Rapporto

2021

sulla sicurezza ICT
in Italia

Indice

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

Prefazione

Un anno fa in queste ore scrivevo la prefazione del Rapporto e riflettevo su quanto stava accadendo.
Era l'inizio del lockdown e l'esplosione della pandemia mondiale.
Scrivevo che quanto stava accadendo avrebbe portato alla comprensione dell'importanza del digitale.

Ed è quello che è accaduto.
Il digitale è diventato centrale per la sopravvivenza di aziende e pubbliche amministrazioni, per garantire un minimo di continuità alle attività scolastiche, per rimanere in contatto con amici e parenti.
Tanti, troppi casi di attacchi riusciti ci hanno anche permesso di riflettere ancora sulla importanza della sicurezza informatica. Non esiste digitalizzazione possibile senza sicurezza.

L'anno passato, con gli attacchi agli ospedali, ha reso ancora più evidente che i criminali non hanno alcuna remora, nessuna etica. Tutto quello che può essere fatto per ottenere denaro sarà fatto. Con buona pace dell'impatto degli attacchi sulla vita delle persone.
Abbiamo però anche assistito a un anno in cui nonostante il crollo epocale del PIL la spesa in sicurezza informatica è aumentata del 4%, con tante, tantissime aziende e pubbliche amministrazioni che hanno approfittato del lockdown per fare awareness e formazione in modalità remota anche sui temi della sicurezza cyber.
Abbiamo avuto l'occasione di avere ospiti e di interloquire più volte con le massime Autorità italiane ed europee del settore.

Si tratta del rovescio della medaglia della pandemia.

Pur nella tragedia degli oltre centomila morti solo in Italia, ci sono tante cose che sono state fatte per migliorare la vita delle persone e che hanno un valore immenso nel contesto in cui viviamo.
Si è scoperto che possiamo fruire di servizi che prima erano riservati a pochissimi in presenza.

Non so se il prossimo anno potremo fare un Security Summit incontrandoci nuovamente. Forse saremo ancora in modalità remota. Ma quello di cui sono sicuro è che quando si potrà di nuovo vedersi, lo faremo. Ma manterremo tante delle modalità che oggi stiamo scoprendo. Quanto valgono due ore non passate in macchina nel traffico in termini di attività che si possono svolgere?

Sfrutteremo tutti molto di più le tecnologie digitali rispetto al pre-pandemia.
E se sarà così, dobbiamo progettare un nuovo modo di vivere. Un modo di vivere in larga parte imperniato sul digitale che dovrà necessariamente essere progettato in modo sicuro.
Come CLUSIT, con il nostro nuovo Direttivo e il nuovo Comitato Scientifico, con la passione e la partecipazione di decine fra i più autorevoli esponenti del nostro settore, proveremo a fare la nostra parte.

*** *** ***

Il rapporto CLUSIT che leggerete è il frutto del lavoro di un pool di esperti che ha analizzato e confrontato una ampia serie di fonti. È forse inutile dire, come sempre, che l'ultimo anno è stato il peggiore di tutti. È il trend in atto da anni e non deve stupire. Forse una riflessione si può fare sull'aumento dei casi in Europa. È forse l'effetto degli obblighi di notifica dei data breach che permette l'emersione del fenomeno nella sua vera ampiezza?

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.
Quest'anno, peraltro, in un contesto di particolare complessità.

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 2021.
Oltre 70.000 copie scaricate e più di 300 articoli pubblicati nel 2020, sono l'evidenza della rilevanza del rapporto CLUSIT ed è quindi importante diffonderlo, leggerlo, farlo conoscere, perché solo dalla consapevolezza può derivare la conoscenza del problema, la capacità di adottare scelte idonee e quindi la sicurezza nostra e di tutti.

Buona lettura.

Gabriele Faggioli
Presidente CLUSIT

Introduzione al Rapporto

Il Rapporto CLUSIT 2021 inizia con una panoramica degli eventi di cyber-crime più significativi avvenuti a livello globale nel 2020, confrontandoli con i dati raccolti nei 4 anni precedenti. Nell'anno della pandemia si registra il record negativo degli attacchi informatici: a livello globale sono stati infatti **1.871 gli attacchi gravi di dominio pubblico** rilevati nel corso del 2020, ovvero con un impatto sistemico in ogni aspetto della società, della politica, dell'economia e della geopolitica. In termini percentuali, **nel 2020 l'incremento degli attacchi cyber a livello globale è stato pari al 12%** rispetto all'anno precedente; negli ultimi quattro anni il trend di crescita si è mantenuto pressoché costante, facendo segnare un aumento degli attacchi gravi del 66% rispetto al 2017. Proprio la **pandemia** ha caratterizzato il 2020 per andamento, modalità e distribuzione degli attacchi: il 10% degli attacchi portati a termine a partire da fine gennaio è stato a tema Covid-19. In particolare, i cybercriminali hanno sfruttato la situazione di disagio collettivo, nonché di estrema difficoltà vissuta da alcuni settori - come quello della produzione dei presidi di sicurezza (ad esempio, delle mascherine) e della ricerca sanitaria - per colpire le proprie vittime. Diverse operazioni di spionaