è:
- tutte le "parole chiave" che stanno **al di sopra della linea** tratteggiata sono "**sottorappresentate**" nel KEV;
- le parole chiave **al di sotto della linea** sono invece "**sovrarappresentate**".

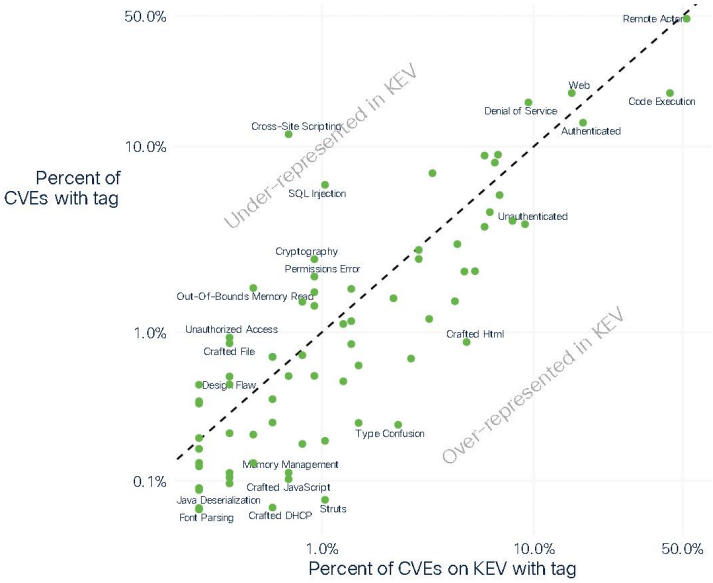


Figura 8: *Distribuzione parole chiave nel KEV rispetto a quella delle CVE sfruttate*

Notiamo che le caratteristiche di Cross-site scripting e SQL injection sono largamente sottorappresentate. Ciò probabilmente risale ai dati degli exploit, che potrebbero essere più inclini a rilevare gli aggressori utilizzando tecniche diffuse di "spray-and-pray" per identificare i sistemi vulnerabili. Le parole chiave "Unauthenticated" e "Authenticated" sono, invece, entrambe sovrarappresentate e ciò porta a riflettere sul fatto che queste espressioni possono essere utilizzate in due modi diversi nelle descrizioni: possono infatti sia indicare che l'aggressore deve essere autenticato o che la vulnerabilità consente all'aggressore di autenticarsi e la sovrarappresentazione indica che è più probabile questa seconda ipotesi.

Quindi, da tutto ciò si desume che ***sia le vulnerabilità sfruttate indicate dal Cyentia Institute che quelle presenti nel catalogo KEV hanno una gravità più elevata rispetto a quelle della popolazione generale delle vulnerabilità.***

Al di là dei grafici e dei confronti specifici, il messaggio chiave che deve rimanere di questa analisi è che il processo di gestione delle vulnerabilità, o meglio la decisione per la prioritizzazione del processo di patching e remediation, deve tener conto di molteplici aspetti, sia tecnici sia di impatto sul business e legati al rischio a cui sono esposti i sistemi e i dati. Affidarsi ad un unico parametro o punteggio, siano essi il CVSS o il KVE, è sicuramente riduttivo: il consiglio è di affidarsi a piattaforme dedicate di Vulnerability Management che sappiano correlare automaticamente dati provenienti da fonti "affidabili" diverse, inclusi i dati di threat intelligence raccolti per lo specifico contesto, e utilizzare algoritmi di data science comprovati per fornire un punteggio personalizzato leggibile anche dai consigli di amministrazione, oltre che dai team di sicurezza.

Next Generation Security Operation Center

[A cura di Aldo Di Mattia, Fortinet]

La crescente adozione di ambienti Cloud ed Ibridi, insieme alla conseguente evanescenza del tradizionale perimetro di sicurezza, hanno generato un panorama delle minacce più complesso ed esteso, incrementando di molto la superficie esposta ad attacchi. Gli analisti di sicurezza faticano a tenere il passo, mentre le stesse aziende lottano con una sempre crescente carenza di personale qualificato.
In questo scenario il tempo impiegato per identificare i possibili incidenti di sicurezza è cresciuto considerevolmente, andando a gravare soprattutto sull'efficacia dell'ecosistema SOC. Anche i dati degli ultimi due anni, infatti, riportano quest'andamento, tant'è vero che gli analisti di sicurezza stimano di dedicare più della metà del loro tempo ad indagare su incidenti che spesso si rivelano falsi positivi o, nel migliore dei casi, eventi a bassa priorità. Inoltre, l'approccio attuale delle Security Operations (SecOps) non sempre riesce a fornire adeguato supporto agli Analisti: c'è costantemente la tendenza a concentrarsi sulla tecnologia a discapito di quello che dovrebbe essere l'elemento umano nella Cybersecurity. Questo paradigma ha portato alla progettazione di SOC costituiti da decine di strumenti, il più delle volte non integrati, che nella quotidianità rappresentano "silos" estremamente dispendiosi da governare sia in termini di tempo che di risorse.
Per poter risolvere un problema, è fondamentale identificarne le cause. I dati riportano le cinque maggiori criticità che un SOC si trova ad affrontare oggi:

1. **Scarsa visibilità**: secondo gli analisti di mercato, due organizzazioni su tre dichiarano che la loro superficie di attacco si è ampliata considerevolmente nell'ultimo anno. La mancanza di visibilità crea inevitabilmente punti ciechi che diventano il bersaglio primario degli attaccanti.
2. **Strumenti non integrati**: sebbene nell'ultimo quinquennio si è discusso molto in merito ai vantaggi derivanti dal consolidamento dei vendor e degli strumenti a disposizione del SOC, tuttavia, le stime ci dicono che, ad oggi, la maggior parte delle aziende utilizza almeno dieci soluzioni diverse, non integrate, al servizio del proprio SOC Team.
3. **Tenere il passo con gli attaccanti**: troppe organizzazioni basano ancora il ciclo di vita del proprio SOC su metodi di rilevamento manuali, spesso obsoleti ed inefficienti, a completo vantaggio degli aggressori. In effetti, il numero di analisti disponibili raramente è sufficiente a gestire il volume di alert di cui sono quotidianamente gravati; acquisire, in maniera agile ed efficiente, le competenze necessarie per utilizzare in modo efficace decine di sofisticati strumenti è estremamente complesso. Il quadro viene ulteriormente complicato dall'elevato turn-over che affligge il comparto della Cybersecurity, principalmente in ambito SOC.

4. **Sovraccarico di informazioni**: la già citata espansione della superficie di attacco implica un esponenziale incremento nel volume degli avvisi di sicurezza. Dal punto di vista dell'analista, una singola rilevazione potrebbe generare decine di avvisi che richiedono un'indagine manuale. Questo lento processo avvantaggia l'attaccante, che ha più tempo per causare danni prima di essere eventualmente rilevato all'interno della rete.
5. **Perdita del focus**: l'elevato numero di alert, molte volte di diversa tipologia, provenienti pure da sistemi differenti, potrebbe comportare che determinati eventi o vulnerabilità possano essere gestiti con minore o errata priorità, se non addirittura trascurati.

L'evoluzione del SOC dovrebbe quindi essere strutturata intervenendo principalmente in tre aree operative

- **Consolidamento dei flussi di lavoro**: un flusso di lavoro unificato implica un consolidamento degli strumenti a disposizione del SOC ed una integrazione reale delle varie tecnologie. In sostanza lo scopo è non solo quello di avere una correlazione tra eventi provenienti da diverse fonti, ma anche di produrre un contesto nel quale inquadrarli in modo da velocizzare in maniera significativa il lavoro dell'analista. Ridurre il numero dei vendor sfruttando un ecosistema di strumenti nativamente connessi è quanto la maggioranza delle aziende di analisi e consulenza suggeriscono oggi in tema evolutivo.
- **Machine Learning/Intelligenza Artificiale**: l'adozione di strumenti di sicurezza basati su ML/AI contribuisce a rendere molto più efficace l'attività del SOC, intervenendo principalmente nella riduzione di attività manuali e ripetitive. Alcuni dei vantaggi di tale tecnologia includono l'automazione della raccolta di informazioni, l'approfondimento sugli eventi con informazioni sulle minacce, la creazione di sequenze temporali o rendering grafico delle stesse, la mappatura dei TTP MITRE o la raccomandazione di risposte. Con l'automazione basata su AI/ML, gli analisti possono lavorare su un incidente in modo esponenzialmente più veloce, a tutto vantaggio dell'efficienza e dei tempi di Detection/Remediation (MTTD/MTTR).
- **Utilizzare framework di mercato e fonti esterne di intelligence**: gli strumenti di carattere open source consentono di utilizzare contenuti e procedure consolidate senza dover necessariamente reinventare la ruota ogni giorno. Un esempio tra tanti sono le Sigma Rules, uno standard di rilevamento aperto che può essere adottato per l'implementazione ed il tuning dei processi di detection e automation del SOC. Le fonti di threat intelligence, inoltre, forniscono in tempo reale preziose informazioni in merito a quanto sta accadendo a livello globale in termini di minacce, reputazioni e contenuti.

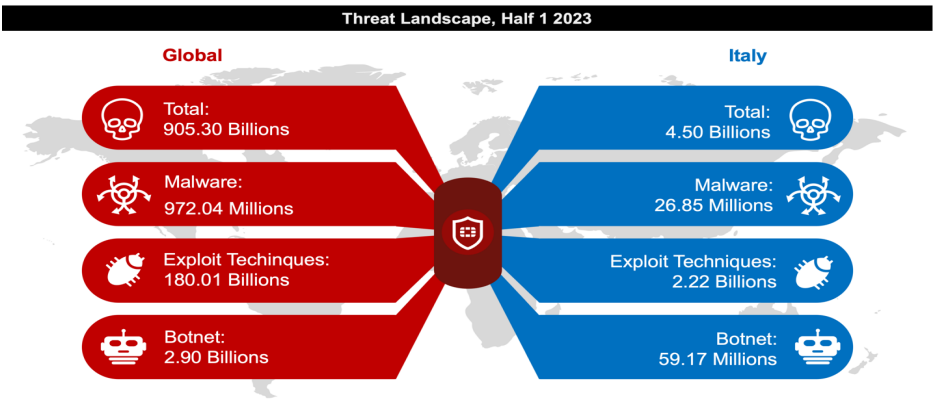
L'utilizzo di un approccio unificato per il proprio SOC rende molto più efficiente il lavoro degli analisti, contribuendo a ridurre significativamente i tempi di indagine e di risposta.
Un SOC "unificato" o **Cyber Fusion Center** (CFC), si basa su automazione, orchestrazione ed integrazione delle informazioni interne (CyberSec, IT, OT, NOC).

Naturalmente il SIEM, pur essendo un elemento chiave di ogni SOC, non è in grado di sopperire a tutte le funzioni proprie di un CFC. Al SIEM, infatti, dovrebbero essere integrate altre tecnologie a supporto, tra le quali il SOAR (Security Orchestration Automation and Response), i sistemi di Deception, le fonti di threat intelligence e gli strumenti di nuova generazione specifici per contesto, come endpoint (EDR/XDR) e rete (NDR). Ridurre al minimo i falsi positivi fornendo allo stesso tempo un contesto sufficiente per le indagini è fondamentale per ottenere risultati concreti ed evidenti.
Realizzare un SOC, o trasformarlo in un CFC, rappresenta sicuramente un investimento importante, molto spesso fuori dalla portata di realtà di dimensioni più piccole, ma non meno vulnerabili. In tal caso, servizi gestiti di Cybersecurity come il "SOC as a Service", servizi di Incident Response e servizi di Analisi di sicurezza (Exposed Surface Recon) possono essere la soluzione giusta in termini di investimento e mitigazione del rischio.

Analisi delle minacce del primo semestre 2023

Analizzando i dati estratti dai FortiGuard Labs si evince che, in termini percentuali, l'Italia è stata impattata dallo 0,5% circa delle minacce totali. Esaminando le minacce specifiche, rispetto ai dati globali, in Italia sono state riscontrate le seguenti percentuali:

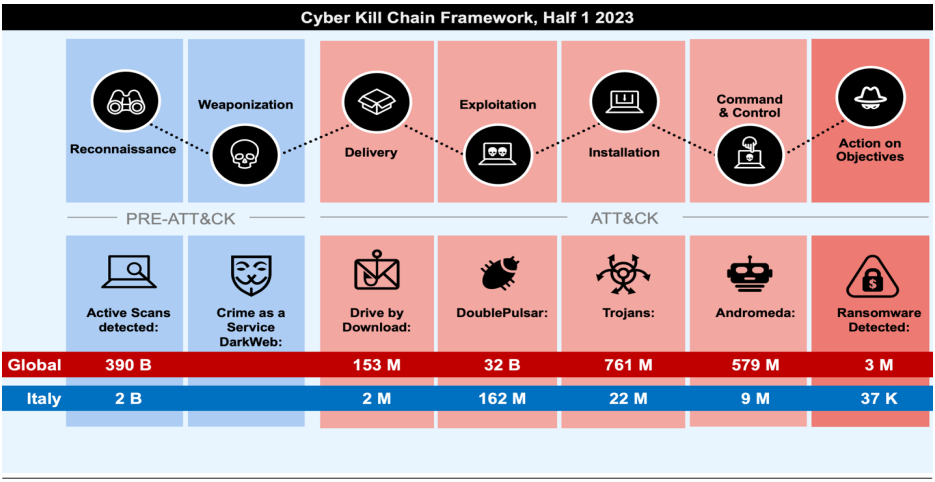
- 2,8% dei malware.
- 1,2% dei tentativi di exploit.
- 2% delle botnet.



Threat Landscape, Half 1 2023, Global & Italy

Strutturando i dati di minaccia rilevati da FortiGuard Labs, sia globali che Italiani, su matrice Cyber Kill Chain (CKC), possiamo evincere, ad esempio, quanto siano significativi i volumi relativi ai momenti "esecutivi" degli attacchi, ovvero Exploitation, Installation e

Command & Control rispetto alle rilevazioni di Reconnaissance iniziale.
Il dato italiano mostrato nell'immagine seguente, pur essendo sostanzialmente in linea con i volumi globali, mostra uno sbilanciamento importante per quanto concerne il rapporto tra il numero totale di eventi di Reconnaissance e quelli di Installation ovvero il momento effettivo di attivazione del malware: a fronte di un rapporto globale dello 0,19 % sul totale degli eventi di Reconnaissance, il dato italiano mostra un volume del'1,1 %, ovvero un valore maggiore di oltre cinque volte (+579 %). La realtà dietro questi numeri è rappresentata principalmente dalla difficoltà di rilevare in tempo utile le minacce, a causa di quanto già indicato, aumento della superficie di attacco e conseguente ampliamento del perimetro di sicurezza tradizionale. Sempre più attacchi vengono infatti rilevati solo in fase avanzata, ovvero nel quadrante destro della CKC.
Strumenti funzionali ad una identificazione precoce, estesa ed accurata delle minacce, in altre parole quanto rappresentato nel quadrante sinistro della Cyber Kill Chain, diventano estremamente efficaci quando affiancati a sistemi e processi SOC "machine speed", governati da modelli altamente automatizzati, ad alta integrazione, e gestiti mediante una orchestrazione "Silos Free".

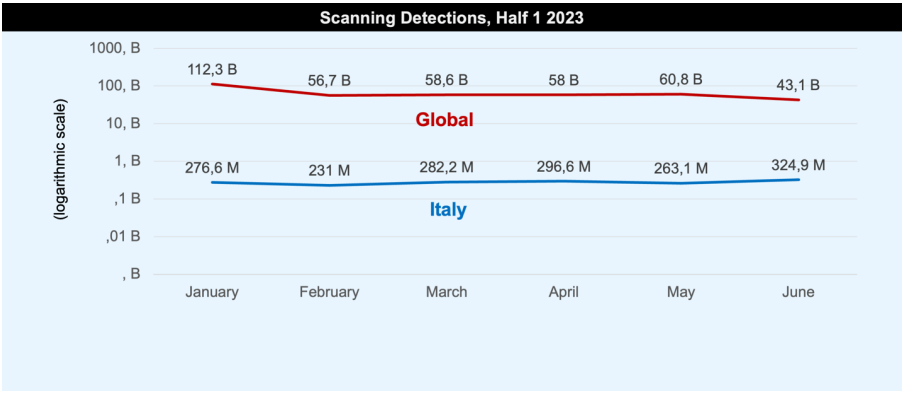


Cyber Kill Chain Framework, Half 1 2023, Global & Italy

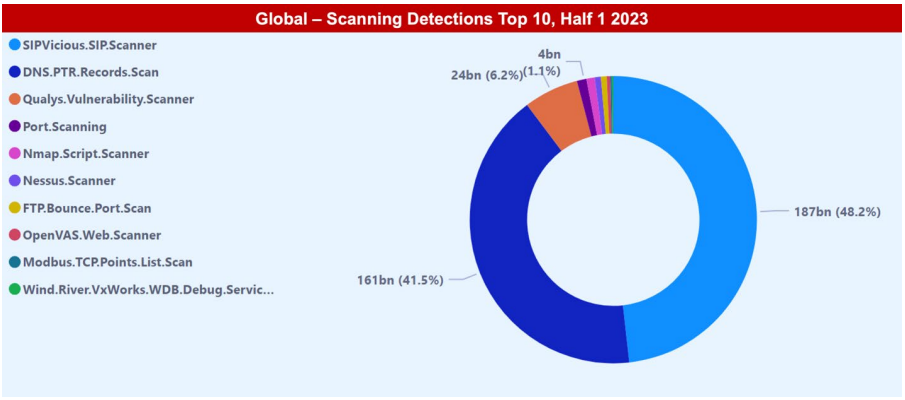
Per completezza, di seguito vengono riportati i dati globali e italiani, estratti dai FortiGuards labs, relativi al primo semestre del 2023 rispettivamente su:

- Scanning Detections;
- Malware Detections;
- Exploitations Attempts;
- Brute Force Attacks.

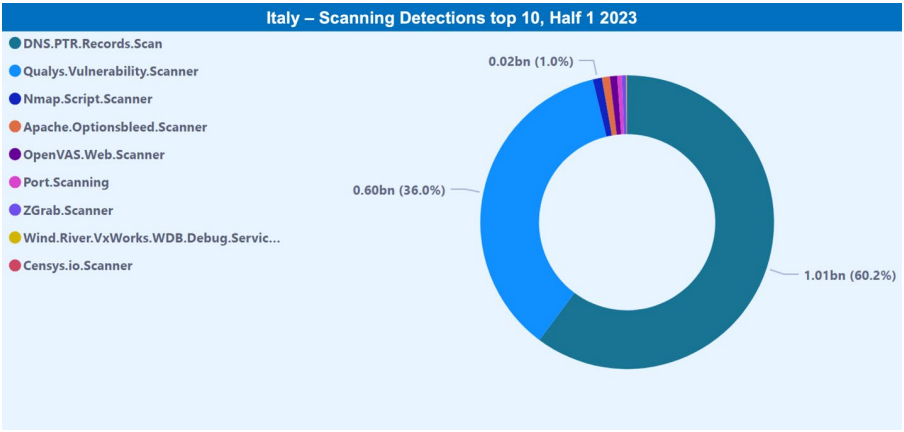
Nei grafici seguenti che mettono a confronto i dati globali con quelli italiani è stato necessario adottare una scala logaritmica per evidenziare l'andamento nazionale. I dati in alcuni casi sono espressi con l'abbreviazione angloamericana, bn/B = miliardi, M = milioni, K = migliaia.
Tutti i dati indicati sono stati estratti dai FortiGuard Labs, l'organizzazione Fortinet globale di threat intelligence e di ricerca sulle minacce. I FortiGuard Labs monitorano la superficie di attacco mondiale e utilizzano l'intelligenza artificiale per estrarre opportunamente i dati. Nei seguenti grafici è possibile vedere il nome delle minacce individuate da Fortinet; sul sito web https://www.fortiguard.com, nel campo di ricerca "search threats advisories", può essere inserito il nome delle firme mostrate così da avere tutti i dettagli, aggiornati in tempo reale.



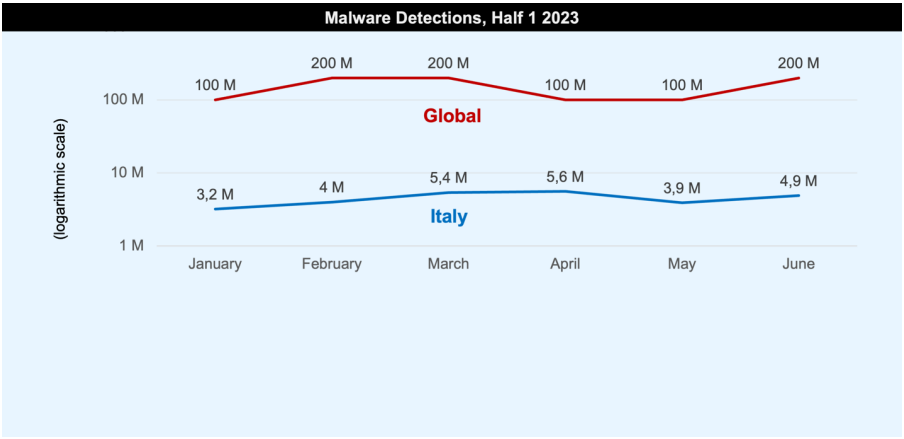
Scanning Detections, half 1 2023, Global & Italy



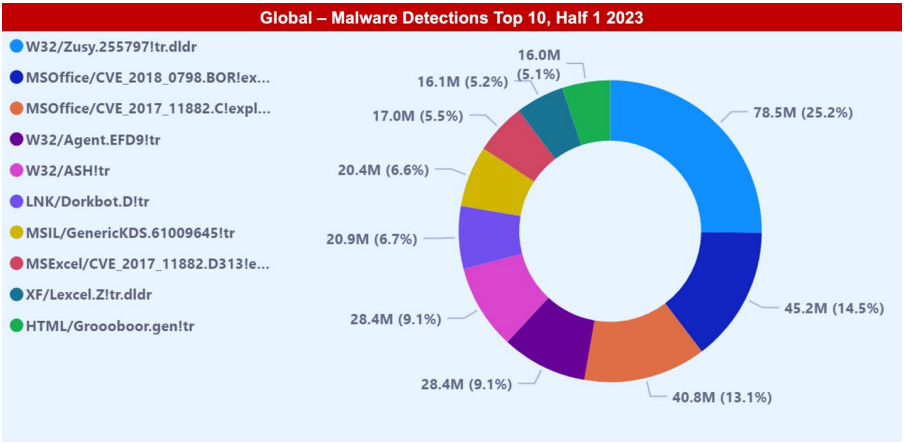
Scanning Detections top 10, half 1 2023, Global



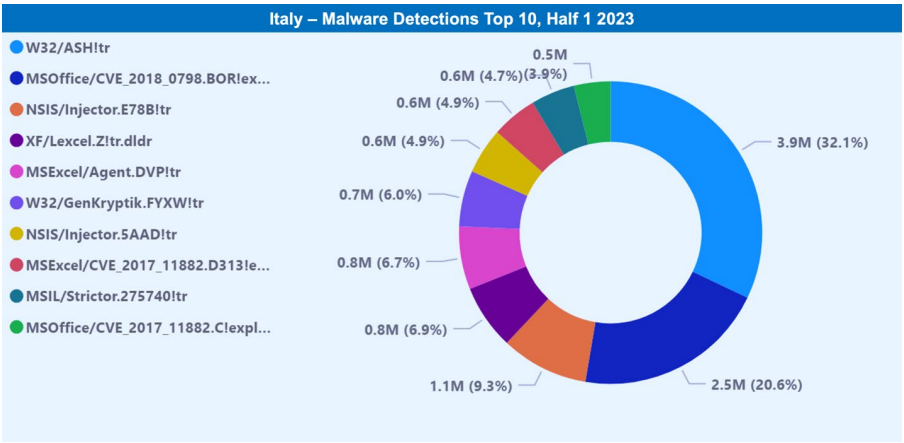
Scanning Detections top 10, half 1 2023, Italy



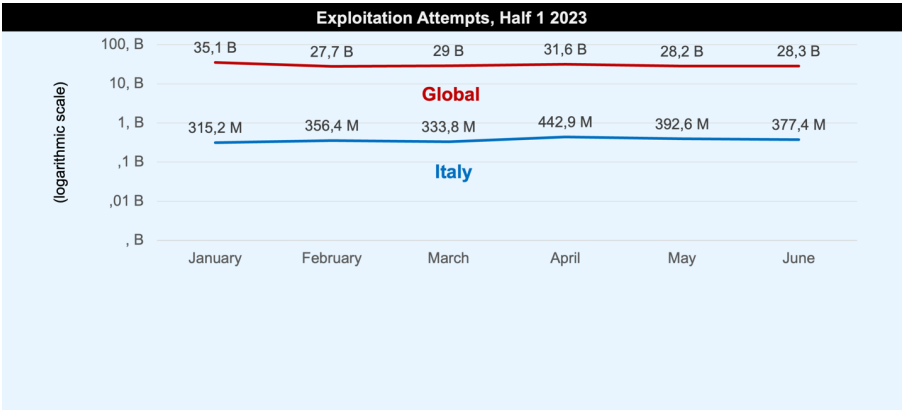
Malware Detections, half 1 2023, Global & Italy



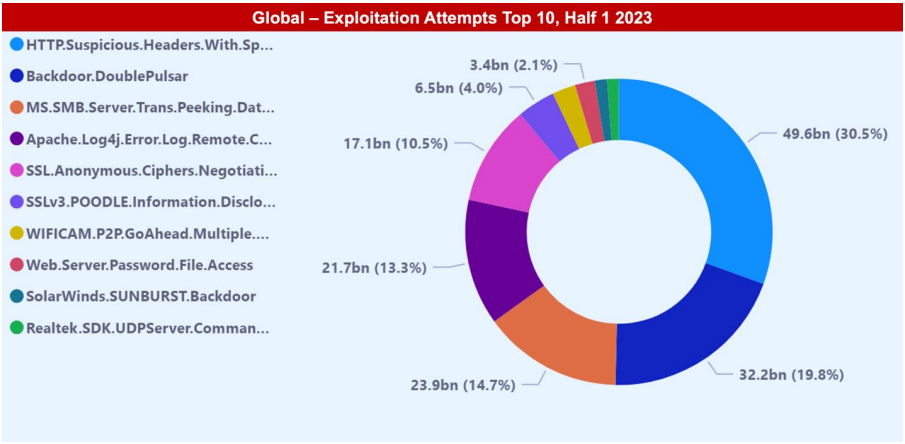
Malware Detections Top 10, half 1 2023, Global



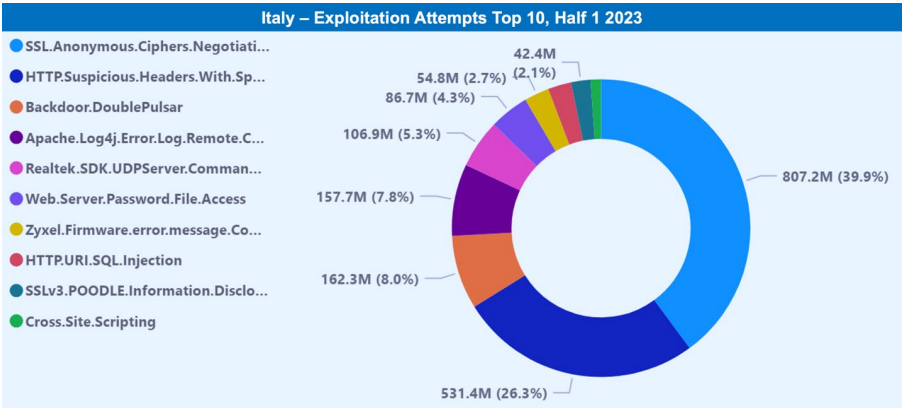
Malware Detections Top 10, half 1 2023, Italy



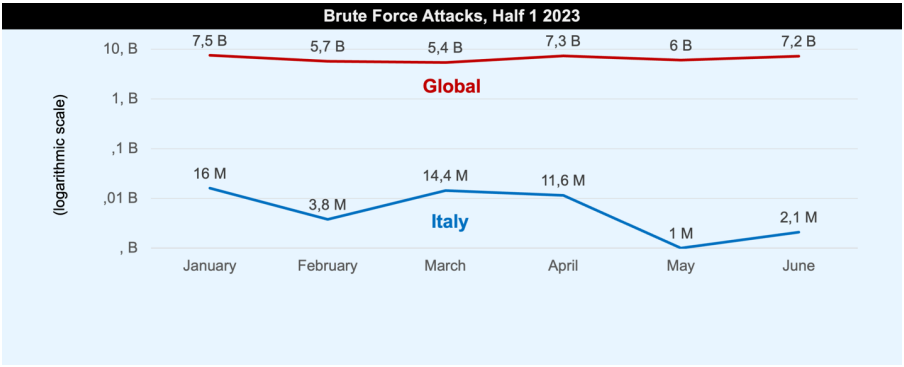
Exploitation Attempts, half 1 2023, Global & Italy



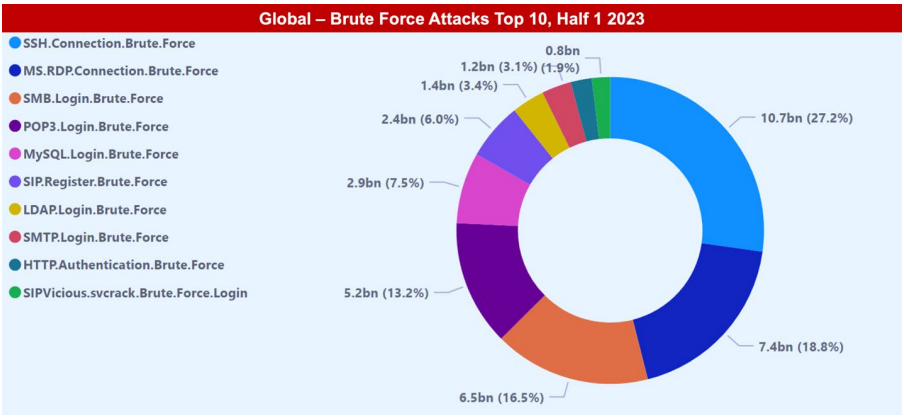
Exploitation Attempts Top 10, half 1 2023, Global



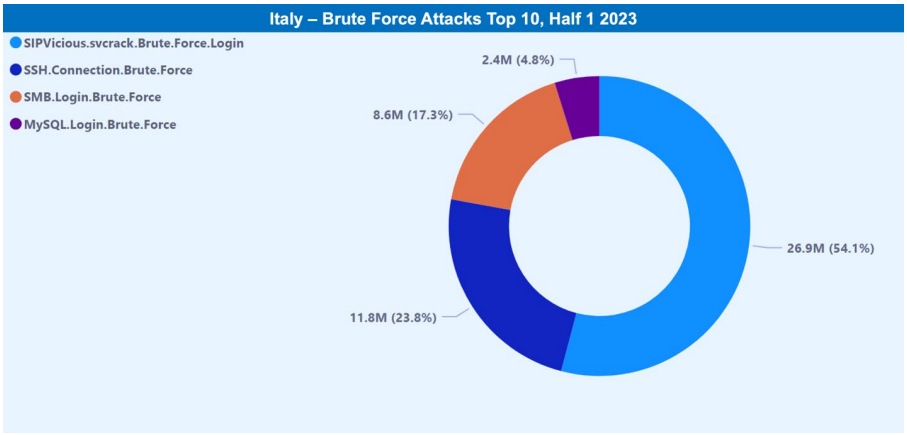
Exploitation Attempts Top 10, half 1 2023, Italy



Brute Force Attacks, half 1 2023, Global & Italy

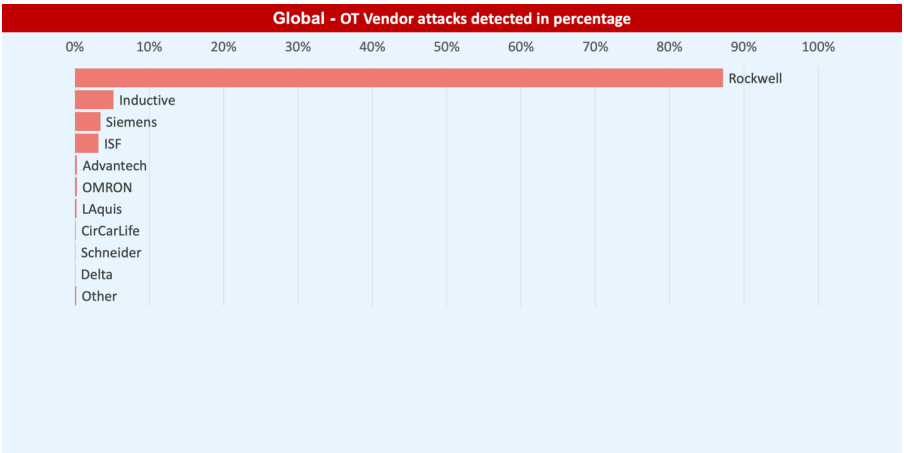


Brute Force Attacks Top 10, half 1 2023, Global

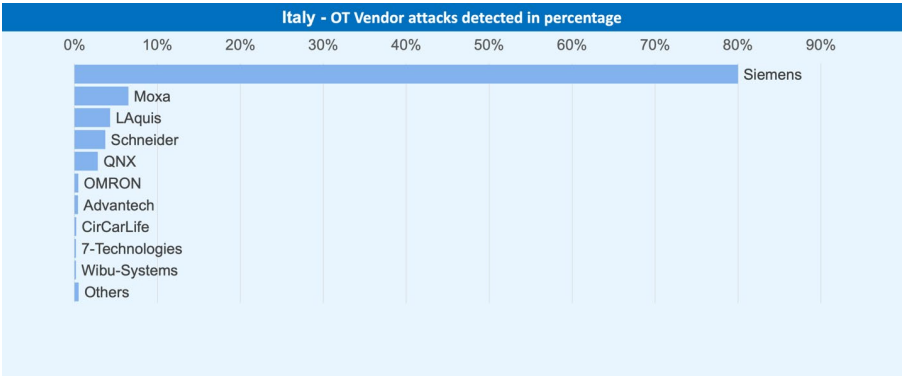


Brute Force Attacks Top 10, half 1 2023, Italy

Infine, di seguito vengono riportati in termini percentuali gli attacchi OT individuati verso specifici vendor di soluzioni di Operation Technology. I dati mostrano le individuazioni globali e italiane, e sono relativi all'ultimo periodo di osservazione della prima metà del 2023.



OT Vendor attacks detected in percentage, Late Half 1 2023, Global



OT Vendor attacks detected in percentage, Late Half 1 2023, Italy

Alcuni di questi attacchi possono essere associati a CVE (Common Vulnerabilities and Exposures), di seguito, le tre più individuate a livello globale sono state:

1. **CVE-2016-5645, Rockwell**: remote attackers can load arbitrary firmware updates.
2. **CVE-2011-4531, Siemens**: remote attackers can cause a Denial of Service.
3. **CVE-2022-35871, Inductive Automation**: an attacker can execute code in the context of system.

Mentre in Italia sono state:

1. **CVE-2016-9361, Moxa**: administration passwords can be retried without authenticating.
2. **CVE-2018-18990, LAquis**: attacker can disclose sensitive information under web server context.
3. **CVE-2011-4859, Schneider**: remote attackers to obtain access via telnet, windriver debug or ftp.

È singolare notare come, nella maggior parte dei casi, si tratti di vulnerabilità individuate più di 5/10 anni fa. Quindici, tra le prima venti CVE italiane riscontrate, sono state datate tra il 2011 e il 2019.

La numerosità e la complessità degli attacchi mostrati comprova come sia difficile oggi poter rendere sicuro il proprio processo di digitalizzazione o evoluzione digitale. Nessuna azienda può permettersi un SOC, o CFC, che non sia state of art. Si può scegliere di costruirne uno a regola d'arte oppure prenderne uno a servizio. Il fallimento della sicurezza implica sempre più il fallimento del servizio offerto, che nelle aziende private si traduce in un impatto significativo del business, mentre nelle PA si tramuta in interruzione di pubblico servizio.

Analisi di oltre un anno di conflitto russo ucraino tra guerra convenzionale, cyber war e tecnologie avanzate

[A cura di Carlo Mauceli, Microsoft]

Quando la guerra non è solo un affare tra gli Stati belligeranti

Negli ultimi anni l'attenzione nei confronti degli attacchi informatici è cresciuta tanto nei mass media e nell'opinione pubblica quanto nelle istituzioni. Ovunque, però, traspare un'evidente incertezza nella definizione di queste operazioni, troppo spesso erroneamente ricondotte all'espressione *cyber war*. Questa semplificazione genera il convincimento che *lo spazio informatico sia un luogo privo di regole* in cui tutto può succedere così da generare una retorica di tipo allarmistico che giustifica l'istituzione di numerosi enti preposti a garantire la sicurezza informatica. Non a caso si parla, a mio modo di vedere, in modo errato di sicurezza informatica di uno Stato pur consapevoli del fatto che lo Stato è un'entità astratta. Al contrario, è necessario stimolare una maggiore conoscenza del fenomeno così che si possano definire le aree attraverso cui catalogare le diverse operazioni informatiche (cyber war, cyber crime, info war, ecc.). In questa prospettiva, il diritto internazionale che disciplina l'utilizzo della forza nella comunità internazionale o jus ad bellum (contenuto nella Carta delle Nazioni Unite[1] e nel diritto consuetudinario) aiuta a comprendere cosa è realmente una cyber war, chi sono i suoi attori, se è mai esistita e quali sarebbero le conseguenze e le peculiarità ad essa connesse. Sulla base di ciò, *possiamo affermare che le operazioni illecite condotte nell'arena informatica sono riconducibili a due realtà ben distinte*: si tratta del cosiddetto *cyber crime*, di cui il rapporto si occupa ampiamente, e della nuova dimensione di conflitto internazionale: la *cyber war*.

Tra questi due "mondi" sono individuabili anche fenomeni empirici distinti, come quelli della info war o del cyber terrorismo[2], che, però, non trovano una specifica autonomia né una precisa collocazione, potendo rientrare, a seconda dei casi e dei soggetti, nell'una o nell'altra disciplina.

Nelle loro definizioni più banali:

- la guerra cibernetica è un conflitto tra soggetti di diritto internazionale condotto tramite operazioni informatiche;
- il cyber terrorismo è un atto di terrorismo in genere, eseguito da un attore non statale;
- l'info war è l'atto di raccogliere informazioni tramite sistemi informatici da parte delle agenzie di sicurezza statali;
- il crimine informatico è un qualsiasi reato commesso utilizzando un computer.

[1] http://ospiti.peacelink.it/cd/docs/1105.pdf

[2] In questa tipologia potrebbe rientrare il collettivo hacker Anonymous, diventato famoso per aver organizzato proteste on-line, nonché veri e propri attacchi cibernetici nei confronti di strutture statali, in particolare contro lo Stato di Israele e, recentemente, molto attivo nel conflitto russo-ucraino.

Alla luce del mutato panorama geopolitico e di quanto sta accadendo nel conflitto russo ucraino possiamo parlare di guerra cibernetica e, dunque, analizzeremo come la tecnologia sia stata e continua ad essere di supporto alla guerra convenzionale utilizzando i dati che Microsoft ha fornito grazie alle analisi e alle indagini condotte.
Gli attacchi informatici sono diventati un elemento chiave della geopolitica, coinvolgendo attori statali e non statali. Gli attacchi agli impianti nucleari iraniani tramite un worm informatico chiamato Stuxnet più di un decennio fa hanno dimostrato come le capacità informatiche possano essere utilizzate per ottenere danni transfrontalieri e fisici. Come abbiamo visto più recentemente nel conflitto Russia-Ucraina, gli attacchi informatici possono precedere o accompagnare l'azione militare come parte della guerra ibrida, con obiettivi chiave che sono le infrastrutture o i servizi critici di un Paese. È difficile da credere, soprattutto per i non addetti ai lavori, ma è un dato di fatto che tutto ciò abbia avuto una ricaduta enorme anche e soprattutto sull'economia tanto che in caso di rischio politico esterno o interno imminente o in rapido aumento (come guerra, escalation del conflitto interno o rischio acuto e crescente per la stabilità istituzionale), società come S&P Global Ratings hanno abbassato il rating sovrano indicativo sulla base del rischio di evento, a seconda dell'entità prevista del conflitto e dell'effetto sulle caratteristiche creditizie del debito sovrano.[3]
Il conflitto russo-ucraino ci costringe a fare i conti con una guerra tradizionale, Stato contro Stato, anziché conflitti civili interni a un Paese, a cui si somma il fatto che siamo nel XXI secolo; una guerra tradizionale arricchita da tecnologie moderne.
La difesa cibernetica per uno Stato è oggi quanto mai importante. Il campo cibernetico ha infatti delle peculiarità di cui bisogna tenere conto.
Molto spesso si tende a sopravvalutarlo perché è un tema di moda e questo avviene soprattutto nell'Europa Occidentale dove si vive nel "lusso dell'inconsapevolezza" e si pensa che le guerre informatiche siano una specie di gioco al computer. La realtà, invece, come stiamo osservando, è molto diversa e la guerra in Ucraina è lì per ricordarcelo.
In un conflitto reale, la dimensione cibernetica è quella meno importante tra le dimensioni classiche militari, cioè terra, mare, aria e spazio. Finora non è stato ancora dimostrato che una guerra cibernetica possa aiutare a vincere in caso di conflitto. La guerra cyber ha però una caratteristica specifica che la rende molto importante: rende le difese rilevanti e friabili allo stesso tempo. Il campo militare cibernetico è quello in assoluto più livellante. In questo ambito, le differenze si assottigliano in modo pericoloso più che non in altre dimensioni. Se pensiamo alla distanza in termini di potenza tra Stati Uniti e Corea del Nord, ad esempio, in ambito cibernetico, questa è infinitamente minore che non in altri campi quali le dimensioni militari marittima, terrestre o spaziale. E questo vale per quasi tutti i soggetti nel pianeta: un livello ottimo di prestazioni cibernetiche è facilissimo da raggiungere da parte di Stati poco sofisticati dal punto di vista tecnologico.
Prima dell'invasione su vasta scala dell'Ucraina da parte della Russia il 24 febbraio 2022,

[3] https://d110erj175o600.cloudfront.net/wp-content/uploads/2022/10/31145231/RatingsDirect_CyberRiskInANewEraHowCyberRiskAffectsSovereigns_53138170_Oct-31-2022.pdf

molti osservatori si aspettavano che una guerra ibrida guidata dalla Russia, come quella osservata quando la Russia ha invaso il Donbass e annesso illegalmente la Crimea nel 2014, avrebbe comportato il matrimonio di armi informatiche, operazioni di influenza e forza militare affinché l'invasione avvenisse rapidamente. Ora, un anno e mezzo dopo la sua invasione su vasta scala, l'esercito russo ha effettivamente causato devastazione fisica in Ucraina, ma non ha raggiunto i suoi obiettivi, in parte perché le operazioni informatiche e di influenza sviluppate da parte di Mosca sono in gran parte fallite.
Gli attacchi informatici russi hanno avuto un andamento fluttuante dal punto di vista dell'intensità e sono stati, molto spesso, respinti. Molte delle campagne di propaganda sostenute dal Cremlino hanno avuto scarso impatto, rivelando i limiti dell'influenza russa quando si sono scontrati con una popolazione ucraina molto resiliente. I threat actor affiliati allo stato russo, tuttavia, non si sono scoraggiati e continuano a cercare strategie alternative all'interno e all'esterno dell'Ucraina. A partire da gennaio 2023, Microsoft ha osservato come le attività di minaccia informatica da parte dei gruppi affiliati alla Russia si siano adattate all'evoluzione degli scenari di guerra per aumentare la capacità distruttiva e di raccolta di informazioni sull'Ucraina e sulle risorse civili e militari dei suoi partner.

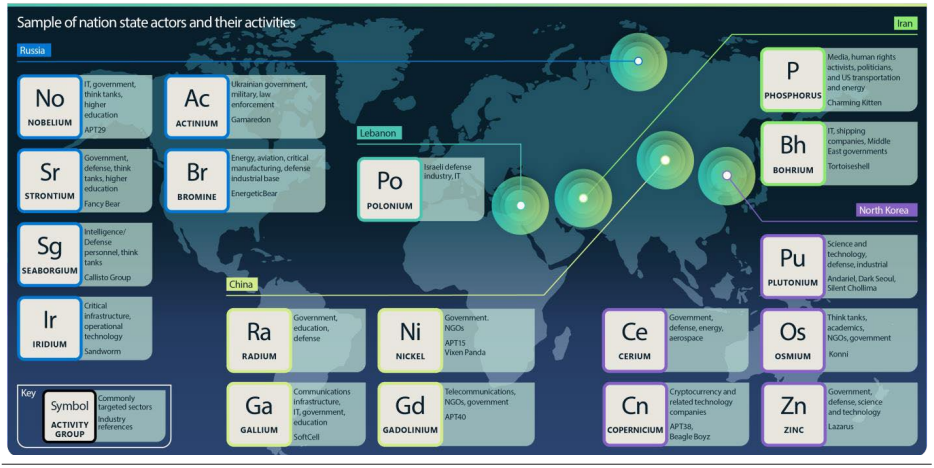


Figura 1: *Mappa dei Threat Actor statali secondo la terminologia Microsoft* [4]

IRIDIUM, noto anche come Sandworm, un threat actor attribuito all'agenzia di intelligence militare russa (GRU), ha svolto una fitta campagna distruttiva contro il governo ucraino e le organizzazioni dei media utilizzando malware quali **Foxblade** e **Caddywiper**.
A partire dalla fine del 2022, il Threat Actor avrebbe testato ulteriori funzionalità in stile ransomware che potrebbero essere utilizzate in ulteriori attacchi verso organizzazioni al di

[4] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us

fuori dell'Ucraina che svolgono funzioni chiave nelle linee di approvvigionamento e di supporto al Paese. L'operazione **ransomware Prestige** contro un'azienda polacca alla fine del 2022 fornisce un precedente per tali attacchi. Le analisi hanno rivelato che i threat actor con legami noti o sospetti con il GRU, l'intelligence estera russa (SVR) e i servizi di sicurezza federale russa (FSB) hanno tentato di ottenere l'accesso alle organizzazioni governative e legate alla difesa nell'Europa centrale e orientale e nelle Americhe.
Tra gennaio e metà febbraio 2023 sono state rilevate attività malevole di matrice russa contro organizzazioni in almeno 17 nazioni europee, con il settore governativo come focus primario. Queste azioni avevano come scopo la raccolta di informazioni delle organizzazioni che forniscono sostegno politico e materiale all'Ucraina.
A partire dal gennaio 2023, una campagna di propaganda russa ha preso di mira la diaspora ucraina nell'Unione europea (UE) e nel Regno Unito (Regno Unito) sostenendo che i rifugiati ucraini all'estero saranno estradati e arruolati con la forza nelle forze armate ucraine.
A metà febbraio, le autorità moldave e ucraine hanno reso pubblico un complotto russo per organizzare un colpo di stato. In quel periodo, il partito filorusso Shor della Moldavia ha organizzato proteste per fare pressione su Chișinău al fine di pagare le bollette energetiche invernali dei cittadini, in linea con gli sforzi del Cremlino di fare pressione sugli stati europei attraverso minacce di riduzione dell'approvvigionamento energetico.
All'inizio dell'anno, il gruppo di hacktivisti filorussi KillNet ha rivendicato attacchi mirati ai siti web del governo moldavo mentre diverse figure politiche moldave sono state bersaglio di una campagna di hack-and-leak amplificata dai media statali russi chiamata "Moldova Leaks".
Come sappiamo, la guerra, intanto, procede così come continuano le operazioni informatiche e di influenza della Russia rivolte all'Ucraina e ai suoi sostenitori ed è interessante notare come le attività informatiche precedano, quasi sempre, le attività belliche. Questa immagine evidenzia come quanto appena espresso sia avvenuto nell'ottobre del 2022.

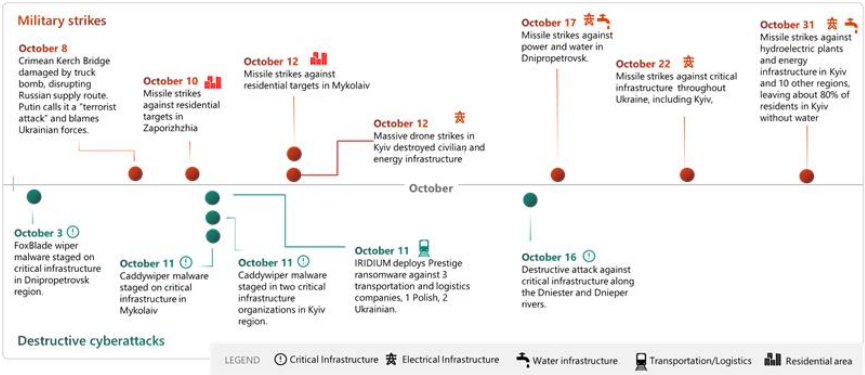


Figura 2: *Relazione tra attività cibernetiche e militari*

Dopo questa ampia panoramica che tra le altre cose mette in evidenza come il conflitto cibernetico si sia allargato a tutti i Paesi che sostengono l'Ucraina, possiamo riassumere questo primo anno e mezzo di conflitto in tre fasi:

- Fase 1 – Gennaio 2022 – Fine Marzo 2022, caratterizzata, in primis, dall'invasione dell'Ucraina da parte della Russia;
- Fase 2 – Fine Marzo 2022 – Settembre 2022, caratterizzata dal ritiro russo da Kiev per concentrarsi sul Donbas;
- Fase 3 – Settembre 2022 ad oggi, caratterizzata dalla reazione della Russia alla contro offensiva dell'Ucraina nelle zone orientali e meridionali.

Fase 1: Operazioni informatiche e di influenza parallele all'invasione militare

Gennaio 2022 – Fine Marzo 2022

I Threat Actor russi hanno concentrato gran parte della loro capacità operativa sul raggiungimento di una rapida vittoria in Ucraina, coerente con il convincimento da parte russa della propria forza militare. [5]

Nel gennaio 2022, l'attore militare russo DEV-0586 ha distribuito il malware WhisperGate contro alcune organizzazioni ucraine[6]. Da quel momento, i russi hanno impiegato almeno *nove nuove famiglie di malware e due tipi di ransomware* contro oltre 100 organizzazioni ucraine. Centinaia di sistemi in tutto il governo ucraino, infrastrutture critiche, media e settori commerciali sono stati colpiti da malware e ransomware che hanno provocato l'eliminazione di file e/o hanno reso le macchine inutilizzabili e la maggior parte di questi attacchi ha coinciso con l'invasione iniziale della Russia tra febbraio e marzo 2022.

La risposta attiva agli incidenti e la condivisione delle informazioni tra i difensori della rete ucraina e gli alleati hanno fatto sì che questa prima ondata di attacchi si interrompesse anche se gli attori in gioco hanno continuato ad operare al fine di studiare e realizzare nuove e diverse famiglie di malware, il che dimostra, se ce ne fosse stato bisogno, come l'industria del "malware" sia in continua evoluzione e, spesso, generi una capacità distruttiva sia di carattere proattivo che reattivo. Ciò a cui si è assistito, però, non è limitato solo alla sfera dei "ransomware" ma ha toccato anche l'ambito delle piattaforme dei social media che sono state inondate da una propaganda atta a tentare di disumanizzare gli ucraini chiedendone la "denazificazione" del paese e allargando il conflitto verso gli Stati Uniti, sostenendo che i bio laboratori americani stavano creando armi biologiche in Ucraina [7-8].

---

5 Russia_Military_Power_Report_2017.pdf (dia.mil); https://www.cna.org/reports/2021/10/russian-military-strategy-core-tenets-and-concepts, pg 3.

6 https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/ https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion

7 https://www.reuters.com/world/russia-demands-us-explain-biological-programme-ukraine-2022-03-09

8 https://www.nytimes.com/2022/03/17/world/europe/ukraine-putin-nazis.html; https://www.interfax.ru/russia/824200

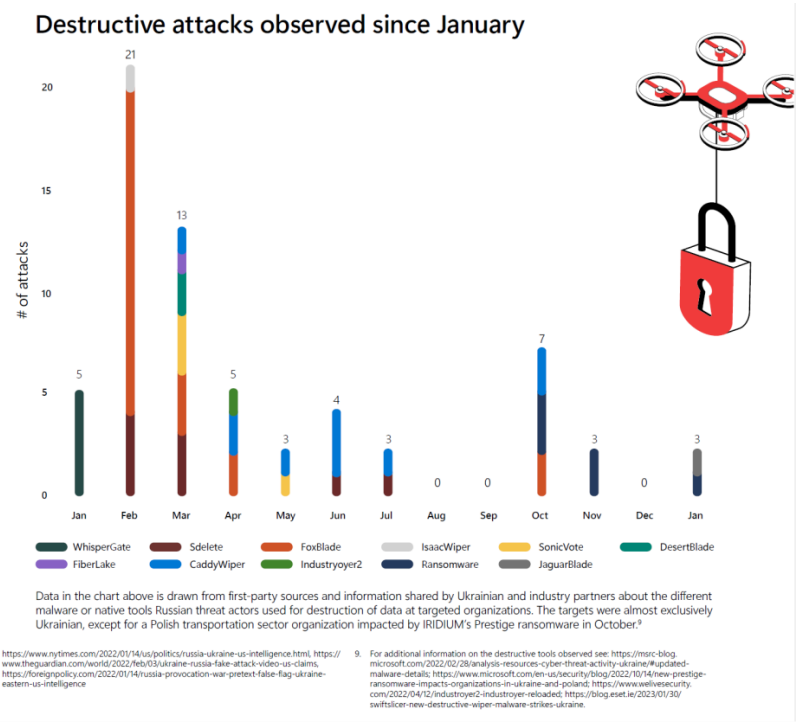


Figura 3: *Andamento degli attacchi informatici a partire da gennaio 2022*[9]

Fase 2: Il focus degli attacchi e la propaganda russa si rivolge a minare il sostegno a Kiev

FIne Marzo 2022 – Settembre 2022

Dalla fine di marzo all'aprile 2022, le forze russe si sono ritirate dai loro fronti di avanzata verso Kiev da nord e da est per concentrarsi sul Donbas e su altre regioni allora occupate. Grazie ai dati ottenuti dalla telemetria si è scoperto che threat actor russi dirigevano i loro attacchi informatici verso il settore della logistica e dei trasporti all'interno dell'Ucraina, probabilmente per interrompere il flusso sia di armi che umanitario verso le linee del fronte. Tra i più attivi, troviamo ancora una volta IRIDIUM che ha operato sia con attività distruttive, tramite malware, che attraverso operazioni di intelligence per raccogliere informazioni contro il settore dei trasporti ucraino.

9 https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW10mGC

Durante lo stesso periodo, le forze russe hanno lanciato numerosi attacchi missilistici contro le infrastrutture di trasporto ucraine provocando l'interruzione del flusso di merci e persone in tutta l'Ucraina. I threat actor hanno anche condotto operazioni di spionaggio informatico contro organizzazioni che forniscono assistenza militare e umanitaria all'Ucraina. Un altro attore, ACTINIUM, noto anche come Gamaredon, ha condotto diverse campagne di phishing rivolte a organizzazioni di aiuti umanitari e a entità coinvolte in indagini sui crimini di guerra avvenuti da aprile a giugno 2022.

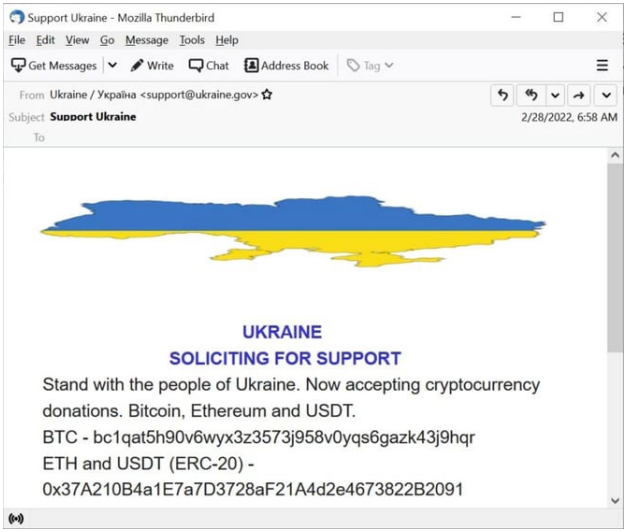


Figura 4: *Screenshot di uno dei messaggi di phishing che ACTINIUM ha inviato*

L'esca di cui sopra, mascherata da comunicazione dell'Ufficio del procuratore generale dell'Ucraina, riguarda le procedure per i rapporti su casi criminali di alto profilo, secondo la traduzione automatica.
Ad aprile, ACTINIUM ha tentato di ottenere l'accesso a reti di entità simpatizzanti dell'Ucraina inviando e-mail di phishing mascherate da "*funzionari militari ucraini*" che chiedevano ulteriore assistenza umanitaria e militare.
Tra maggio a giugno, il gruppo ha inviato e-mail di phishing mirate a diverse organizzazioni umanitarie con sede in Ucraina e nei Paesi Baltici nonché ad agenzie intergovernative che assistono le vittime di guerra e ne documentano i crimini.
A partire da maggio, SEABORGIUM, noto anche come ColdRiver, ha inviato messaggi di phishing a organizzazioni che producono o trasportano armi, droni, dispositivi di protezione e altre forniture militari per clienti militari statunitensi ed europei. Molte delle **organizzazioni prese di mira forniscono servizi a sostegno dell'Ucraina.**

Mosca ha anche riattivato le campagne di propaganda per colpire le popolazioni all'interno del territorio ucraino occupato e all'estero, concentrandosi sui combattimenti che hanno colpito la centrale nucleare di Zaporizhzhia nel sud dell'Ucraina, con i propagandisti russi che allarmavano gli attacchi nucleari.

Con l'obiettivo di ottenere una copertura allineata al Cremlino sulla stampa internazionale, il governo russo ha sponsorizzato un tour di pubbliche relazioni nel Donbas in primavera, con membri della stampa in visita da Francia, Germania, India e Turchia, tra gli altri, nonché visite alla centrale nucleare di Zaporizhzhia.
Le autorità di occupazione affiliate al Cremlino hanno persino preso il controllo di stazioni radio e di organi di stampa locali in molte città occupate.

Fase 3: L'unione delle operazioni informatiche e cinetiche
Settembre 2022 – Ad oggi

A seguito della vittoriosa controffensiva ucraina meridionale e nord-orientale, da fine agosto a settembre, il governo russo ha aumentato le sue rivendicazioni sul territorio ucraino e intensificato le operazioni militari progettate per spezzare la volontà del popolo ucraino. Mosca ha annunciato una parziale mobilitazione militare alla fine di settembre e ha annesso illegalmente le regioni ucraine di Luhansk, Donetsk, Zaporizhzhia e Kherson all'inizio di ottobre. Quasi immediatamente dopo aver rivendicato la sovranità sull'est, l'esercito russo ha lanciato una raffica di attacchi missilistici su infrastrutture energetiche critiche in tutte le principali città ucraine, tagliando l'energia ai civili nelle aree colpite con l'arrivo dell'inverno. A dicembre, il presidente russo Vladimir Putin ha ignorato le critiche internazionali relative all'attacco missilistico, sostenendo che gli attacchi alle infrastrutture energetiche sarebbero continuati. Contemporaneamente, sono aumentate le attività cibernetiche e a dicembre, IRIDIUM ha diretto attacchi malware wiper contro infrastrutture civili elettriche e idriche in Ucraina, anticipando, di fatto, gli attacchi missilistici a quelle stesse infrastrutture.
Al di fuori dell'Ucraina, IRIDIUM ha intensificato le operazioni per interrompere le catene di approvvigionamento verso l'Ucraina mentre altri gruppi collegati al GRU hanno preso di mira le organizzazioni occidentali legate alla difesa, probabilmente perraccogliere ulteriori informazioni. Nello stesso periodo, IRIDIUM ha esteso gli attacchi con l'operazione ransomware Prestige citta in precedenza contro il settore dei trasporti in Polonia, membro della NATO e hub logistico chiave per le forniture dirette in Ucraina.
A partire da ottobre, un altro gruppo collegato al GRU, STRONTIUM, aveva compromesso una società polacca del settore dei trasporti e in seguito aveva dato inizio ad una fase di ricognizione delle organizzazioni affiliate alla NATO creando le basi per condurre future intrusioni contro questo set di obiettivi.

La **Figura 5** mostra i media e gli sforzi in termini di pubbliche relazioni sostenuti dall'inizio della guerra e progettati per sostenere le tesi del Cremlino negli ambienti dei media locali. Affermati agenti ed influencer russi hanno promosso canali di propaganda locali lanciati

attraverso Radio Tavria e Za! TV per rilanciare narrazioni allineate al Cremlino nei territori occupati e annessi. Questi agenti sono anche fondamentali per mantenere gli attuali sforzi di pubbliche relazioni sponsorizzati dallo stato russo nei territori occupati, promuovendo organizzazioni giovanili filorusse come Yunarmia (Esercito della Gioventù), Molodaya Gvardia (Guardia della Gioventù di Russia Unita) e YugMolodoy (Gioventù del Sud).

Figura 5: *Ecosistema della propaganda russa*

Gli influencer hanno anche intensificato le attività di crowdfunding per sostenere lo sforzo bellico della Russia. Uno di questi esempi è "Readovka Helps", un'organizzazione affiliata all'outlet filorusso Readovka e guidata da Alexander Ionov che è stato incriminato dal Dipartimento di Giustizia degli Stati Uniti per aver lavorato in collaborazione con l'FSB e "orchestrato una campagna di influenza ritenuta straniera durata anni". Nonostante pretenda di mantenere una missione umanitaria, Readovka Helps ha raccolto forniture per i soldati russi. Da un punto di vista digitale, i siti web che si presentano come agenzie di stampa locali ucraine estraggono contenuti da fonti affiliate allo stato russo e mostrano in modo prominente lo "ZOV" della Russia.

Mentre alcuni dei siti sono rimasti inattivi, in particolare quelli creati su misura per le città ucraine che la Russia non è riuscita a occupare, altri hanno persistito, riciclando apertamente i media russi e i messaggi pro-Cremlino. I gruppi di social media filorussi come l'"Esercito digitale della Russia", creato nel gennaio 2023, usano tattiche come l'attacco

coordinato da parte di un gruppo di utenti per spammare le comunità dei social media ucraine online con propaganda di guerra russa.

Conclusioni

Se le immagini dei palazzi residenziali sventrati dai missili e i cadaveri per le strade ci restituiscono l'orrore dell'invasione russa e dei crimini compiuti ai danni dei civili, altrettanto distruttivi sono stati gli attacchi cyber, passati in sordina dopo le prime, convulse settimane di guerra, ma non per questo sospesi. Anzi.

Per riassumere, nel 2022 in Ucraina sono stati registrati 4.500 cyber attacchi. Il triplo rispetto al 2021 (1.400), più di cinque volte quelli del 2020, secondo i dati forniti a Wired dal Centro nazionale ucraino di coordinamento della sicurezza informatica.

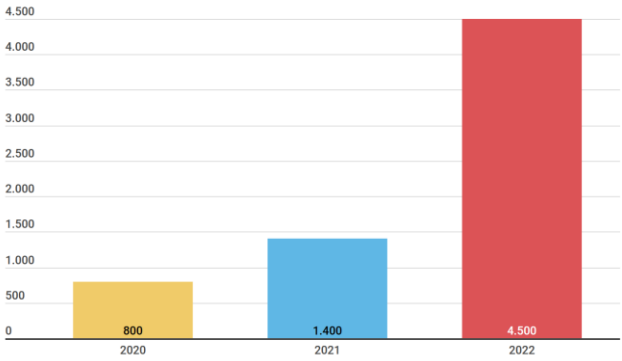


Figura 6: *La crescita degli attacchi informatici in Ucraina*

In una conferenza stampa a gennaio, peraltro oggetto, secondo gli ucraini, di un tentato attacco informatico da parte della Russia, Yurii Shchyhol, a capo del Servizio statale di protezione speciale delle comunicazioni e delle informazioni, ha detto che "*lo scopo principale degli attacchi cyber è lo spionaggio, la distruzione delle infrastrutture critiche, la guerra informativa e psicologica così come il reperimento di dati su cittadini, sistemi e logistica all'interno del Paese, incluso il movimento delle truppe*".

Le incursioni informatiche non servono solo a mettere ko reti, server e telecomunicazioni. *La Russia ha un approccio ibrido. Dopo aver rubato i dati, li usa per creare campagne di disinformazione*. Un amplificatore del panico generato dalla guerra, ma anche un'arma per raccogliere consenso all'estero, minare il sostegno all'Ucraina e confondere le acque. La difesa non è meno costosa, in termini di tecnologie, risorse e tempo.

Ci sono due lezioni da mandare a memoria. La prima è "dotarsi di staff informatici", perché la difesa richiede risorse. E la seconda è il ruolo chiave del cloud, "che ha permesso all'Ucraina di archiviare i dati al di fuori del raggio d'azione del nemico". Tanto che la Nato sta spingendo perché i suoi alleati investano nel cloud per la difesa, per assicurare continuità dei dati e delle operazioni, il coordinamento di attività in più domini (terrestre, cibernetico, navale). Lo spiegava a Wired Antonio Calderon, responsabile servizi di rete e infrastrutture informatiche dell'agenzia della Nato per le comunicazioni, Nci, a un evento del settore organizzato in Belgio lo scorso autunno: "È una delle tecnologie che riteniamo più importanti per aiutarci a sviluppare sistemi di difesa, ma pone varie sfide, dalla segregazione delle informazioni classificate all'interoperabilità dei programmi fino ai temi di sovranità del dato". In definitiva, al mondo d'oggi, la sfera digitale pervade ogni singolo elemento della nostra società e Il conflitto tra Russia-Ucraina è fonte di nuove pratiche e nuove tecnologie di guerra, così come nuove modalità di cybercrime e mai come oggi risuonano vere le parole del presidente Xi Jin-ping: "La tecnologia avanzata è l'arma più affilata dello stato moderno. Se i Paesi occidentali sono stati in grado di dominare il mondo in epoca moderna è anche perché detenevano il primato tecnologico".

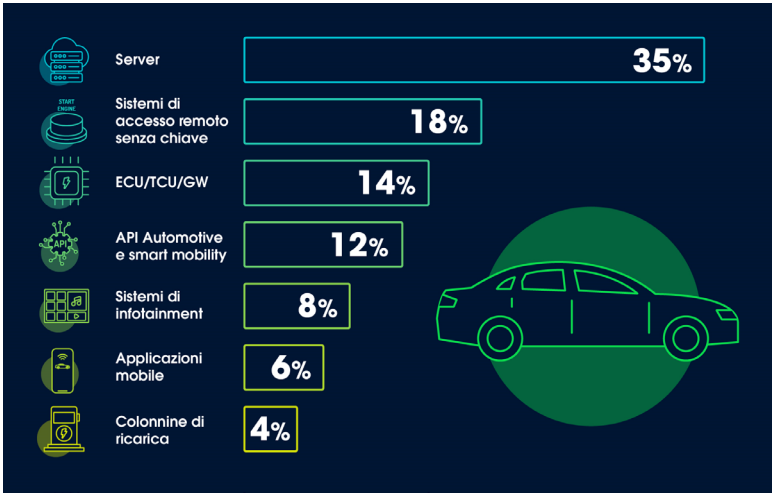
Smart Mobility API e recharge line come nuovi vettori di attacco

[A cura di Gaspare Silvestri, BearIT]

Immaginiamo una moderna automobile come un sistema multimediale interconnesso, in grado di offrire servizi di supporto e di esperienza al guidatore (infotainment), in grado di comunicare dati di telemetria utili alla predittività delle problematiche sul veicolo, piuttosto che garantire avanzati sistemi di comunicazione in grado di supportare azioni di geolocalizzazione del veicolo, utili in caso di situazioni potenzialmente impattabili la sicurezza fisica degli occupanti dell'abitacolo.
Tutte queste informazioni, scambiate verso sistemi esterni centrali in grado di elaborarle sia in termini qualitativi che quantitativi, risultanto essere tanti utili per il loro buonuso quanto potenzialmente dannose, in caso di accesso improprio ed utilizzo non autorizzato degli stessi, da parte di attori malevoli, il cui scopo potrebbe essere portare a compimento azioni di natura offensiva.
In quest'ottica, un'automobile è quindi da vedersi come un complesso sistema informatico che però, a dispetto dei suoi omologhi di natura ICT standard, presenta un livello di rischio molto più alto, in quanto i meccanismi di esposizione citati in precedenza risultano essere scarsamente protetti, o la cui sicurezza è gestita in maniera ancora non strutturata come potrebbe essere per un sistema infrastrutturale informatico standard. In quest'ottica, risulta quindi facile immaginare che il livello degli attacchi verso questa tipologia di dispositivi risulta essere aumentato nel corso degli ultimi anni.
Da uno studio del primo semestre dell'anno 2023 di Upstream Security[1], la percentuale di incidenti informatici e relativi databreach, nel periodo indicato, risulta soggetta ad un aumento del 37%,con un ampliamento del classico vettore di attacco (centralina intelligente interconnessa delle moderne automobili) verso i nuovi scenari di Smart Cities e Smart Mobility, con particolare riguardo verso le smart mobility API (software component) e verso la rete interconnessa di colonnine di ricarica elettrica (hardware component), in un'ottica di indebolimento o interruzione di servizio a disposizione delle masse e dei cittadini, con relativi impatti su tutto quanto concernente la quotidianità e la possibilità di operare in maniera smart negli spostamenti su ruota.
Nello specifico, i vettori di potenziale attacco risultano avere le seguenti percentuali di ripartizione sul perimetro:

- Backend server → 35%;
- Keyless system → 18%;
- ECU/TCU/GW → 14%;
- Smart mobility API → 12%;
- Infotainment → 8%;
- Mobile App a supporto dei sistemi di infotainment → 6%;
- Colonnine di ricarica → 4%

Le colonnine di ricarica elettrica e le Smart Mobility API risultano essere due nuovi segmenti di interesse, in termine di attività di offensive, come da dettaglio dei paragrafi relativi.



Smart mobility

Il modello di vendita ed acquisto delle auto sta subendo, nel corso degli ultimi anni, un rapido ed inarrestabile cambio di paradigma, passando dalla classica vendita dell'oggetto di proprietà verso una figura di acquirente, ad un più moderno e flessibile modello di noleggio a servizio, sulla base del quale un utente finale noleggia a tempo un veicolo per spostarsi all'interno di un ecosistema interconnesso, con la capacità di ottenere dati aggregati in grado di facilitare le azioni di analisi predittiva o comportamentale del perimetro di riferimento.
In questo scenario è fortemente agevolata la facilità di attacco ai servizi informatici a supporto della smart mobility, essendo a disposizione un perimetro estremamente esteso e, ad oggi, sostanzialmente non coperto in maniera adeguata rispetto alle esigenze di servizio.
Le componenti principali oggetto di analisi in questo articolo saranno le due di seguito elencate:

- Smart Mobility API;
- Recharge line (colonnine di ricarica elettrica).

API

Tutto l'ecosistema di Smart Mobility si basa, da un punto di vista di componentistica software, su applicazioni in grado di effettuare un interscambio dati rapido e massivo tra loro, al fine di garantire la veridicità del dato presente, oltre ad elevati livelli quantitativi e qualitativi di informazioni, utili ad arricchire l'ecosistema di big data a supporto dei servizi di settore.

L'ampliamento dell'esposizione di servizi di Smart Mobility API ha portato ad un incremento del 380% complessivo degli attacchi sull'area funzionale specifica [2] , con una percentuale di successo di incidenti estesi (data breach e danni dimostrati all'operatività) pari al 12% del totale.
I principali tentativi di attacco registrati nel corso dell'anno 2023 sono stati:

- controllo remoto del veicolo (accensione, spegnimento, gestione di componenti connesse) tramite chiamate malevole ai servizi e metodi esposti tramite le API di settore;
- privilege escalation e controllo remoto dei veicoli attraverso le chiamate API alle componenti GPS fisicamente installate;
- possibilità di controllo remoto di veicoli di appartenenza nord americana, attraverso l'utilizzo di scripting pubblici e disponibili su piattaforme online di source code repository (GitHub).

Hardware (smart components, recharge line)

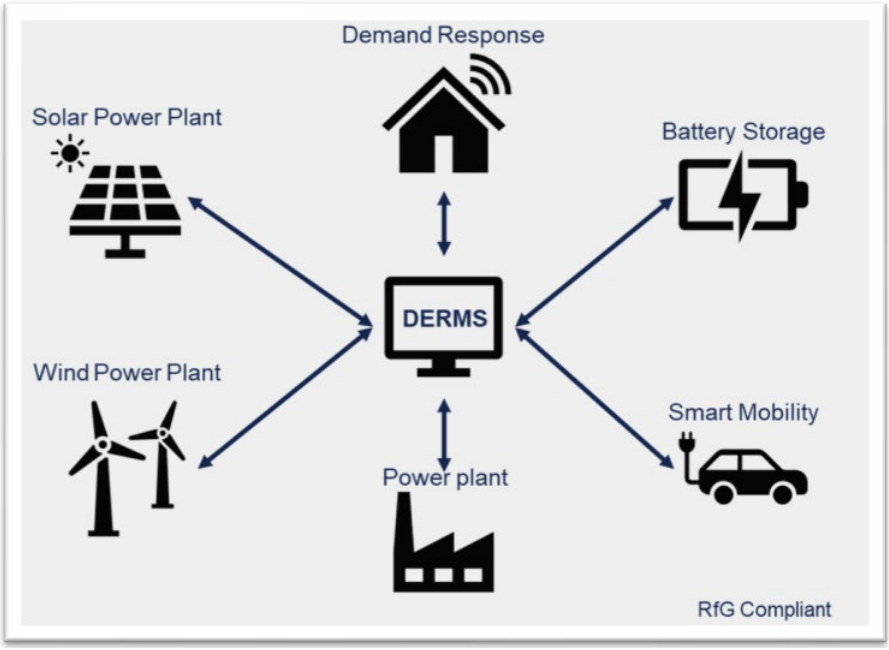
L'evoluzione tecnologica messa a disposizione con il modello delle smart city vede quindi la presenza di nuovi modelli anche di rifornimento per i **veicoli as a service** a disposizione degli utenti finali. Nello scenario di cambiamento a livello mondiale che stiamo vivendo entrano quindi prepotenti i veicoli elettrici, sia privati che per attività produttive, parte integrante di un miglioramento qualitativo globale messo proprio a disposizione dalle smart city. In questo scenario, quindi, le nuove modalità di rifornimento dei veicoli passeranno non più per i vecchi distributori di carburante classico (diesel, benzina, GPL, metano), ma per colonnine di ricarica elettrica per i mezzi di trasporto full electric.
Una colonnina di ricarica elettrica è un componente hardware in grado di erogare elettricità ad una potenza sufficiente tale da garantire la ricarica di una batteria di un'automobile, all'incirca nell'ordine dei 43 kW in corrente alternata o fino a 350 kW in corrente continua, per supporto della ricarica veloce delle auto elettriche.
La componente hardware, invece, viene gestita e resa operativa attraverso un software intelligente ospitato da un sistema operativo minimale, tipicamente su base Linux, e remotamente gestibile per attività di aggiornamento o di manutenzione; partendo da questo assunto, la colonnina risulta essere quindi un oggetto esposto e potenzialmente vulnerabile, alla stregua delle automobili che usufruiscono dei loro stessi servizi.

In quest'ottica, è possibile identificare i seguenti principali canali e vettori di attacco alla rete di ricarica:

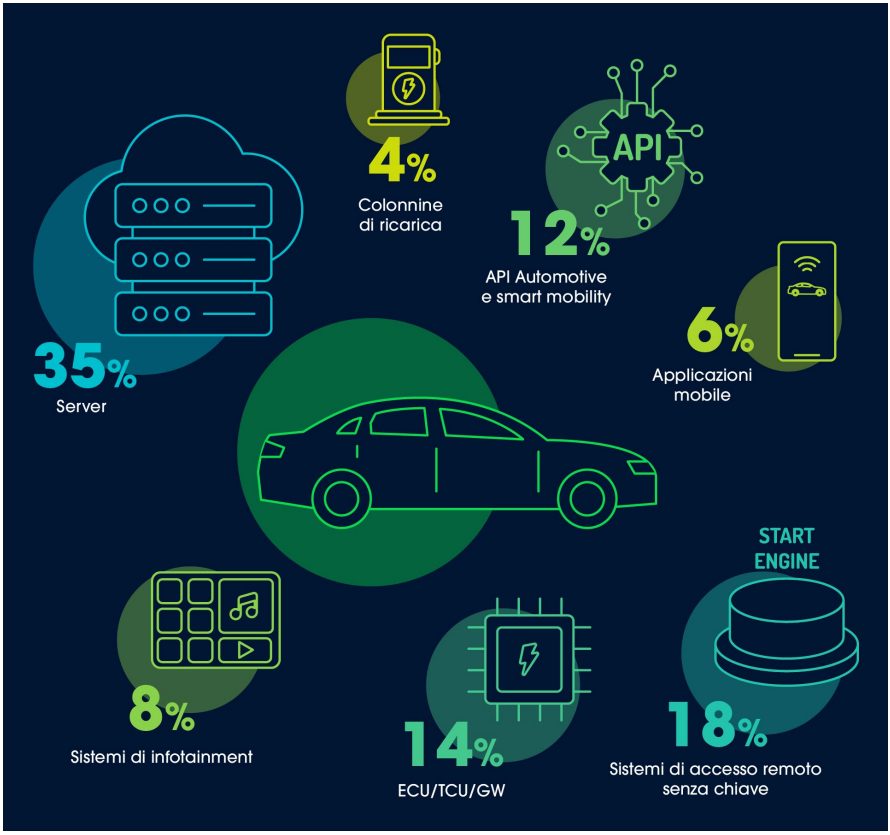
- **dall'auto alla rete di ricarica**: in questo scenario, i vettori di attacco possibili sono l'impersonificazione di un veicolo ed i relativi impatti sulle azioni malevole di pagamento, oppure l'utilizzo dell'auto come base di diffusione / spreading dell'oggetto malevolo verso la rete elettrica di ricarica, con relativi impatti sull'operatività e la fruibilità globale dei servizi;
- **dalla rete di ricarica all'auto**: in questo scenario,la colonnina di ricarica viene infettata o controllata remotamente al fine di fare injection di contenuti malevoli o di remote

control verso il veicolo agganciato in ricarica, così da poter prendere controllo e possesso dell' **ECU (Electronic Control Unit)**. Lo stesso scenario può essere immaginato con un attacco in batteria alla flotta connessa in ricarica, quindi con interruzioni di servizio o impatti in larga scala;

- **attacco al sistema di gestione di ricarica**: in questo scenario, il **CSMS (Clearing and Settlement Mechanisms)** diventa oggetto di attacco cercando di comprometterne i meccanismi di fatturazione e pagamento associati, impattando le transazioni in essere o modificando impropriamente conti e costi di ricariche elettriche, con impatti riguardanti l'utenza finale del servizio;
- **attacco al protocollo di comunicazione tra stazioni di ricarica** (**OCPP – Open Charge Point Protocol** [3])**:** in questo scenario, al protocollo di interconnessione tra stazioni di ricarica vengono inviati comandi errati atti a generare comportamenti non previsti nella colonnina fisica di ricarica, con relativa necessità potenziale, quindi, di reboot della stessa e quindi di temporaneo o prolungato disservizio sulla stazione. Alternativamente, una volta preso il controllo della stazione di ricarica, l'attaccante potrebbe effettuare l'installazione di componentistica software e firmware dannosa, estendendo la capacità di azione sulla rete di ricarica anche verso sistemi terze parti interconnessi (immagine di riferimento sottostante);



- **attacco ai metodi di ricarica esposti dalle smart mobility API**: in questo scenario, si ritorna alle modalità di utilizzo improprio dei metodi API di smart mobility esposti, come da dettagli precedenti, con la sola modifica al target di riferimento (non più le componenti software dirette, ma le componenti software legate all'interfacciamento con la componentistica hardware quale, ad esempio, la rete di ricarica elettrica).



Il ruolo del veichle SOC (vSOC)

Il mercato della cyber security applicata all'automotive risulta essere in forte crescita, con una stima di impatto nel 2032 pari a circa **16 miliardi di dollari americani,** con un dato di partenza del 2023 stimato in circa **3,6 miliardi di dollari americani** [4]**.**

Tutta la telemetria generata da un ecosistema completo come quello delle smart city (veicoli, sistemi di interscambio dati, applicativi e metodi di esposizione, hardware per ricarica dei veicoli) a oggi genera una quantità di dati (big data) che sarebbero di complessa analisi

e gestione da parte di personale non qualificato. In quest'ottica, è sempre più attiva la presenza sul mercato di strutture e sale controllo dedicate a questo tipo di applicazione in ambito automotive, chiamate vehicle SOC (vSOC), identificabili come un'evoluzione mirata e settoriale di una classica sicura di Security Operation Center (SOC), rispondente ad algoritmi e paradigmi di analisi studiati ad hoc per il settore automotive, con il sempre maggiore apporto di soluzioni e piattaforma di intelligenza artificiale, per una più puntuale e mirata attività di controllo dei soli dati rilevanti, in un contesto in cui i dati generati ed archiviati dai sistemi di centralizzazione (SIEM, log concentrator) potrebbero essere in un numero troppo elevato per una attività di log & event management di tipo standard, non ottimizzata tramite componenti di AI.

I processi di importanza rilevante da prevedere all'interno di un vehicle SOC dovrebbero essere i seguenti:

- rilevazione delle anomalie di attacco attraverso la profilazione di filoni specifici di correlazione, dove le sorgenti dati che confluiscono all'interno del data lake dei big data raccolti dovrebbero essere regolamentati da motori di AI (intelligenza artificiale) e da meccanismi correlati di machine learning;
- gli stessi meccanismi di machine learning dovrebbero, una volta terminata la fase di auto apprendimento, essere in grado di strutturare delle baseline comportamentali e poterne calcolare gli scostamenti, così da attivare gli alert necessari da mettere a disposizione degli operatori attivi su un vSOC;
- risorse operative sufficienti, sia in termini di personale che di tecnologia, per essere in grado di gestire la mole di dati enorme ricevuta dai concentratori, con delle estreme ottimizzazioni di aggregazione e filtering dei risultati a monte, così da garantire che il personale operante vada ad intervenire in maniera puntuale su segnalazioni realmente rilevanti e su nuovi scenari, lasciando la gestione delle comunicazioni standard e di natura ricorsiva ai sistemi soggetti ad AI e ML (machine learning).

In termini di meccanismi di regolamentazione e compliance, un vSOC dovrebbe rispondere agli standard delle certificazioni R155, R156 ed ISO/SAE 21434, delle quali di riporta di seguito un estratto di alcuni punti principali:

- **R155**
  - regolamentazione qualitativa di tutto il ciclo di vita del prodotto (introduzione **anno 2022**);
  - analisi di qualità e controlli di sicurezza sulla supply chain;
  - imposizione dei vincoli qualitativi ed applicazione delle best practices di Cyber Security per tutti i fornitori di casa madre coinvolti nella realizzazione di uno componente.

- **R156**
  - regolamentazione dei meccanismi per la rispondenza alle best practices di settore per l'aggiornamento dei software on board in modalità "over the air", quindi tramite controllo remoto e governance dell'aggiornamento della soluzione software, in termini di compliance e di principi di cyber security (introduzione **anno 2024**);

- **ISO/SAE 21434**
  - Framework necessario alla garanzia di corretta postura di sicurezza delle componenti on board automobili, garantendone la validità per tutto il ciclo di vita del componente;
  - applicazione di meccanismi di valutazione e gestione del rischio;
  - applicazione di meccanismi di validazione dello scambio sicuro di informazioni tra componenti;
  - applicazione di una strategia di mitigazione e controllo degli incidenti informatici.

Riferimenti

1. Upstream's 2023 Global Automotive Cybersecurity Report
2. Upstream's 2023 Global Automotive Cybersecurity Report
3. Whitepaper-OCPP-IEC-61850-a-winning-team-Report-No.23-3107-08-09-2023-Version.1.0.pdf (openchargealliance.org)
4. Automotive Cybersecurity Market Size To Hit USD 16.43 Bn By 2032 (precedenceresearch.com)

Cyber Threat Intelligence
Advancing security decision making

[A cura di Luca Nilo Livrieri, CrowdStrike]

Le minacce informatiche continuano ad evolversi, sia dal punto di vista tecnico che da quello organizzativo; sono sempre più frequenti le specializzazioni dei threat actor che suddividono le proprie attività in microservizi operativi, così da essere sempre più specializzati nelle diverse fasi dell'attacco. Lo strumento tecnico resta un meccanismo di difesa fondamentale ma per essere efficiente necessita di informazioni per poter capire, contestualizzare e prevenire un attacco.

È possibile avere informazioni sulle tecniche usate dai threat actor, l'approccio che adottano per i diversi bersagli, come interagiscono tra loro e, infine, utilizzare questi dati per incrementare la postura di sicurezza del proprio ecosistema. La domanda però è, come scaricare a terra tutto il know how della threat intelligence? Quali sono i livelli con i quali dobbiamo lavorare quando si parla di Threat Intelligence?

Di solito in Crowdstrike diciamo che non esiste un problema di malware, esiste un problema di avversari e attaccanti. Dietro ogni attacco informatico si nasconde un avversario umano con motivazioni, obiettivi e abilità distinte. Più ne si sa , meglio è possibile difendere la propria azienda.

Negli ultimi anni, la threat intelligence è diventata un ingrediente fondamentale per la maggior parte dei moderni team di sicurezza e parte integrante dei loro strumenti. Consente alle organizzazioni di avere una migliore comprensione degli avversari per anticipare eventuali minacce emergenti e prendere decisioni di sicurezza proattive per proteggersi da queste minacce.

L'85% delle organizzazioni ha riferito di "produrre" o "consumare" qualche tipo di intelligence sulle minacce. Sebbene la cyber threat intelligence (CTI) sia diventata una componente essenziale di una strategia di sicurezza matura e sana, il suo pieno valore non è ancora necessariamente ben compreso. Tuttavia, se utilizzata in modo efficiente, la CTI può offrire ai team di sicurezza vantaggi sostanziali, non solo durante un incidente, ma anche prima ancora che inizi un attacco. Fornendo informazioni dettagliate sulle minacce per ottimizzare la prevenzione, la detection e la risposta, la threat intelligence aiuta i team di sicurezza a rimanere un passo avanti rispetto agli avversari.

Poiché la threat intelligence può essere applicata ad un'ampia varietà di casi d'uso e viene fornita in molte forme, sono comuni incomprensioni su ciò che la CTI comporta e come dovrebbe essere resa operativa in organizzazioni di diverse dimensioni, livelli di maturità e profili di rischio.

La threat intelligence può derivare da diverse fonti, tra cui log di sistema e telemetria di rete, feed di minacce esterne, open source, forum sul deep e dark web, esempi di malware e scambio di informazioni con partner fidati e esperti del settore. Tuttavia, una buona intelligence sulle minacce diventa utile quando è realmente utilizzabile dai team di sicurezza,

ovvero quando migliora il processo decisionale e la postura di sicurezza informatica di un'organizzazione affrontando casi d'uso specifici a livello strategico, operativo e tattico. A livello tassonomico di massima infatti, la threat intelligence può essere suddivisa in queste tre categorie principali: tattica, operativa e strategica.

1. La threat intelligence tattica è quella più "tecnica" e a breve termine e può essere considerata la più semplice. Per banalizzare è quella che ha fra le sue caratteristiche quella di cercare tracce di attacchi, per esempio, gli indicatori di compromissione (IOC).
2. L'intelligence operativa è quella che fornisce il contesto comprendendo e profilando gli attori delle minacce, concentrandosi sul presente o sul breve termine.
3. L'intelligence strategica informa sui rischi informatici associati agli eventi geopolitici, sulle tendenze delle minacce globali e sull'impatto a lungo termine che ciò può avere sulle organizzazioni, riflettendo sugli impatti delle decisioni prese in ambito di rischio informatico.

La threat intelligence tattica

La threat Intelligence tattica si concentra sull'impatto operativo immediato e supporta le operazioni difensive raccogliendo, analizzando e sfruttando gli indicatori di compromissione e di attacco (IOC e gli IOA) e le tattiche, le tecniche e le procedure (TTP) degli attori delle minacce per migliorare le capacità di protezione e rilevamento in tutto l'ambiente di sicurezza. L'utilizzo di feed di IoC in diversi strumenti di sicurezza come piattaforme di intelligence sulle minacce, SIEM, strumenti di protezione degli endpoint, firewall o gateway e-mail consente una protezione, una detection e una reazione più rapidi.
Merita un approfondimento la differenza fra IOC e IOA per distingure anche i diversi livelli di threat intelligence oggi sul mercato. Gli indicatori di attacco (IOA) si concentrano sul rilevamento dell'intento di ciò che un utente malintenzionato sta tentando di realizzare, indipendentemente dal malware o dall'exploit utilizzato in un attacco, sono quindi indicatori comportamentali. Un indicatore di compromissione (IOC) è spesso descritto nel mondo forense come prova su un computer che indica che la sicurezza della rete è stata violata. Gli investigatori di solito raccolgono questi dati dopo essere stati informati di un incidente sospetto, su base programmata o dopo la scoperta di chiamate insolite dalla rete. Idealmente, queste informazioni vengono raccolte per creare strumenti "più intelligenti" in grado di rilevare e mettere in quarantena i file sospetti in futuro. Gli IOC di solito comprendono indirizzi IP malevoli, URL, hash di file, nomi di dominio pericolosi conosciuti, ecc, sono molto utili ma più "semplici" rispetto agli IOC.
Se le domande principali che circondano un incidente sono caratterizzate dal "quando e dove", la threat intelligence tattica risponde al "cosa" dell'incidente ed in questo "cosa" è molto utile cercare il comportamento dell'attaccante. A causa dell'aumento delle attività malevole e del sempre in crescita aumento delle superfici di attacco, I dati di threat intelligence devono essere leggibili dai software di sicurezza, direttamente consumabili dagli

strumenti di sicurezza sotto forma di di feed o tramite integrazione API. Per questo è fondamentale che gli indicatori forniti (IoC o IoA) siano ad alta confidenza e possano essere subito operativi.
Focalizzata sull'immediato futuro, la CTI tattica è il livello di threat intelligence più comunemente offerto, in quanto è anche la più facile da raccogliere e generare. Infatti può essere fornita tramite open-source e persino feed gratuiti e di solito ha una durata molto breve, poiché spesso gli IOC come IP dannosi o nomi di dominio possono diventare obsoleti in pochi giorni o anche ore. Inoltre, se la fonte non è sempre tempestiva o ad alta fedeltà, la threat intelligence tattica può essere incline a generare falsi positivi.

La threat intelligence operativa

La threat intelligence operativa sulle minacce fornisce informazioni fruibili che consentono ai team di sicurezza di rilevare, prevenire e rispondere alle minacce in tempo reale. Fornisce una comprensione più completa del panorama delle minacce rispetto a quella tattica, compresi gli avversari e le loro motivazioni, le capacità e gli intenti. Consente ai team di sicurezza di migliorare le proprie capacità di rilevamento, aggiungendo il contesto strategico e tecnico a qualsiasi indagine e consentendo di eseguire la ricerca delle minacce per scoprire qualsiasi minaccia emergente. La threat intelligence operativa consente di eseguire un monitoraggio attivo del rischio digitale degli asset dell'organizzazione sull'open, deep e dark web per essere avvisati di qualsiasi minaccia imminente e porre rimedio immediati.
La CTI operativa fornisce il contesto comprendendo e profilando I threat actor o i cluster di attività malevole. Focalizzato sul breve termine, risponde al "come", al "perché" e al "chi" dietro gli incidenti. Si concentra sulle motivazioni, l'intento e le capacità degli avversari e fornisce approfondimenti su come gli avversari pianificano, conducono e sostengono campagne e le operazioni principali. Le tattiche, le tecniche e le procedure avversarie (TTP) sono una componente chiave della threat Intelligence operativa sulle minacce. L'analisi di tali dati fornisce informazioni sugli attacchi imminenti e le campagne in corso.
Le macchine da sole non possono creare informazioni operative sulle minacce. L'analisi umana è necessaria per convertire metadati di attacco e gli approfondimenti dell'underground criminale dai forum o dal dark web market, in un formato facilmente utilizzabile. Mentre la threat intelligence operativa richiede di più risorse rispetto alla threat intelligence tattica, ha una durata generalmente più lunga perché è più difficile per avversari cambiare i loro TTP di quanto non lo sia per loro cambiare i loro strumenti, come un tipo specifico di malware o l'infrastruttura che utilizzano. Per questo motivo la presenza di Indicatori di attacco (comportamentali) nella CTI la rende di maggior valore rispetto ai semplici IOC.

La threat intelligence strategica

La threat intelligence strategica consente alle organizzazioni di comprendere meglio l'evoluzione del panorama delle minacce, le motivazioni e le intenzioni degli avversari, siano essi stati-nazione, criminali informatici o hacktivist, le tendenze emergenti e il potenziale impatto su risorse, infrastrutture e obiettivi aziendali critici. Fornisce approfondimenti e

raccomandazioni di alto livello riguardanti il contesto più ampio delle minacce alla sicurezza informatica per aiutare le principali parti interessate come il CISO, il CIO e il comitato executive per mitigare i rischi, allocare risorse e sviluppare strategie di sicurezza proattive. L'intelligenza strategica informa sulle tendenze di alto livello e sui motivi che possono accompagnare condizioni geopolitiche o tendenze della criminalità finanziaria. La CTI strategica mostra come l'eCrime globale, eventi internazionali, politiche estere e movimenti politici possono avere un impatto sulla sicurezza informatica di un'organizzazione. Questo livello di intelligence sulle minacce aiuta i decision makers a comprendere le implicazioni dei rischi informatici per l'intera organizzazione e capire quali investimenti in sicurezza informatica proteggono al meglio la loro azienda e si allineano con le sue priorità strategiche. La forma più avanzata di intelligence strategica richiede la raccolta e l'analisi dei dati aziendali e richiede sia una profonda comprensione della sicurezza informatica che della situazione geopolitica mondiale. L'intelligence strategica di solito si presenta sotto forma di report o documenti di sintesi.

In che modo la cyber threat intelligence può migliorare le difese

Qualunque sia il suo livello, la threat intelligence può fornire valore solo se è fruibile ovvero sfruttata e tradotta in azioni (in inglese il significato si rende molto meglio con la parola "actionable"). Nonostante una tendenza importante dell'aumento delle sottoscrizioni e dell'uso della threat intelligence, l'attuale utilizzo della threat intelligence rimane spesso tattica. Al di là dei casi d'uso banali come l'integrazione, la condivisione dei feed di intelligence a prodotti di sicurezza esistenti come IPS, firewall o SIEM, la maggior parte delle aziende sta ancora lottando per sfruttare appieno le informazioni che la threat intelligence fornisce. Di seguito troviamo quattro casi d'uso, a puro scopo di esempio di come la CTI può essere utilizzata per fornire una migliore sicurezza.

1. Ottimizzare la prevenzione e rafforzare le difese per prevenire gli attacchi

Come già anticipato precedentemente, l'applicazione più comune e più banale della threat intelligence è probabilmente l'utilizzo di indicatori per bloccare IP malevoli noti, URL, hash maliziosi, ecc. A tale scopo, i feed degli aggiornamenti delle minacce possono essere inseriti automaticamente nei prodotti di sicurezza per aggiornare le blacklist, il controllo degli accessi (ACL), I modelli o firme. L'integrazione diretta della threat intelligence "tecnica" in gateway, sistemi di rilevamento delle intrusioni (IDS), firewall di nuova generazione (NGFW) e gli endpoint migliora la capacità di un'organizzazione di rilevare minacce emergenti e note e difendersi automaticamente da loro.

Ciò che è invece meno comune e più avanzato è l'utilizzo della CTI operativa come opportunità per essere proattivi e stare veramente un passo avanti agli attaccanti. La threat intelligence operativa fornisce dettagli sulle minacce emergenti. Ad esempio, può identificare quali avversari sono i più probabili che prendano di mira un'organizzazione, nonché come e perché tali tentativi possono verificarsi. La threat intelligence può anche aiutare a ricono-

scere altri segnali in anticipo, come la creazione di infrastrutture a supporto di un attacco: che potrebbero prevedere campagne di attacco in preparazione.

Le informazioni di intelligence operativa consentono ai team di sicurezza di mettere in atto misure appropriate come l'applicazione di patch e l'eliminazione delle vulnerabilità, per proteggere la propria organizzazione ancor prima che un attacco abbia inizio. Ad esempio, apprendere tramite report di intelligence se la propria organizzazione è un potenziale bersaglio per un avversario e sapere quali exploit e kit di exploit sono comunemente utilizzati in tali attacchi, può aiutarti a dare priorità alle patch ed eliminare le vulnerabilità prima che l'attaccante abbia la possibilità di cominciare.

L'intelligence operativa può anche fornire altri segnali di allarme precoci, come la creazione di infrastrutture di attacco, che possono essere un segnale di campagne di attacco in divenire. Il ransomware Locky di qualche tempo fa è un esempio di come il team di CrowdStrike Intelligence abbia fornito un tale warning. Locky cambiava continuamente domini per l'accesso ai server di Command & Control (C2) usati per cifrare i file sull'hard disk della vittima. CrowdStrike Intelligence ha decifrato l'algoritmo di generazione del dominio di Locky e, attraverso questa analisi, è stato in grado di prevedere quale server e domini C2 Locky avrebbe usato. Con questo livello di intelligence operativa, i clienti di CrowdStrike sono stati in grado di bloccare in modo proattivo quei domini e proteggersi da Locky senza alcuno sforzo manuale.
Un esempio più recente di attacco noto sotto il nome Scattered Spider ha attirato l'attenzione a causa dell'impatto che ha avuto a partire dal secondo trimestre 2023 in ambienti cloud e ibridi.
Scattered Spider è un avversario di eCrime che conduce campagne mirate di social engineering principalmente verso aziende di customer care, nonché società di telecomunicazioni e tecnologia. L'avversario utilizza principalmente pagine di phishing per acquisire credenziali di autenticazione per Okta, Microsoft O365/Azure, VPN, ecc. Usando anche il "phishing vocale" per condividere codici OTP (one-time-password) utilizzando la "MFA fatigue" ossia la "fatica" delle notifiche di autenticazione a più fattori, che fondamentalmente spamma gli utenti con messaggi di autenticazione fino a quando non si arrendono e fanno clic sulla notifica stessa.
Scattered Spider ha anche dimostrato la sua competenza nell'ottenere persistenza ed evitare i principali strumenti NGAV implementando una vasta gamma di strumenti legittimi di monitoraggio e gestione remota, raccogliendo credenziali cloud su numerosi fornitori di servizi e disabilitando il software di sicurezza degli endpoint utilizzando una varietà di nuove tattiche.
In questo caso CrowdStrike Intelligence ha scritto quasi 70 report sulle minacce di Scattered Spider, fornendo IOC e IOA per rilevare le tecniche e identificando le vulnerabilità comuni che sfruttano per consentire ai team di sicurezza di implementare contromisure proattive per fermarli, prima che inizi l'attacco.

Maggiore è il livello dell'intelligence che un team di sicurezza ottiene su chi potrebbe prendere di mira la propria organizzazione e su come gli attaccanti operano, maggiore è la crescita del livello di formazione e consapevolezza dello stesso team di sicurezza che ne fruisce. Utilizzando la threat intelligence un'organizzazione può rafforzarsi meglio contro gli avversari dando priorità alle attività per contrastare le minacce ad alta probabilità e proteggere gli asset che hanno maggiori probabilità di essere prese di mira.

2. Velocizzare l'efficacia della detection

Le detections basate sull'intelligence (Intelligence-driven detections) sono anche un caso d'uso comune per la CTI tattica. A un livello elementare, l'ingestion e l'applicazione degli indicatori tecnici nei SIEM o nelle soluzioni di detection & response (EDR) possono accelerare enormemente l'efficacia delle detection. Potenziate (armate) con la threat intelligenze più recente, queste soluzioni possono correlare e rilevare automaticamente gli incidenti più velocemente e con maggiore precisione eliminando il tempo e le competenze necessarie per creare nuovi regole di detection.

Un uso più avanzato della threat intelligence per la detection si trova nella ricerca delle minacce (threat hunting). I programmi di threat hunting cercano in modo proattivo la presenza di attività di attacchi precedentemente non rilevati piuttosto che aspettare che i controlli di sicurezza interni diano l'allarme. Ma il threat hunting può essere scoraggiante, poiché sapere da dove iniziare e cosa cercare non è, purtroppo, necessariamente ovvio. In queste situazioni, l'aggiunta di informazioni di threat intelligence che diano nozioni operative è inestimabile; perché offre una migliore conoscenza di chi potrebbe attaccare l'organizzazione e perché il team di sicurezza può andare a caccia delle tracce lasciate dagli attaccanti. È possibile cercare dettagli anche minimi come le modifiche alle impostazioni del registro, le rimozioni di file, I processi in esecuzione e altri potenziali segni della presenza di un utente malintenzionato nell'ambiente. Inoltre, conoscere la motivazione e gli obiettivi di un avversario aiutano a restringere il campo e l'analisi ai sistemi che hanno maggiori probabilità di essere attaccati, in modo che possano essere inclusi nella ricerca.

3. Velocizzare i tempi di indagine e risposta agli incidenti

La threat intelligence svolge anche un ruolo importante nella definizione delle priorità, nell'indagine e nella risposta agli incidenti. Di fronte a troppi avvisi, troppi falsi positivi e una mancanza di contesto, i team di sicurezza possono avere difficoltà a determinare su quali incidenti concentrarsi. Possono anche spendere di più tempo del necessario per indagarli.
Fornendo le informazioni di contesto e attribuzione, la threat intelligence aiuta a dare priorità alle risposte e ad accelerare l'investigazione. Un alert che è attribuito ad un avversario sofisticato sarà evidenziato sopra ad avvisi irrilevanti come I rilevamenti di malware di "basso livello". Ciò consente ai team di risposta di dare priorità agli avvisi in modo rapido e appropriato. Con contesto e attribuzione, la gestione degli incidenti diventa gestibile.

I team di sicurezza possono iniziare a separare, come si dice in gergo, gli "alberi" dalla foresta" e applicare la corretta definizione delle priorità al carico di lavoro e al flusso di lavoro.

Quando inizia l'investigazione, l'attribuzione fornisce il contesto che rende possibile per chi deve rispondere all'incidente (Incident responders) di reagire efficacemente. Un aspetto essenziale di tale contesto è la comprensione delle motivazioni e delle tattiche, tecniche e procedure dell'avversario (TTP). In questo modo i responders possono reagire in modo rapido e preciso per proteggere gli asset presi di mira (targeted). Inoltre, se il profilo avversario fornito dalla threat intelligence include anche IOC correlati a quell'avversario, il team di risposta sarà in grado di eseguire ricerche sia a livello di infrastruttura sia a livello storico per valutare e comprendere appieno la portata dell'incidente. Questo può rivelare quanti sistemi potrebbero essere stati interessati in passato o se è la prima volta che l'azienda incontra quell'aggressore.
L'utilizzo del contesto e delle informazioni aggiuntive fornite dalla threat intelligence consente inoltre agli incident responders di vedere la correlazione tra gli avvisi che potrebbero sembrare isolati ad una prima analisi, per scoprire attacchi avanzati.
Si immagini, ad esempio, che la soluzione di protezione degli endpoint attivi un avviso perché uno degli endpoint si è connesso a un URL o a un indirizzo IP noto come dannoso dalla propria fonte di intelligence sulle minacce. Esaminando ulteriormente il rilevamento, ci si collega a un report CTI che informa che questo URL o IP è attualmente utilizzato per una campagna di infezione da malware attiva contro il proprio settore. Ci sono informazioni anche sull'attaccante che sta dietro la campagna e sui TTP associati con quell'avversario e un'analisi tecnica approfondita degli IOC e IOA che possono rivelare la loro presenza.
È ora possibile utilizzare questi indicatori per eseguire ricerche nell›ambiente, rivedere i registri e interrogare le soluzioni SIEM o EDR per determinare la reale portata e la gravità dell'incidente. Inoltre, è possibile inserire le firme e gli IOC nei sistemi di sicurezza per prevenire ulteriori tentativi di attacco. Infine è possibile condividere il know-how con le controparti di altre aziende nello stesso settore e condividere informazioni con loro.

4. Migliorare la sicurezza e le decisioni executive

A livello tattico, sapere chi, come e perché gli avversari potrebbero colpire la propria organizzazione consente ai decision makers di allocare le proprie risorse e focalizzare I propri investimenti per proteggere ciò che conta di più.
A un livello più alto, la CTI strategica può consentire un processo decisionale esecutivo ottimale.
Le decisioni strategiche possono includere un'efficace gestione del rischio informatico, il che significa identificare e valutare la prevalenza del rischio informatico globale e il loro impatto per selezionare l'opzione di risposta e gestione dell'incidente più efficace. del rischio. Ciò significa che i decision makers devono prendere dei rischi calcolati guidati da informazioni affidabili sulle minacce e sullo stato dell'arte degli attaccanti. Ad esempio, la CTI strategica può aiutare a determinare se aprire un nuovo ufficio in un'area geografica ad alto

rischio fornendo una valutazione completa della sicurezza informatica prima di effettuare un investimento in nuove strutture e assumere nuovi dipendenti.
Inoltre, la sicurezza informatica è diventata un argomento discusso nella maggior parte o in tutte le riunioni del consiglio di amministrazione. Sfortunatamente, molti dirigenti e C-level mancano di una visione strategica che consenta loro di capire se la loro attuale strategia di sicurezza è veramente ottimizzata per corrispondere ai loro profili di rischio. Quando si arriva a quelle conversazioni con i membri del consiglio di amministrazione, i team di security possono beneficiare delle informazioni sulle minacce date da una fonte di intelligence strategica affidabile in grado di fornire informazioni che siano ad alta confidenza per aiutare a rispondere alle domande e ai dubbi necessari per dare il contesto di business.

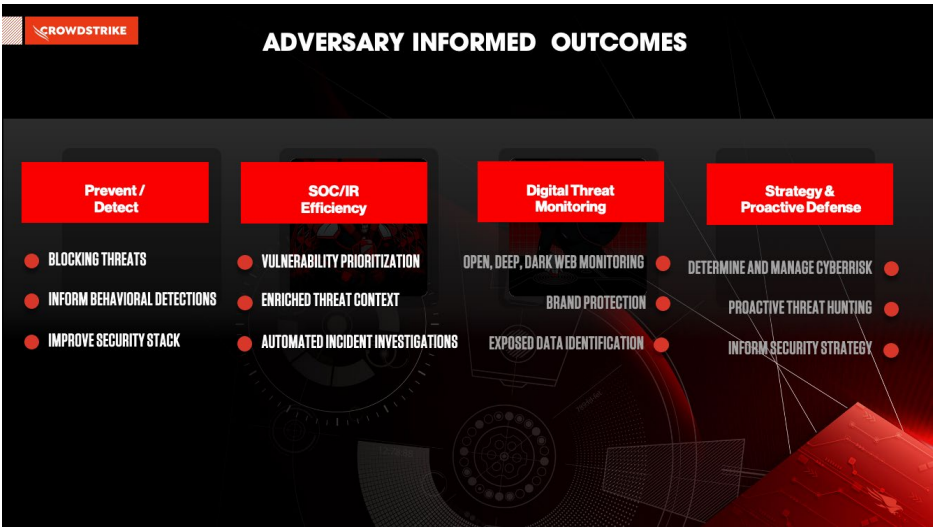


Figura 1: *Come la CTI può aiutare diversi settori dell'azienda*

Intelligenza Artificiale (IA), dati e cybersecurity: triangolazione perfetta o triangolo delle Bermuda? Potenzialità e sfide.

[A cura di Federica Maria Rita Livelli]

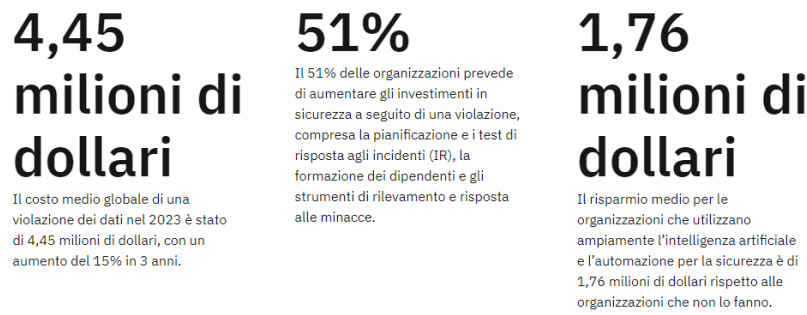
Attualmente viviamo in un mondo in cui i rischi sono imprevedibili, sempre più complessi e in rapida evoluzione. Ci troviamo nell'era della "datocrazia", in cui i dati sono diventati fondamentali per ottenere informazioni utili per semplificare e ottimizzare l'acquisto di polizze assicurative, finanziamenti e per comprendere meglio il rischio, grazie all'utilizzo di piattaforme basate sull'Intelligenza Artificiale (IA).
Le organizzazioni, grazie alla tecnologia e all'analisi automatizzata dei dati, possono perseguire in modo strutturato e consapevole la resilienza organizzativa e operativa. Tuttavia, è necessario gestire correttamente i rischi derivanti dai dati e dalla loro elaborazione tramite l'IA e dai rischi cyber per garantire la resilienza del business. Ovvero, si tratta di garantire una "triangolazione perfetta" tra dati, intelligenza artificiale e cybersecurity (scaturita da un approccio basato sul rischio e sulla resilienza), al fine di evitare che tutto ciò si trasformi in un "triangolo delle Bermuda".

Dati - L'evoluzione dei processi decisionali dell'IA è alimentata dal proliferare dei Big Data. Questi forniscono informazioni dettagliate che possono essere esplorate e analizzate per ottenere vantaggi significativi. Di fatto, l'analisi dei Big Data potenzia l'uso dell'IA e del Machine Learning, consentendo di combinare e analizzare grandi quantità di dati per individuare modelli e generare informazioni utili. Ciò si traduce in decisioni più rapide e migliori, migliorando l'efficienza, i ricavi e i profitti delle organizzazioni e permettendo una gestione più accurata dei rischi.

AI vs. gestione ed elaborazione dei dati - Le nostre vite sono state trasformate dalla presenza del digitale e diventa sempre più importante sfruttare le potenzialità offerte dalla tecnologia. I Big Data, la connettività tra persone, oggetti e sistemi, creano dinamiche connessioni che consentono di organizzare e ottimizzare situazioni in tempo reale, generando valore aggiunto. L'IA sta diventando una potente leva strategica e con un numero di applicazioni teoricamente illimitato.

Grazie alla capacità di elaborare una quantità sempre maggiore di dati disponibili, l'IA può offrire nuove possibilità e approcci strategici per le organizzazioni, nonché essere utilizzata nella previsione e nella valutazione dell'impatto dei vari rischi in diversi settori della società e dell'azienda. Di conseguenza, i framework per la gestione del rischio, della business continuity e cybersecurity subiranno un cambiamento di paradigma e adotteranno misure preventive che, in molti casi, verranno attivate automaticamente. Pertanto, grazie a monitoraggi e segnalazioni più accurati, sarà possibile prendere decisioni più appropriate e vincenti.

È doveroso ricordare che i dati vanno altresì protetti, considerando che secondo l' "*IBM Cost of a Data Breach Report 2023*", il costo medio globale di una violazione dei dati nel 2023 è stato di 4,45 milioni di dollari, il 15% in più rispetto al 2020.



Fonte dati IBM Cost of a Data Breach Report 2023

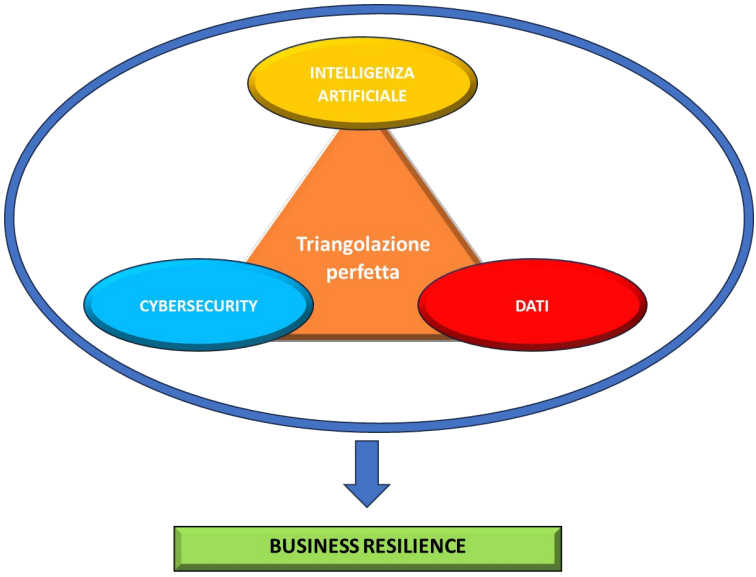
Ebbene, l'IA può anche contribuire a ridurre i costi degli attacchi informatici. Le organizzazioni che hanno utilizzato ampiamente l'IA per la sicurezza e le funzionalità di automazione nel loro approccio hanno riscontrato, in media, un tempo inferiore di 108 giorni per identificare e contenere la violazione. Dal report si evince che queste organizzazioni hanno inoltre segnalato costi inferiori per la violazione dei dati di 1,76 milioni di dollari rispetto alle organizzazioni che non hanno utilizzato funzionalità di automazione e IA per la sicurezza.
Sebbene una maggiore sicurezza e rilevamento consentano di risparmiare denaro e limitare l'esposizione, solo il 51% delle organizzazioni intervistate prevede di aumentare gli investimenti in sicurezza a seguito di una violazione, concentrandosi sulla pianificazione e sui test di risposta agli incidenti (*Incident Response -IR*), sulla formazione dei dipendenti e sulle tecnologie di rilevamento e risposta alle minacce. Le organizzazioni che hanno segnalato livelli elevati di pianificazione e test IR hanno risparmiato 1,49 milioni di dollari nel corso dell'anno rispetto a quelle che hanno segnalato livelli bassi.

La sfida della triangolazione perfetta: come bilanciare AI, dati e cybersecurity

L'automazione della gestione e della modellazione del rischio sta diventando sempre più diffusa, portando al miglioramento della qualità delle decisioni non solo per le organizzazioni, ma anche per i vari stakeholder.
Di fatto, in questo contesto, i dati elaborati dall'IA diventano sempre più strategici, in quanto possono semplificare e ottimizzare ad esempio, il valore dell'organizzazione, l'accesso al credito, la sottoscrizione di polizze assicurative, migliorando allo stesso tempo la compren-

sione del rischio e consentendo una categorizzazione più precisa e dettagliata.
Tuttavia, le nuove tecnologie che utilizzano i dati, pur aumentando le nostre capacità, modellano e guidano attivamente le nostre azioni, sia in positivo sia in negativo.
Pertanto, diventa sempre più importante garantire quella che abbiamo chiamato una "triangolazione perfetta". Essa rappresenta un equilibrio tra l'impiego dei Big Data, dell'IA, e della cybersecurity. Ovvero, una triangolazione che si converte in un prezioso strumento per garantire un futuro resiliente e sostenibile, facilitando il processo di digitalizzazione che inevitabilmente influisce sui processi e ridefinisce il modo in cui facciamo le cose.

Ne consegue che, affinché la triangolazione non si trasformi in un "triangolo delle Bermuda", è necessario assicurarsi che la tecnologia non dimentichi di essere uno strumento al servizio dell'umanità. Ciò significa acquisire una conoscenza adeguata dell'IA e della qualità dei dati su cui si basa, al fine di evitare i rischi intrinseci ad essa, valutarli e gestirli. In questa direzione, l'Unione Europea sta adottando l'AI Act e il Cyber Resilience Act, che sottolineano la necessità di modificare l'approccio al rischio nel contesto dell'innovazione tecnologica basata sui sistemi di IA, sulla garanzia della hsicurezza ed in conformità al GDPR.



In altre parole, diventa estremamente importante considerare la gestione del rischio fin dalla fase di progettazione dei modelli di AI, in modo che la supervisione sia costante e simultanea allo sviluppo interno e all'approvvigionamento esterno dell'AI in tutta l'organizzazione, adottando un approccio di "*derisking AI by design*".
Questo approccio consente di affrontare in modo proattivo i rischi associati all'AI, garantendo che la gestione del rischio sia integrata nel processo di sviluppo dell'AI stessa, riducendo così l'opacità dei modelli e consentendo una maggiore comprensione e controllo dei processi decisionali.
Ancora, ogni organizzazione che utilizza un modello di IA dovrà essere in grado di sviluppare un sistema di governance che consideri i seguenti aspetti:

- **Responsabilità aziendale:** l'organizzazione deve assumersi la responsabilità delle azioni compiute dal sistema di IA e garantire che siano conformi ai valori e agli obiettivi dell'azienda.
- **Comportamento adeguato verso clienti e dipendenti**: l'organizzazione deve assicurarsi che il sistema di IA si comporti in modo etico ed equo nei confronti dei propri clienti e dipendenti.
- **Rispetto dei requisiti normativi**: l'organizzazione deve rispettare le leggi e i regolamenti in vigore e prepararsi ad affrontare eventuali nuovi requisiti normativi futuri.

L'adozione dell'IA può migliorare significativamente la pianificazione della continuità aziendale (BCP) e aiutare a gestire il rischio cyber in modo più efficace. Le tradizionali metodologie di BCP e di Disaster Recovery potrebbero non essere sufficienti per affrontare la complessità e la velocità dei cambiamenti attuali. L'ottimizzazione della pianificazione delle varie strategie con l'IA può fare la differenza tra la stabilità e il collasso dell'organizzazione. Inoltre, l'IA può generare scenari per testare l'efficacia dei piani di risposta e valutare l'impatto di diverse strategie. In sintesi, la "triangolazione perfetta" tra IA, dati e cyber resilience permette di creare veri e propri "cruscotti intelligenti" che fungono da guida per le organizzazioni, consentendo loro di comprendere il contesto, identificare i rischi e le soluzioni più efficaci, nonché pianificare la continuità aziendale e il disaster recovery in modo ottimale ed evitare di trovarsi a operare in un "triangolo delle Bermuda".

"Cultura della sicurezza digitale: promuovere la sicurezza in un contesto basato sui dati e sull'intelligenza artificiale"

Una solida cultura della sicurezza all'interno delle organizzazioni è fondamentale per garantire la "triangolazione perfetta" tra IA, dati e resilienza. Ovvero, una cultura che promuove una migliore collaborazione tra i team di sicurezza e gli altri dipartimenti, migliora la conformità e aumenta la fiducia dei clienti. Inoltre, una cultura della sicurezza solida influisce positivamente sulla postura di sicurezza dell'organizzazione, preparandola alle nuove minacce e consentendo una resistenza e una ripresa più efficaci dagli attacchi informatici.

Ecco alcuni passi chiave per costruire e mantenere una forte cultura della sicurezza che promuova anche la resilienza e la fiducia digitale in organizzazioni che si basano sull'artificial intelligence e sui dati:

- **Leadership -** Una cultura della sicurezza parte dalla leadership. Il top Management dovrebbe essere il primo a adottare una mentalità orientata alla sicurezza e dare l'esempio al resto dell'organizzazione.
- **Conoscere e valutare -** Prima di migliorare la cultura della sicurezza, è necessario comprendere la cultura dell'organizzazione e la sua attuale posizione in termini di sicurezza. Ovvero si tratta di allineare la sicurezza alla cultura esistente e, successivamente effettuare una valutazione approfondita della sicurezza per identificare i propri asset critici, le potenziali minacce e vulnerabilità, e utilizzare i risultati per sviluppare una strategia di sicurezza completa.
- **Sviluppo di una strategia di sicurezza -** Una strategia di sicurezza è una vera e propria roadmap che definisce gli obiettivi, le finalità e il piano d'azione del programma di sicurezza di un'organizzazione. La strategia dovrebbe includere anche politiche e procedure che guidano i dipendenti nella gestione delle informazioni sensibili, nella segnalazione degli incidenti di sicurezza e nel rispetto dei requisiti normativi. Inoltre , risulta fondamentale allineare la strategia con il business e cercare di integrare la sicurezza in tutti gli aspetti del business, i.e.: dalla gestione degli acquisti allo sviluppo del prodotto e al servizio clienti.
- **Formazione e consapevolezza -** La formazione sulla consapevolezza della sicurezza è essenziale per aiutare i dipendenti, i collaboratori e i partner a comprendere sia i propri ruoli sia le responsabilità in materia di sicurezza. Una formazione continua, non un evento una tantum per ottemperare alle normative, considerando che sessioni di formazione regolari sulle migliori pratiche di sicurezza aiutano i dipendenti a comprendere i rischi e le conseguenze delle violazioni della sicurezza e promuovono una cultura orientata alla sicurezza.
- **Stakeholder interni -** Quando si tratta di sicurezza, è essenziale conoscere i propri stakeholder interni. Diverse funzioni possono avere diverse preoccupazioni in materia di sicurezza. Pertanto, sapere con chi stai parlando, comprendere le loro esigenze specifiche e i loro problemi risulta quanto mai strategico e fondamentale nella predisposizione dei messaggi e delle iniziative rivolte a tali interlocutori in modo che possano rimanere coinvolti e informati.
- **Preparazione -** La resilienza è la capacità di resistere e riprendersi da un attacco informatico. Richiede una combinazione di misure tecniche e organizzative, come backup, ridondanza, piani di ripristino da disastri e procedure di risposta agli incidenti. Una solida cultura della sicurezza promuove la resilienza attraverso la promozione di una mentalità di prontezza e la simulazione di scenari di ciò che potrebbe accadere durante un vero attacco informatico, grazie alla disponibilità di dati e cruscotti intelligenti.
- **Fiducia digitale -** Costruire fiducia digitale significa garantire ai clienti, ai partner e ad altri stakeholder che l'organizzazione può mantenere al sicuro i loro dati e proteggere la

loro privacy. Per fare ciò, le organizzazioni devono essere trasparenti e responsabili nell'uso dei dati delle persone e rispettare leggi e regolamenti come GDPR. Avere una solida cultura della sicurezza è un modo per promuovere un comportamento etico e il rispetto della privacy, che può contribuire a costruire fiducia digitale.

- **Politiche semplici -** Le politiche di sicurezza guidano una parte importante della cultura della sicurezza. Le politiche e procedure di sicurezza dovrebbero essere chiare, collaborative e accessibili a tutti i dipendenti. Tutti dovrebbero sapere cosa ci si aspetta da loro e le conseguenze in caso di mancato rispetto.
- **Creazione di una community di campioni della sicurezza -** I team di sicurezza di solito hanno un numero limitato di membri. Pertanto, riunendo un gruppo di persone dedicate provenienti da diverse squadre e background, può favorire un senso di comunità che sostiene e favorisce, da parte di tutti, la priorità alla sicurezza e la creazione di un ambiente sicuro.
- **Monitoraggio, misurazione e reporting -** Monitorare e misurare l'efficacia delle iniziative della cultura della sicurezza è essenziale. Pertanto, è quanto mai necessario effettuare regolari sondaggi e valutazioni per valutare le conoscenze e il comportamento dei dipendenti e utilizza i risultati per individuare eventuali aree di miglioramento, oltre a condividere queste metriche con i principali stakeholder per dimostrare il ritorno sull'investimento del programma e utilizzare i risultati per identificare eventuali aree che necessitano di ulteriore supporto.
- **Cultura di consapevolezza positiva sulla sicurezza -** Una cultura della sicurezza efficace non dovrebbe essere basata sulla paura o su un approccio punitivo. È possibile valutare se una cultura della sicurezza è positiva osservando come i dipendenti interagiscono con il team responsabile della sicurezza. È importante riconoscere e premiare i dipendenti che dimostrano comportamenti corretti in materia di sicurezza, ad esempio segnalando incidenti o preoccupazioni sulla sicurezza. Questo riconoscimento può assumere diverse forme, come un apprezzamento pubblico o un piccolo bonus, e contribuisce a promuovere una cultura della sicurezza consapevole e impegnata.

Conclusione

Le organizzazioni, per trarre valore dai dati e dalle numerose tecnologie dell'IA e garantire la cyber resilience, devono affrontare sfide relative alle persone, ai processi e alla tecnologia. È fondamentale capire come ottimizzare l'utilizzo dell'IA, considerandola come un costrutto umano che richiede l'analisi e la valutazione delle scienze umane. Questo implica l'applicazione di un approccio etico nello sviluppo delle intelligenze artificiali, mantenendo l'uomo al centro dei processi decisionali al fine di contrastare l'algocrazia.

Stiamo vivendo una vera e propria trasformazione a causa dell'accelerato processo di digitalizzazione e innovazione in corso. I Big Data elaborati dalle piattaforme di IA sempre più strutturate offrono la possibilità di gestire non solo i rischi, ma anche la continuità operativa, la cybersecurity, la governance e la compliance grazie a cruscotti appositamente progettati. Questo crea nuove opportunità e servizi di risk management, risk engineering,

business continuity e cybersecurity per prevenire le perdite e garantire una resilienza operativa strategica in un mondo sempre più digitalizzato e incerto.

In conclusione, dobbiamo sfruttare la tecnologia in progress e i dati a nostra disposizione per potenziare la crescita, l'innovazione, l'efficienza, la resilienza e la competitività dell'organizzazione, mantenendo sempre un approccio risk-based e resilience-based. Il nostro chiodo fisso deve essere uno: anticipare l'inaspettato.

Intervista a Paola Girdinio, Presidente del Centro di Competenza START 4.0 e approfondimento su "*Fattore umano: le sfide metodologiche legate alle competenze e alla consapevolezza*"

Riproponiamo, in questa edizione del Rapporto, la sezione dedicata agli attori istituzionali (Autority, Agenzie, Forze dell'Ordine e Centri di Competenza) con cui il Clusit ha stretto accordi operativi per diffondere la cultura della sicurezza informatica presso le Aziende, la Pubblica Amministrazione e i cittadini.

Abbiamo quindi intervistato la **Prof.ssa Paola Girdinio, Presidente del Centro di Competenza START 4.0**, che si è prestata a rispondere alle nostre domande.

Cos'è il Centro di Competenza START 4.0?
Il Centro di Competenza START 4.0 è un partenariato pubblico-privato con sede a Genova, istituito nel 2019 come uno degli 8 Centri nazionali nell'ambito del Piano Industria 4.0, supporta la crescita e la competitività delle imprese italiane e il livello di digitalizzazione del Paese.
Siamo diventati un punto di riferimento per la transizione sostenibile e digitale di imprese e Pubbliche Amministrazioni, con un focus tecnologico sulla sicurezza fisica e cyber in vari ambiti tra cui porti, filiera della logistica, infrastrutture critiche e città.

Quali sono i principali campi di attività del Centro?
Le attività del Centro si articolano con l'erogazione di servizi, a partire da *test before invest* di tecnologie avanzate, la formazione e aggiornamento professionale certificato su temi cruciali come la cybersecurity, sia IT che OT, e le tecnologie 4.0, coinvolgendo dipendenti di grandi imprese, PMI e enti pubblici, la consulenza per la progettazione dell'innovazione, lo scouting di bandi e il supporto all'accesso ai finanziamenti.
Il Centro di Competenza, inoltre, partecipa a importanti iniziative nazionali e internazionali ed eroga contributi finanziari per progetti di innovazione tramite bandi, contribuendo così al co-finanziamento di progetti di valore significativo, con un focus su tecnologie chiave come Intelligenza Artificiale, 5G, Machine Learning, Big Data, IoT e cybersecurity.

Perché oggi è fondamentale la trasformazione digitale del nostro Paese in particolare per le Industrie e le infrastrutture critiche?
Secondo l'analisi DESI 2022 su 27 Paesi membri UE, l'Italia si piazza al diciottesimo posto per livello di digitalizzazione complessiva, questo dato già dice tanto di quanto sia importante la digitalizzazione nel nostro Paese e di quanta strada si debba fare. La trasformazione digitale sostiene la competitività e favorisce l'agilità e la resistenza a eventuali crisi, innalzando i livelli di efficienza e produttività, aggiornando non solo i propri modelli di business ma anche quelli formativi.
Tra i pilastri dell'attività di Start 4.0 infatti, c'è proprio quello della formazione, con l'at-

tenzione alle sia alle *soft* che alle *hard skills* di operatori, imprenditori e mondo economico per creare le condizioni di un upgrade sui temi 4.0 con particolare attenzione a quelli della cybersecurity.
La digitalizzazione diventa fondamentale anche per le infrastrutture, con l'obiettivo di migliorare per esempio la gestione dei nodi intermodali, la sicurezza stradale, visto il crescente numero di vittime e i target europei da rispettare, ma anche la qualità dei viaggi sia per la mobilità delle persone che delle merci.
La digitalizzazione delle infrastrutture critiche in particolare diventa strategica per raggiungere obiettivi come quello della transizione energetica, attraverso una rete di distribuzione dell'energia più efficiente.

In che modo START 4.0 contribuisce alla realizzazione del Piano Nazionale di Ripresa e Resilienza (PNRR)?
Start 4.0 è soggetto attuatore del PNRR e attraverso le determinazioni del MIMIT disporrà dei finanziamenti del Piano (11, 8 milioni) innanzitutto per erogare servizi agevolati e gratuiti alle imprese, assorbendo il costo dei servizi stessi, ampliando anche il catalogo con nuovi verticali tecnologici e nuove opportunità per le imprese. Inoltre, potrà potenziare infrastrutture e laboratori, co – finanziare progetti di innovazione delle imprese, supportare e accompagnare il tessuto imprenditoriale in complessi progetti di innovazione e favorire lo scouting e l'accesso ai finanziamenti nazionali ed europei.

START 4.0 ha recentemente aderito al Clusit. Quali scenari e opportunità apre questa collaborazione?
Intanto, voglio dire che per me questa collaborazione è motivo di orgoglio e rappresenta la chiusura di un cerchio. Il Clusit è l'associazione di riferimento per la sicurezza informatica e io da sempre, nei numerosi convegni o in aula con gli studenti, utilizzo i rapporti annuali nelle mie presentazioni. Dati chiari, verificati e credibili. Il Clusit è una garanzia e portare il Centro di Competenza Start 4.0 ad aderire è una grande opportunità. Gli obiettivi sono quelli di favorire la formazione e orientamento delle imprese (grandi e piccole) attraverso percorsi che accrescano la consapevolezza dei rischi cyber, considerando l'incessante crescita globale degli attacchi. La nostra sinergia può mettere a fattor comune competenze e risorse nell'ambito della strategia nazionale per la sicurezza informatica.

Fattore umano: le sfide metodologiche legate alle competenze e alla consapevolezza

[A cura di Paola Girdinio e Georgia Cesarone, START 4.0]

Il fattore umano continua a rappresentare l'anello debole della catena di protezione in ambito cybersecurity.
Secondo il report "ENISA Threat Landscape 2023" pubblicato il 19 ottobre 2023, il 74% delle violazioni ha coinvolto l'elemento umano (dati Verizon). Il dato confortante è che sia gli errori umani che quelli di sistema sono diminuiti raggiungendo gli stessi numeri osservati nel 2020, ma raggiungono comunque il terzo posto tra le minacce più pericolose. Verizon ha osservato che il 50% dell'ingegneria sociale si basa sul pretesto, che passa dalla paura e dall'urgenza alla costruzione di una storia verosimile e realistica creando un falso senso di fiducia.
Sulla base di questi dati, è evidente perché la sicurezza delle aziende e di tutti gli enti passi per una formazione metodologicamente e strategicamente strutturata e gestita come un vero e proprio asset aziendale. Perché il fattore umano lo è ed è sicuramente l'asset più rilevante di ogni realtà.
Il Centro di Competenza START 4.0 ha elaborato una metodologia denominata **Behaviour-based Cybersecurity Training** (BbCT) che utilizza per tutti i progetti formativi in ambito Cybersecurity Awareness. La BbCT prende spunto dallo studio dei comportamenti e si basa sull'evoluzione in ambito cyber security e cyber safety degli studi scientifici avviati nei primi anni '70 sugli effetti positivi di *feedback* e *rinforzi*.
L'analisi comportamentale applica i principi e le leggi della scienza del comportamento, attraverso l'applicazione di un rigoroso metodo scientifico, ai problemi legati alla sicurezza nella vita lavorativa di tutti i giorni (che si applicano ugualmente alla vita privata di ciascuno di noi).
La BbCT, sfruttando le conoscenze raggiunte dalle scienze comportamentali e applicandole ai contesti della Cyber Security e della Cyber Safety, cerca di anticipare le reazioni degli utenti posti di fronte a stimoli elaborati secondo le tecniche più avanzate di social engineering.
Il modello di riferimento è quello delle conseguenze del comportamento antecedente (anche denominato Modello ABC) uno strumento che aiuta ad esaminare un comportamento per comprenderne meglio le componenti chiave, inclusi gli eventi scatenanti che lo precedono e le conseguenze che ne seguono.
Questo consente anche di indagare come mai, in determinate circostanze, non venga messo in atto un comportamento adeguato impostando strategie correttive che si fondano sull'attivazione e sulla valorizzazione del potenziale delle persone, ultimo baluardo di difesa in caso di attacco non filtrato dai sistemi di protezione.
Essendo una metodologia data-driven, la BbCT si basa sulla raccolta di informazioni tramite una piattaforma di formazione correttamente configurata atta ad individuare le aree aziendali che necessitino di miglioramento, effettuare misurazioni oggettive e proporre azio-

ni formative che si concentrino più sugli aspetti cognitivo-comportamentali che su aspetti legati alle competenze.
Il tutto avendo cura di creare un ambiente in cui il feedback dell'utente sia il vero scopo finale da raggiungere e l'attivazione dello stesso venga percepito come l'elemento utile e benefico alla salvaguardia della realtà in cui è inserito. È dimostrato, infatti, che l'effetto dei rinforzi positivi porti ad interiorizzare il comportamento desiderato assicurandone l'attivazione in modo stabile e duraturo nel tempo.
Dal punto di vista operativo, un progetto formativo di Cybersecurity Awareness prevede 3 principali macro-fasi di attività che seguono il ciclo: valutare, istruire, rinforzare, misurare con modalità, tempi ed obiettivi differenti:

- le campagne di attacchi simulati comprendono attacchi di phishing, smishing, vishing e con dispositivi fisici che preparano le persone a identificare, gestire e segnalare ogni anomalia che potrebbe essere sintomo di un attacco e quindi cambiare nel tempo il comportamento delle persone nei riguardi di richieste o di dispositivi sospetti e a segnalarle ai propri riferimenti aziendali;
- le campagne di assessment che valutano la consapevolezza degli utenti attraverso domande finalizzate non tanto alla valutazione delle competenze acquisite dagli utenti quanto alla fragilità degli stessi nei confronti di tecniche di social engineering;
- le campagne di formazione si compongono di moduli interattivi grazie ai quali è possibile informare i dipendenti sulle possibili minacce relative alla cybersicurezza sul posto di lavoro.

I moduli vengono assegnati al singolo discente in funzione dei risultati delle diverse fasi di progetto rendendo il progetto formativo individuale e personalizzato anche in aziende con migliaia di dipendenti, come richiesto dalle migliori metodologie didattiche e con specifici KPI da raggiungere nelle varie fasi progettuali.
Le attività formative evolvono nel tempo sia dal punto di vista contenutistico che dal punto di vista strategico (forma/impostazione) seguendo il piano di progetto definito dal cronoprogramma che viene aggiornato sulla base dei risultati delle campagne.

La ricaduta più evidente di un progetto di Cybersecurity Awareness è la ricaduta personale che questo tipo di formazione ha nella vita privata dei partecipanti. Il cambio di comportamento, infatti, non avverrà solo in azienda, ma produrrà attenzione e consapevolezza nella vita privata degli utenti, molto più esposta agli attacchi cyber poiché priva dei sistemi di protezione aziendale.

Essendo la Cybersecurity un mondo molto complesso in generale, dal punto di vista formativo essa amplifica le sfide presenti nel mondo della sicurezza. Per questo START 4.0 ha costruito, oltre alla metodologia BbCT per la Cybersecurity Awareness, anche piani formativi verticali che insistono sulle competenze specialistiche ed avanzate, affrontando la tematica a tutti i livelli e per ogni mansione aziendale con obiettivi e metodologie differenti.

Ad esempio, per le mansioni apicali è fondamentale e non più rimandabile la conoscenza e la gestione della governance dei processi legati alla cybersicurezza all'interno di un quadro normativo internazionale ed europeo in continua evoluzione che prevede opportunità e rischi con un impatto diretto sul business aziendale e sui settori di riferimento.

Così come deve essere specialistica e approfondita la formazione e l'aggiornamento continuo di IT Manager e CISO (Chief Information Security Officer) su tecnologie e strumenti di analisi e protezione in continua evoluzione che molto spesso richiedono la conoscenza complementare di diverse tecnologie abilitanti, basti pensare alla convergenza dei mondi OT e IT, all'introduzione di dispositivi IoT con una pluralità di protocolli di connettività o alle nuove applicazioni di machine learning e intelligenza artificiale alla cybersecurity.
Vista la competenza rilevante del Centro di Competenza sulle infrastrutture strategiche, per coloro che si occupano di infrastrutture critiche sono stati sviluppati piani formativi ad hoc sulla cybersecurity IT/OT/IoT su ambiti settoriali specifici quali reti e centrali elettriche, ferrovie, porti, monitoraggio di infrastrutture civili, ospedali, ecc. che necessitano di programmi personalizzati dedicati e dettagliati.

Da notare che la metodologia formativa è strettamente dipendete dal target, cui sono associati gli obiettivi che abbiamo esplicitato: lezioni in presenza e da remoto, formati ibridi sincroni e asincroni, attacchi simulati e laboratori tecnici che si appoggiano sui nodi infrastrutturali e sui laboratori di START 4.0 con simulatori avanzati di reti elettriche e di componentistica elettronica. Una menzione speciale sull'uso di realtà aumentata e virtuale per contesti critici e strettamente legati ad esempio alla cyber safety e alla gestione di incidenti su cui START 4.0 sta sviluppando un'esperienza significativa grazie ai suoi partner tecnici di rilevanza internazionale.

Tutto concorre, con forme e metodologie didattiche avanzate basate sui paradigmi 4.0, a creare una nuova competenza e consapevolezza nell'ambito della sicurezza a tutto tondo e nella cybersecurity in particolare grazie alla quale contribuire alla messa in sicurezza del nostro paese e della risorsa più importante che abbiamo: le persone!

GLOSSARIO

Account hijacking	Compromissione di un account ottenuta ad esempio mediante *phishing*.
Account take-over	Acquisizione illecita di un account al fine di impersonificare la vittima (ad esempio di effettuare transazioni finanziarie sui suoi conti).
ACDC (Advanced Cyber Defence Center)	Progetto europeo la cui finalità è offrire soluzioni e creare conoscenza per aiutare le organizzazioni in tutta Europa a combattere le botnet. (www.acdc-project.eu/).
Adware	Tipo di *malware* che visualizza pubblicità solitamente senza il consenso dell'utente. Può includere funzionalità *spyware*.
AISP (Account Information Service Provider)	Prestatori di servizi di informazione sui conti di pagamento che forniscono ai clienti che detengono uno o più conti di pagamento online presso uno o più Istituti di Credito, servizi informativi relativi a saldi o movimenti dei conti aperti.
Altcoins (Alternative coins)	Criptovalute di seconda generazione. Spesso implementano funzioni o caratteristiche aggiuntive a quelle originariamente ipotizzate dai creatori di Bitcoin. Tra esse vi sono un maggior livello di anonimato o la non tracciabilità delle transazioni (Monero, Zcash, DeepOnion), la possibilità di generare e gestire *smart contract* o creare token di sviluppatori terzi ospitati sulla medesima *blockchain* (Ethereum, NEO, Stratis), l'aumento della velocità dei trasferimenti e della scalabilità del sistema (Ripple, Stellar Lumens), nonchè la predisposizione per l'utilizzo tramite dispositivi dell'Internet of Things (IOTA).
Analytics-As-A-Service	Servizi on demand per l'analisi di dati utilizzabili anche nell'ambito della sicurezza, ad esempio, per passare al setaccio i dati della rete aziendale e individuare eventi anomali ed eventuali attacchi.

Apt (Advanced Persistent Treath)	Schemi di attacco articolati, mirati a specifiche entità o organizzazioni contraddistinti da: • un accurato studio del bersaglio preventivo che spesso continua anche durante l'attacco • l'impiego di tool e malware sofisticati • la lunga durata o la persistenza nel tempo cercando di rimanere inosservati per continuare a perpetrare quanto più possibile il proprio effetto.
Arbitrary File Read	*Vulnerabilità* che consente ad un attaccante di accedere a file tramite richieste Web remote.
Attacchi Pivot back	Tipo di attacco nel quale viene compromessa una risorsa nel public cloud per ottenere informazioni che possono poi essere usate per attaccare l'ambiente on premise.
Backdoor	Soluzione tecnica che consente l'accesso ad un sistema superando i normali meccanismi di protezione.
BCP (Business Continuity Plan)	Documenti che riportano le soluzioni di preparazione e recovery messe in atto dalle aziende.
BEC fraud (Business e-mail compromise)	Tipi di attacco phishing mirati verso figure aziendali al fine di convincere le vittime a trasferire somme di denaro o rilevare dati personali. (Vedi anche CEO fraud)
BIA (Business Impact Analysis)	Tecnica di valutazione delle conseguenze sul business di un'organizzazione (economiche, reputazionali, legali…) di interruzioni derivanti da vari scenari avversi (indisponibilità del sistema informativo o parte di esso, indisponibilità del personale, indisponibilità dei locali…).
Blocj	Tecnica utilizzata nell'ambito dell'*e-voting*. Con la firma elettronica cieca (blind signature) la preferenza espressa dall'elettore viene cifrata. Successivamente viene apposta la firma elettronica da un ufficiale elettorale, che autentica il voto e infine si ha il deposito nell'urna.
Blockchain	Tecnologia che consente la registrazione di transazioni, in uno scenario trustless, fra gli attori della stessa blockchain mediante l'utilizzo di un registro digitale immodificabile presente su vari nodi della rete, costituito da blocchi (block) fra loro concatenati (chain).
Booter-stresser	Strumenti a pagamento che consentono di scatenare attacchi *DDOS*.

Botnet	Insieme di dispositivi (compromessi da *malware*) connessi alla rete utilizzati per effettuare, a loro insaputa, un attacco ad esempio di tipo *DDOS*.
Buffer overflow	Evento che ha luogo quando viene superato il limite di archiviazione predefinito di un'area di memorizzazione temporanea.
Business continuity	Soluzioni di natura tecnica ed organizzativa predisposte per garantire la continuità dell'erogazione di un servizio (eventualmente con uno SLA ridotto).
BYOD (Bring You Own Device)	Politica che consente l'uso di dispositivi personali anche per finalità aziendali.
CAL (Cybersecurity Assurance Level)	Indicatore dinamico dello sforzo necessario per garanzia la sicurezza di un elemento, derivante dai rischi relativi a tutti i suoi asset.
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.

CFC (Cyber Fusion Center)	Approccio olistico e multidisciplinare alla gestione della sicurezza che mira a superare la tradizionale suddivisione fra compiti (intelligence, analisi, risposta…) e team.
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.
CLOSINT (Close Source Intelligence)	Processo di raccolta di informazioni attraverso la consultazione di fonti chiuse, cioè non accessibili pubblicamente: intelligence feed, fonti governative, informazioni classificate, etc.
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.
CNP (Card-Not-Present)	Indica un pagamento effettuato senza la presenza fisica di una carta di pagamento, ad esempio su Internet.
CoA (Courses of Action)	Nella dottrina militare identifica un piano che descrive le strategie e le azioni operative scelte per portare a termine una determinata missione. Nell'ambito della *Cyber Intelligence* rappresenta le attività poste in essere rispettivamente dagli attaccanti o dai difensori per la conduzione o il contrasto delle azioni funzionali ad un attacco cyber.
Cognitive Security	Applicazione all'ambito della sicurezza delle soluzioni di Cognitive Computing.
Constituency	Nell'ambito di un *CERT* indica a chi è rivolto il servizio (ad esempio Pubblica Amministrazione Centrale, Regioni e Città metropolitane).

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.
Counterintelligence	Identificazione, valutazione, neutralizzazione e sfruttamento delle attività di intelligence svolte da entità avversarie.
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*).
Credential Stuffing	Attacco nel quale vengono utilizzate coppie di user id/password raccolte in precedenza in modo fraudolento.
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.
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.
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)
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 crime	Attività criminali effettuate mediante l'uso di strumenti informatici.
Cyber Diplomacy	"Incoraggiamo tutti gli Stati a impegnarsi in comportamenti rispettosi delle leggi e delle norme e che concorrano al rafforzamento della fiducia nel rispettivo uso delle TIC. Approcci collaborativi contribuirebbero anche a lottare contro l'uso del cyberspazio ad opera di attori non-Stato, a scopo terroristico e criminale". *(Dichiarazione del G7 sul comportamento responsabile degli stati nel cyberspazio) www.esteri.it/mae/resource/doc/2017/04/declaration_on_cyberspace_ita.doc*
Cyber espionage	Attività di spionaggio effettuata mediante l'uso di tecniche informatiche illecite.

Cyber intelligence	Attività volte a raccogliere e rielaborare informazioni al fine prevedere possibili minacce (non esclusivamente di natura informatica) agli asset oggetto di tutela.
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.
Cybersquatting	Attività volta ad appropriarsi di nomi di dominio di terzi, in particolare di marchi commerciali di rilievo, al fine di trarne profitto.
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-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).*
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.

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.
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)*
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.
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.

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*.
Diamond Model	Framework strutturato per l'analisi tecnica di possibili intrusioni. *(Adversary, Infrastructure, Victim, Capability).*
Digital Scarcity	In una blockchain la capacità di rendere non riproducibili informazioni digitali come file o pagamenti.
Directory Traversal	
DMARC (Domain-based Message Authentication, Reporting and Conformance	Standard di autenticazione delle e-mail che aiuta a prevenire la falsificazione del mittente (spoofing) e il phishing.
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 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.
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).
Double extortion	Attacchi ransomware che, oltre a cifrare i file, ne fanno anche una copia di "sicurezza" con il loro trasferimento sui computer dei cyber criminali minacciando di procedere alla loro diffusione pubblica e/o metterli all'asta nel dark web per la vendita al miglior offerente.
Downloader	Software deputati a scaricare ulteriori componenti malevoli dopo l'infezione iniziale.
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)
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.
Dropper	Codice che installa il *malware* sul computer della vittima.
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.
Enterprise Architecture	Sistema informativo che, raccogliendo dati da tutte le funzioni dell'organizzazione, li collega in un unico modello informativo consentendo di visualizzare complessivamente lo stato dell'organizzazione e contemporaneamente di immaginarne la possibile evoluzione futura, rinforzandone la capacità di reagire ad eventi esterni.
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).
Extended Vehicle	Tecnologia che consiste nel trasferire i dati di ogni veicolo, organizzati e strutturati, ai fini della loro condivisione, su dei server che rappresentano un'estensione, a terra, dei veicoli. Il concetto di "extended vehicle" è standardizzato dalla ISO 20077 "Road Vehicle - Extended Vehicle (ExVe) Methodology".
Fake news	Notizie destituite di fondamento relative a fatti od argomenti di pubblico interesse, elaborate al solo fine di condizionare l'opinione pubblica, orientandone tendenziosamente il pensiero e le scelte.
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).
Ghost broking	Pratica secondo la quale il frodatore, spacciandosi per agente di un'impresa assicurativa, a seguito del pagamento di un "premio" rilascia al cliente una polizza assicurativa, ovviamente falsa.

GRE (Generic Routing Encapsulation)	Protocollo di tunneling che incapsula vari protocolli di livello rete all'interno collegamenti virtuali point-to-point.
GSR (General Safety Regulation)	REGOLAMENTO (UE) 2019/2144 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 novembre 2019 relativo ai requisiti di omologazione dei veicoli a motore e dei loro rimorchi, nonché di sistemi, componenti ed entità tecniche destinati a tali veicoli, per quanto riguarda la loro sicurezza generale e la protezione degli occupanti dei veicoli e degli altri utenti vulnerabili della strada…
Hacktivism	Azioni, compresi attacchi informatici, effettuate per finalità politiche o sociali.
Hate speech	Il Comitato dei ministri del Consiglio d'Europa definisce gli hate speech come le forme di espressioni che diffondono, incitano, promuovono o giustificano l'odio razziale, la xenofobia, l'antisemitismo o più in generale l'intolleranza, ma anche i nazionalismi e gli etnocentrismi, gli abusi e le molestie, gli epiteti, i pregiudizi, gli stereotipi e le ingiurie che stigmatizzano e insultano. RECOMMENDATION No. R (97) 20 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES ON "HATE SPEECH" - Adopted by the Committee of Ministers on 30 October 1997
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.
IBAN Swapping	Sostituzione delle coordinate di pagamento IBAN o del wallet elettronico; questo ultimo caso soprattutto per i malware sui dispositivi mobili.
ICMP (Internet Control Message Protocol)	Protocolli che consentono ai dispositivi di una rete di comunicare informazioni di controllo e messaggi.
ICS (Industrial Control System)	Sistemi di controllo industriale.
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.

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.
Information warfare	Insieme di tecniche di raccolta, elaborazione, gestione, diffusione delle informazioni, per ottenere un vantaggio in campo militare, politico, economico…
Infostealer	*Malware* finalizzato a sottrarre informazioni, quali ad esempio credenziali, dal dispositivo infetto.
Instant 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.
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.
IoA (Indicatori di attacco)	Informazioni funzionali all'individuazione di un potenziale attacco anche prima che ci sia contatto diretto tra attaccante e attaccato.
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)
IP Fragmentation	Tipo di attacco DDOS (Destribuited Denial of Service) che sfrutta il principio di frammentazione del protocollo IP.

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.
Keylogger	*Malware* (o dispositivi hardware) in grado di registrare quello che la vittima digita sulla tastiera (o altrimenti inserisce), comunicando tali informazioni all'attaccante.
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.
Malvertising	Tecniche che utilizzano l'ambito della pubblicità on line come veicolo di diffusione di *malware*.
Malware	Definizione generica di applicazioni finalizzate a arrecare in qualche modo danno alla vittima (ad esempio raccogliendo o intercettando informazioni, creando malfunzionamenti nei dispositivi sui quali sono presenti, criptando i file al fine di richiedere un riscatto per renderli nuovamente intellegibili…).
Man in the browser	Tecnica che consente di intercettare le informazioni trasmesse dalla vittima, quali le credenziali di accesso al sito di una banca, al fine di poterle riutilizzare.
Memcached	Software spesso usato sui server web per effettuare caching di dati e per diminuire il traffico sul database o sul backend. Il server memcached è pensato per non essere esposto direttamente su Internet, per questo nella sua configurazione di default non richiede autenticazione e risponde sia via TCP che via UDP.

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)
OPSEC (Operation Security)	Processo mediante il quale, durante un'operazione di intelligence, si previene l'esposizione involontaria di informazioni sensibili/riservate/classificate riguardanti le proprie attività, intenzioni o capacità.
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.
OT (Operation Technology)	Componenti hardware e software dedicati al monitoraggio ed alla gestione di asset fisici in ambito industriale, trasporti…
OTP (One Time Password)	Dispositivo di sicurezza basato sull'uso di password utilizzabili per una sola volta, di norma entro uno spazio temporale limitato.
Payload	Letteralmente carico utile. Nell'ambito della sicurezza informatica è la parte di un *malware* che arreca danni.
Password hard-coded	Password inserite direttamente nel codice del software.
Pharming	Tecnica che consente di indirizzare la vittima verso un sito bersaglio simile all'originale (ad esempio un sito bancario) al fine di intercettare ad esempio le credenziali di accesso.
PHI (Protected Health Information)	Informazioni personali relative alla salute fisica o mentale di una persona fisica, comprese le relative valutazioni, cure… ed i relativi pagamenti, indipendentemente dalla forma o dal media utilizzato per la loro rappresentazione.
Phishing	Tecnica che induce la vittima, mediante una falsa comunicazione in posta elettronica, a collegarsi verso un sito bersaglio simile all'originale (ad esempio il sito di una banca) al fine di intercettare informazioni trasmesse, quali le credenziali di accesso.

Phone hacking	Attività di hacking che ha come oggetto i sistemi telefonici; ad esempio mediante l'accesso illegittimo a caselle vocali.
Ping flood	Attacco basato sul continuo ping dell'indirizzo della macchina vittima. Se migliaia e migliaia di computer, che fanno parte di una botnet, effettuano questa azione continuamente, la vittima esaurirà presto le sue risorse.
Ping of Death	Attacco basato sull'inoltro di un pacchetto di ping non standard, forgiato in modo tale da mandare in crash lo stack di networking della macchina vittima.
PIR (Priority Intelligence Requirements)	Requisiti informativi che orientano le priorità nella pianificazione delle attività di intelligence.
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.
Price tracer	Software di tracciamento dei prezzi.
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.
Retrieving data	Fase di ricerca e raccolta dei dati relativi all'obiettivo individuato durante un'attività *OSINT*. In questa fase gli analisti sfruttano i motori di ricerca, scandagliano i siti web alla ricerca di documenti di interesse avendo cura di conservare ogni traccia raccolta come ad esempio testi, URL, video, immagini, documenti, etc.
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.
SBOM (Software Bill of Materials)	Inventario "nested" di tutti i prodotti software e relativi componenti e fornitori presenti all'interno dell'azienda.
Scrubbing center	Letteralmente centro di pulizia. In uno Scrubbing center il traffico di rete viene analizzato e "ripulito" delle componenti dannose.

Security Architecture (NIST)	Insieme di rappresentazioni logiche e fisiche di un'architettura di sistema rilevanti dal punto di vista della sicurezza, che raccoglie le informazioni su come il complessivo sistema sia organizzato in domini di sicurezza, e ne fa uso per rinforzare le policy che prescrivono come dati ed informazioni debbano essere protetti all'interno di un dominio di sicurezza e nelle relazioni tra i domini.
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.

SMB (Server Message Block)	Protocollo per la condivisione di file e stampanti nelle reti locali. Se esposto su internet può essere utilizzato per accedere a documenti e file condivisi.
Smoking Guns	Termine che indica una prova (quasi) certa dell'aver commesso un crimine.
SOAR (Security Orchestration Automation and Response)	Approccio che consente di orchestrare le tecnologie di sicurezza al fine di avere una gestione il più possibile automatizzata della raccolta, analisi e risposta agli eventi di sicurezza.
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.
SOCMINT (Social Media Intelligence)	Ramo dell'Open Source Intelligence specificatamente dedicato alla raccolta di informazione attraverso i social network.
SOP (Standard Operating Procedure)	Procedure operative standard che indicano i passi da seguire durante la conduzione di indagini *OSINT*, consentendo di rendere efficiente l'esecuzione di operazioni ripetitive e di ottenere uniformità nelle prestazioni, nella qualità degli output ed evitando il mancato rispetto di standard e normative di settore, eventualmente imposte dalla propria organizzazione.
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.
TARA (Threat Analysis Risk Assessment)	Metodologia utile per dettagliare tutti i possibili threat a cui un prodotto può essere soggetto e assegnare un rischio basandosi su parametri, sempre descritti nello standard ISO/SAE 21434, che coprono l'ambito della safety, della privacy dell'utente, dell'impatto economico e dell'impatto sull'operatività del prodotto e del veicolo.
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 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.

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.
Telnet	Protocollo utilizzato per la gestione di host remoti, accessibile da riga di comando.
TLP (Traffic Light Protocol)	Protocollo per facilitare la condivisione delle informazioni "sensibili" che definisce il grado di possibile diffusione (red, amber, green, white) stabilito dalla controparte inviante.
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).
Tradecraft	Combinazione di metodi, capacità e risorse che un attaccante sfrutta nel compimento delle proprie azioni.
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.
UBA (User Behavior Analytics)	Tecnologia atta ad apprendere il "normale" comportamento degli utenti di un sistema informativo mediante l'analisi di rilevanti quantità di dati (log…), e di segnalare successivamente il verificarsi di attività anomale messe in atto dagli stessi.
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.
VNC (Virtual Network Computing)	Strumento di condivisione del desktop da remoto.
Vetting	Il processo di identificazione dei partecipanti ad una blockchain.

VHUMINT (Virtual Human Intelligence)	Estensione al mondo virtuale del concetto di Human Intelligence, cioè di una metodologia investigativa imperniata sulla raccolta di informazioni per mezzo di contatti interpersonali. Attraverso la VHUMINT vi è dunque l'interazione proattiva con gli attori della minaccia al fine di raccogliere informazioni di contesto necessarie a mitigare efficacemente la minaccia.
Vishing	Variante "vocale" del phishing.
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.
Wiper	Tipologia di virus che hanno come unico scopo quello di distruggere il sistema target (IT e OT).
XDR (Extended Detection and Response)	Dispositivi che integrano tutte le componenti della soluzione di sicurezza in un'unica piattaforma di individuazione (detection) e risposta agli incidenti (Incident Response) portando l'intelligenza di protezione fino al terminale del dipendente, sia esso un computer o uno smartphone.
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.
Zoom bombing	Irruzione virtuale in una videoconferenza finalizzata a creare disturbo.

Gli autori del Rapporto Clusit
Edizione ottobre 2023

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.

Lorenzo Beliusse, classe '78, nato a Busto Arsizio, dopo un diploma da perito informatico e una laurea in Information Technology presso l'Università degli studi di Milano, inizia un percorso che lo porta a maturare la consapevolezza che le idee, per trovare il giusto "spazio" nel mondo reale, hanno bisogno di un'attenta applicazione di metodi e tecniche di Management, senza tralasciare però l'aspetto più importante: l'engagement delle persone. Il suo viaggio all'interno dei progetti che vanno dalla Finanza al no-profit, lo portano infatti a comprendere come l'intelligenza emotiva (e lo sviluppo della competenza emotiva) sia una delle chiavi di volta per raggiungere l'eccellenza all'interno di team, aziende e organizzazioni. Consapevole che la creatività e la generazione di idee disruptive, sono il risultato di un lavoro collegiale, promuove le tecniche che incoraggiano il pensiero divergente quali il Think tank o i Sei cappelli per pensare. L'attenzione ai temi di comunicazione e al senso di community, lo portano, attraverso un percorso che passa dallo Storytelling in scuola Holden all'analisi di Bilancio, a occuparsi di uno degli incarichi più importanti per un'azienda: il Marketing. Riuscire ad "umanizzare" il volto di un marchio, è per lui uno degli aspetti strategici per il successo. Oggi è impegnato nel ruolo di Direttore Marketing di Reti S.p.A., B Corp e società benefit quotata su Euronext Growth Milan, una realtà ipertecnologica nel cuore di Busto Arsizio, che ha dato vita ad una vera e propria cittadella della tecnologia: Campus Reti. Questo è il luogo dove vengono coltivati i giovani talenti dell'Artificial Intelligence, della Data Science

e della Cyber Security, che diventeranno i protagonisti della trasformazione digitale del futuro. Appassionato di tecnologia e di tutto ciò che è figlio del progresso ricopre inoltre il ruolo di curatore TEDx.

Giancarlo Butti ha acquisito un master in Gestione aziendale e Sviluppo Organizzativo presso il MIP Politecnico di Milano. Referente ESG(*) e Inclusion del Comitato Scientifico del CLUSIT. Si occupa di ICT, organizzazione e normativa dai primi anni 80. Auditor, security manager ed esperto di privacy. Affianca all'attività professionale quella di divulgatore, tramite articoli, libri, white paper, manuali tecnici, corsi, seminari, convegni. Oltre 150 corsi e seminari tenuti presso ISACA/AIEA, ORACLE/CLUSIT, ITER, INFORMA BANCA, CONVENIA, CETIF, IKN, UNIVERSITA DI MILANO, CEFRIEL, ABI…; già docente del percorso professionalizzante ABI - Privacy Expert e Data Protection Officer e master presso diversi atenei. Ha all'attivo oltre 800 articoli e collaborazioni con oltre 40 testate. Ha pubblicato 25 fra libri e white paper alcuni dei quali utilizzati come testi universitari; ha partecipato alla redazione di 25 opere collettive nell'ambito di ABI LAB, Oracle Community for Security, Rapporto CLUSIT. Socio e già proboviro di AIEA è socio del CLUSIT e del BCI. Partecipa a numerosi gruppi di lavoro. Ha inoltre acquisito le certificazioni/qualificazioni LA BS7799, LA ISO/IEC27001, CRISC, CDPSE, ISM, DPO, CBCI, AMBCI.

(*) Già ricercatore nell'ambito delle energie rinnovabili (UNESCO - International directory of new and renewable energy information sources and research centers, 1986).

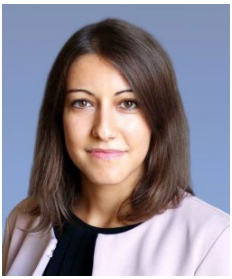
Georgia Cesarone, ingegnere elettronico con un master di secondo livello in Trasferimento tecnologico, Imprenditorialità e Innovazione nei settori dell'alta tecnologia, è innovation manager riconosciuto dal Ministero delle Imprese e del Made in Italy e PM certificato. Fondatrice di due start-up innovative, con un forte background nell'elettronica hardware e nella gestione di progetti di R&I, negli ultimi anni si è concentrata sull'introduzione delle tecnologie e lo sviluppo delle competenze che abilitano la trasformazione digitale sicura nelle aziende. È Responsabile Formazione e Innovazione del Centro di Competenza START4.0. È Consigliere Segretario dell'Ordine degli Ingegneri di Genova, Vicepresidente FIDA Inform (Federazione Nazionale delle Associazioni Professionali di Information Management) e Presidente del Club per le Tecnologie dell'Informazione CTI Liguria.

Mauro Cicognini, parte del team che ha fondato Rexilience nel 2021, si occupa di ICT dal 1989 e di cybersecurity dal 1996. Ha lavorato in aziende dei servizi e dell'alta tecnologia (software, systems integration, telecomunicazioni, automazione industriale), progettando e gestendo software, servizi e reti ICT in realtà che spaziano dalla multinazionale alla PMI. Le sue aree di responsabilità hanno toccato Europa, Africa, Sud America e Medio Oriente; parla inglese, italiano, spagnolo e francese. Interviene sui media nazionali e di settore, ed ha tenuto sessioni su IoT, sul GDPR, sulla Business Continuity, sulla sicurezza fisica, e così via. La sua attività convegnistica è rivolta sia agli specialisti di settore sia, a livello divulgativo, alle scuole ed alle iniziative civiche. Dal 2019 è docente presso il Cefriel – Politecnico di Milano nell'ambito del Corso di Alta Formazione per DPO. Ha fatto parte del Comitato Direttivo e poi del Comitato Scientifico di Clusit ininterrottamente dal 2006. Si è laureato nel 1995 al Politecnico di Milano in ingegneria elettronica (indirizzo bioingegneria), ed ha conseguito nel 2009 un "Executive Certificate in Management and Leadership" presso il Massachussetts Institute of Technology.

Alfredo Di Gennaro, laureato in Ingegneria Elettronica a Roma e con un Master in Gestione della Sicurezza per le Aziende e la Pubblica Amministrazione, lavora di oltre 25 anni nel campo della IT Security con trascorsi presso multinazionali del settore, come Symantec, McAfee, Trend Micro e Vodafone. Da 6 anni in Cisco si occupa di Progettazione di Architetture di Sicurezza per i grandi clienti Europei e del Middle East lavorando insieme ai grandi System Integrators e Service Providers per offrire soluzioni all'avanguardia che seguono le costanti evoluzioni del mercato. Pro-bono si occupa anche di diffondere nelle scuole tematiche difficili come la salvaguardia contro le pratiche sempre più diffuse del Cyber-Bullismo.

Aldo Di Mattia è entrato in Fortinet nel 2012 con il titolo di System Engineer per poi diventare nel 2018 Principal System Engineer & team leader, nel 2020 Manager Systems Engineering e nel 2022 Senior Manager Systems Engineering. Oggi è il responsabile di un team di sistemisti che supportano in tutta Italia le pubbliche amministrazioni centrali e locali, la difesa e le infrastrutture critiche. Nel 2005 si è laureato in informatica all'università La Sapienza di Roma con una tesi sperimentale sulla sicurezza di rete, lavorando tra il 2004 e il 2012 per due tra i più importanti System Integrator italiani nella sicurezza informatica in qualità di Systems Engineer, Security Consultant, Sr. Systems Engineer and Team Leader. In questi anni di lavoro ha maturato im-

portanti competenze ed esperienze nel settore, conseguendo nel tempo più di venticinque certificazioni specialistiche sui principali vendor di sicurezza informatica, la certificazione indipendente CISSP di ISC2 e ha depositato quattro brevetti con Fortinet presso USPTO (United States Patent and Trademark Office's) contenti innovazioni tecnologiche nella cybersecurity in relazione a: API Cooperation; End-point protection and smart working; Deception; SD-WAN.

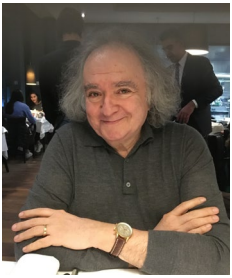


Giorgia Dragoni si è laureata nel 2014 in Ingegneria Gestionale al Politecnico di Milano e nello stesso anno ha iniziato a lavorare negli Osservatori Digital Innovation. Attualmente è ricercatrice sui temi della Cybersecurity & Data Protection e dei Big Data Analytics e Direttore dell'Osservatorio Digital Identity. Nel 2022 ha conseguito l'Executive Master in Management presso la Polimi GSoM. È membro del Comitato Scientifico del Clusit e delle Women for Security.

Gabriele Faggioli, legale, è amministratore delegato di Digital360 e di Partners4Innovation, Presidente del Clusit e Responsabile Scientifico dell'Osservatorio Cybersecurity & Data Protection del Politecnico di Milano. Gabriele è inoltre Adjunct Professor del MIP – Politecnico di Milano ed è stato membro del Gruppo di Esperti sui contratti di cloud computing della Commissione Europea. È specializzato in contrattualistica informatica e telematica, in information & telecommunication law, nel diritto della proprietà intellettuale e industriale e negli aspetti legali della sicurezza informatica, in progetti inerenti l'applicazione delle normative inerenti la responsabilità amministrativa degli enti e nel diritto dell'editoria e del markerting. Ha pubblicato diversi libri fra cui: "I contratti di cloud computing: Comprendere, affrontare e negoziare i contratti con i cloud" (Franco Angeli), "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.

Ivano Gabrielli, Laureato in Giurisprudenza e Scienze Politiche con il massimo dei voti, master in Scienze della Sicurezza e master in Homeland Security, è nella Specialità Polizia Postale e delle Comunicazioni dal 2006. Dopo 3 anni in forza al Compartimento Polizia Postale e delle Comunicazioni di Genova, dal 2009 è al Servizio Polizia Postale del Dipartimento della PS. Dal maggio 2012 è il Responsabile del Centro nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC). Dal luglio 2017 è il Direttore della III Divisione del Servizio Polizia Postale e delle Comunicazioni, a cui fanno riferimento il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche – CNAIPIC, la Sezione Cyber Terrorismo e la Sezione per il contrasto al Financial Cyber Crime e dal gennaio 2022 è Direttore Supplente del Servizio Polizia Postale e delle Comunicazioni.

Paola Girdinio è professore ordinario di elettrotecnica presso l'Università degli Studi di Genova, è stata preside della facoltà di ingegneria e membro del consiglio di amministrazione di Ateneo. È stata consigliere di amministrazione di Enel, di Ansaldo STS, , del Distretto ligure delle tecnologie marine, di Banca Carige, della società D'Appolonia, di Fondazione Carige, di Banca Popolare di Bari, ricopre attualmente analogo incarico in Ansaldo Energia, in Wsense, in Fondazione Costa Crociere e in Fondazione Amga. È presidente del Centro di Competenza sulla sicurezza e ottimizzazione delle infrastrutture strategiche 4.0 e presidente dell'Osservatorio Nazionale per la Cyber Security, Resilienza e Business Continuity dei Sistemi Elettrici. L'attività di ricerca di Paola Girdinio riguarda i settori della superconduttività applicata, dei materiali dielettrici a basse temperature, del calcolo di campi elettrici e magnetici con metodi numerici e della progettazione assistita da calcolatore di dispositivi elettrici e magnetici, compatibilità elettromagnetica industriale, cybersecurity per le infrastrutture.



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, membro del Comitato Direttivo di Clusit, è fondatore e senior partner di Rexilience. Già esperto di sicurezza cibernetica presso l'Agenzia per l'Italia Digitale/ CERT-AGID (2015-2020) con la responsabilità dello sviluppo del CERT della Pubblica Amministrazione, già membro (mandati 2010-12, 2012-15, 2015-17 e 2017-20) dell'Advisory Board dell'Agenzia dell'Unione Europea per la Cybersecurity (ENISA). In oltre 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. Ha collaborato per 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 partecipato a progetti internazionali di contrasto alla cybercriminalità e al cyberterrorismo con l'Ufficio delle Nazioni Unite per il Controllo della Droga e la Prevenzione del Crimine (UNODC) e l'Agenzia dell'Unione europea per la formazione delle autorità di contrasto (CEPOL). È docente in numerosi Master Universitari. 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. L'Università di Roma Tor Vergata gli ha conferito la laurea magistrale honoris causa in Ingegneria di Internet e delle Tecnologie per l'Informazione e la Comunicazione.

Pier Paolo Glave, laureato in Ingegneria Elettronica con indirizzo Reti di Telecomunicazioni al Politecnico di Milano, ha lavorato come Software Engineer e Architect nei settori delle telecomunicazioni e della TV digitale, collaborando con Italtel, Ericsson, Pirelli e Sky Italia. Si occupa di cybersecurity dal 2017, lavorando nel gruppo di Customer Success in Cisco. In questo ruolo, ha aiutato più di 100 grandi aziende in Italia e nel Sud Europa a migliorare la sicurezza delle loro infrastrutture, utilizzando e configurando al meglio soluzioni di protezione come firewall, network access control, EDR, XDR, sistemi di analisi di rete. Detiene certificazioni tecniche, tra cui CISSP, CCNP, ITIL. A titolo volontario ha collaborato con le scuole del territorio, per migliorare la sicurezza e la consapevolezza nell'uso di internet, insieme a Cisco e Telefono Azzurro. Dal 2023 è docente del corso di sicurezza informatica presso la UTE di Lainate.

Lorenzo Ivaldi, ingegnere elettronico e funzionario tecnico dell'Università di Genova è consulente in materia di sicurezza industriale. Oltre a svolgere attività di sistemista, esperto di sicurezza informatica ed informatico forense, è relatore in convegni e docente in master universitari negli stessi ambiti. È membro del comitato scientifico del Clusit.

Federica Maria Rita Livelli è in possesso della certificazione Business Continuity - AMBCI BCI, UK e CBCP DRI, USA, Risk Management FERMA Rimap ®. consulente di Business Continuity & Risk Management, svolge attività di diffusione e di sviluppo della cultura della resilienza presso varie istituzioni ed università. Inoltre ricopre il ruolo di Training Center Director in BeDisruptive. È membro del Board di ANRA, del Board del BCI Italy Chapter, del Comitato Scientifico di CLUSIT e di diverse Commissioni tecniche CLUSIT ed UNI. È membro del Conduct Professional Committee – BCI, UK e del Digital Committ di FERMA. Docente di moduli di introduzione di: ISO 22301 - Business Continuity & Resilience (Università POLIMI–BOCCONI e Università di Verona, Università di Cagliari, Master Ambientale Università di Padova, Università di Castellanza LIUC, Università di Genova); ISO 31000 - Risk Management (Università Statale di Milano e Università di Castellanza, LIUC). Inoltre, svolge attività di Docente rif. Moduli di Business Continuity, Risk Management, Cybersecurity & Supply Chain Resilience presso Università SUPSI, Lugano. È relatrice e moderatrice in diversi seminari, conferenze nazionali ed internazionali. Autrice di numerosi articoli su diverse riviste online, ha partecipato, in qualità di co-autrice, alle edizioni 2020, 2021, 2022 e 2023 del Rapporto Clusit, a libri tematici CLUSIT su Intelligenza Artificiale (2020), Rischio Cyber (2021) e Supply Chain Risk (2022) e al libro "Lo Stato in Crisi" ed. Angeli (2021).

Luca Nilo Livrieri è l'SE Manager di CrowdStrike per il Sud Europa. L'ingresso in CrowdStrike avviene nel maggio 2021, con la responsabilità di seguire lo sviluppo e la crescita della struttura di prevendita nel Sud Europa e Israel. Partecipa ormai da parecchi anni come relatore a diversi eventi nazionali e internazionali su privacy, sicurezza, cloud e digital transformation fra cui Security Summit, ISMS forum, IDC e Cybertech. Prima di Crowdstrike, Livrieri è stato manager per l'Italia, la Spagna e il Portogallo della struttura prevendita di Forcepoint. Ha maturato esperienze come membro dell' "Office of the CSO" e Senior SE per il mercato enterprise, e la formazione

e affiancamento del canale di rivendita in Websense e Surfcontrol. Prima di svolgere il ruolo di SE ha lavorato come consulente Gfi-Ois per la programmazione web presso alcune importanti aziende italiane. Precedentemente ha conseguito la Laurea magistrale in Comunicazione nella Società dell'Informazione, con tesi specialistica presso il dipartimento di informatica dell'Università Degli Studi Di Torino.

Giuseppe Massa rappresenta la Cybersecurity Governance di Cisco in Italia, come National Cybersecurity Officer ed è responsabile dei programmi di collaborazione, in ambito cyber, con ACN ed ENISA, con i Clienti Strategici e della Difesa. Laureato in Ingegneria Elettronica al Politecnico di Torino e specializzato in Telecomunicazioni, dopo un'esperienza da ricercatore sulle tecnologie xDSL e alcuni anni in Ericsson, è entrato in Cisco nel 1999. Ha ricoperto diversi ruoli nei gruppi tecnici di progettazione e prevendita in Cisco Italia e come manager in Cisco Olanda. È stato responsabile del primo progetto di Telefonia IP realizzato da Cisco in Italia nel 2000 e ha seguito la progettazione di oltre 600 reti e sistemi di telecomunicazione in Italia, Europa e Asia. Dal 2012 è specialista in Cybersecurity e nel corso della sua carriera ha conseguito diverse certificazioni tecniche, tra cui CISSP, ITIL, CCSP, CMNA.

Carlo Mauceli è National Digital Officer e National Security Officer della filiale italiana di Microsoft, con la responsabilità di promuovere l'innovazione del Paese, gestendo i rapporti con le government élites, i leader accademici e i decisori pubblici e contribuendo alla definizione di una politica tecnologica funzionale alla digitalizzazione del territorio. In qualità di National Security Officer, Carlo collabora con l'ACN, promuove la cultura della sicurezza e gestisce le crisi legate agli attacchi informatici. È membro del consiglio direttivo di Clusit.

Alessio L.R. Pennasilico, Information & Cyber Security Advisor, Security Evangelist, noto nell'hacker underground come -=mayhem=-, è internazionalmente riconosciuto come esperto dei temi legati alla gestione della sicurezza delle informazioni e delle nuove tecnologie. Per questa ragione partecipa da anni come relatore ai più rilevanti eventi di security italiani ed internazionali ed è stato intervistato dalle più prestigiose testate giornalistiche, radio e televisioni nazionali ed internazionali. All'interno di P4I, per importanti Clienti operanti nei più diversi settori di attività, sviluppa progetti mirati alla riduzione dell'impatto del rischio informatico/cyber sul business aziendale, tenendo conto di compliance a norme e standard, della gestione del cambiamento

nell'introduzione di nuovi processi ed eventuali tecnologie correlate. Credendo che il cyber risk sia un problema organizzativo e non un mero problema tecnologico, Alessio da anni aiuta il top management, lo staff tecnico e l'organizzazione nel suo complesso a sviluppare la corretta sensibilità in merito al problema, tramite sessioni di awareness, formazione e coaching. Alessio è inoltre membro del Comitato Scientifico di Clusit.

Pier Luigi Rotondo è Technical Specialist per le soluzioni di Threat Management di IBM Italia. Ha contribuito a molti progetti internazionali su soluzioni per il Threat Management, l'Identity e l'Access Management, il Single Sign-on, e la Threat Intelligence. Con una 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 e le tendenze del mercato della cyber security. È membro del Comitato Scientifico del CLUSIT.

Leonardo Sartore si è diplomato in "Industrial Cyber Security" presso l'ITS Academy Meccatronico Veneto nel 2022. Durante il conseguimento del titolo di studio, ha ricoperto il ruolo di Information & Cyber Security Analyst come tirocinante in un'azienda del settore manifatturiero. Attualmente lavora per Partners4Innovation ricoprendo il ruolo di Information & Cyber Security Advisor.

Sofia Scozzari, Appassionata di tecnologia da sempre, ha oltre 30 anni di esperienza nell'IT e 16 nella Cyber Security. Ha maturato esperienze come System Administrator, ICT Consultant, Project Manager, Pre-sale, Cyber Security Consultant e Manager per principali realtà Italiane e multinazionali. Da 5 anni risiede negli Emirati Arabi Uniti dove ha fondato e dirige Hackmanac, con cui elabora dati sulle minacce Cyber a supporto di attività di Threat Intelligence e Risk Management. È membro del Comitato Direttivo Clusit e di Women For Security. Fin dalla prima edizione nel 2011 contribuisce come co-autore al Rapporto Clusit, curando l'analisi di migliaia di attacchi informatici ogni anno e diversi approfondimenti verticali. È inoltre autrice di diversi articoli e guide in tema di Cyber Security, e co-autrice delle pubblicazioni

«Cybersecurity e IoT: come affrontare le sfide di un mondo connesso» (2022, Women For Security), «Blockchain & Distributed Ledger: aspetti di governance, security e compliance» (2019, CLUSIT) e «La Sicurezza dei Social Media» (2014, Oracle Community for Security). È infine speaker ad eventi e convegni di Cyber Security, sia in Italia che in UAE, e trainer in materia di Cyber Security Awareness.

Gaspare A. Silvestri è CEO di BearIT, professionista ICT con oltre 20 anni di esperienza nel settore come esperto di sicurezza informatica e infrastrutture critiche complesse in realtà *Enterprise* del panorama italiano e multinazionale, coinvolto in diversi progetti IT, tra cui la virtualizzazione e il consolidamento dei sistemi, *hardening compliance & risk management*, consulenza strategica sugli asset critici aziendali. Queste esperienze gli hanno permesso di ampliare la vision strategica fino al punto di realizzare quella che da sempre era un'idea, ossia quella di avere un'azienda che potesse mettere a disposizione del mercato principi di affidabilità e offerta tecnologica estremamente avanzata.

Claudio Telmon, Consulente sui temi di rischio e sicurezza ICT. Membro del Comitato Direttivo di Clusit. Senior Partner di Partners4Innovation.

Enzo Maria Tieghi, imprenditore, informatico, milanese, da oltre 30 anni si occupa di software per automazione e controllo di impianti, di security e compliance a standard e normative dei diversi settori industriali e delle infrastrutture in cui opera. È Amministratore Delegato di ServiTecno srl di Milano, Azienda che dal 1985 distribuisce e supporta software di GE Digital per sistemi OT industriale, SCADA, Industrial Internet, IIoT, Plant Intelligence, Analytics e tool per protezione di reti e sistemi nell'industria ed utility. Attivo in Associazioni di settore (quali AIIC, Clusit, CSA Cloud Security Alliance, ISPE, Anipla, ISA, AFI, Assintel, ecc.), tiene lezioni e partecipa come speaker ad eventi specialistici sia in Italia che all'estero, oltre a contribuire con articoli e memorie a riviste specializzate e conferenze internazionali. Autore del Quaderno Clusit "Introduzione alla protezione di reti e sistemi di controllo ed automazione (DCS,

SCADA, PLC, ecc.)", ha curato per Fondazione Amga ed Edizioni Franco Angeli l'edizione italiana del volume "SCADA Good Security Practices per il settore delle acque potabili" ed ha partecipato alla stesura del Rapporto Clusit 2012 sulla Sicurezza ICT in Italia e del ROSIv2. Attualmente in CLUSIT fa parte del Comitato Scientifico come referente della OT/IIoT Security, inoltre è socio AIIC, Senior Member di ISA e Senior Member ISPE, ove partecipa al GdL CyberSecurity di ISPE/GAMP Italia.

Anna Vaccarelli è Dirigente Tecnologo del Consiglio Nazionale delle Ricerche; responsabile delle Relazioni esterne, media, comunicazione e marketing del Registro .it, gestito dall'Istituto di Informatica e Telematica del Cnr. Dal 2010 coordina e promuove un'azione di diffusione della cultura di internet nelle scuole, con laboratori dalle primarie alle secondarie di secondo grado attraverso la Ludoteca del Registro .it. È tra gli ideatori di Internet Festival e coordinatore del Comitato Esecutivo del Festival. Fa parte del Comitato Direttivo di Women for Security dal 2020 e del Comitato direttivo del Clusit. È stata docente in corsi di Cybersecurity, responsabile scientifico di progetti nazionali e internazionali, coautore di oltre 100 pubblicazioni scientifiche e tecniche.

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. È membro del Comitato Scientifico del 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.

Clusit
Associazione Italiana per la Sicurezza Informatica

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 19a edizione.
- Le Conference specialistiche: i Security Summit Streaming Edition, i Security Summit On Site (a Milano, Roma, Cagliari e Verona), gli Atelier della Security Summit Academy, Le Tavole Rotonde Verticali (Energy & Utilities, Health Care, Finance, Manufacturing).
- I Gruppi di Lavoro della Clusit Community for Security.
- Rapporti Clusit: Rapporto annuale, con aggiornamento semestrale, sulla sicurezza ICT in Italia, in produzione dal 2012.
- Il Mese Europeo della Sicurezza Informatica, iniziativa di sensibilizzazione promossa e sostenuta ogni anno nel mese di ottobre in Italia da Clusit.

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, Autorità Garante per la tutela dei dati personali, Cyber 4.0 - il Centro di Competenza nazionale ad alta specializzazione per la cybersecurity, Start 4.0 - Centro di Competenza per la Sicurezza delle Infrastrutture Strategiche Digitali, 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 Cybersecurity), 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 2024

Per il 2024 sono previste delle edizioni tutte in presenza a Milano (19-20-21 marzo), Roma (19 giugno), Cagliari (in settembre) e Verona (in ottobre). Continueranno gli Atelier della Security Summit Academy, che si terranno tutto l'anno, e gli Eventi Verticali, programmati il 28 maggio (Energy & Utilities), 19 giugno (Healthcare), 24 ottobre (Manufacturing). L'anno sarà chiuso come sempre da una edizione interamente in streaming, a novembre.

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/

In collaborazione con

CROWDSTRIKE

Microsoft

SECURITY SUMMIT

www.securitysummit.it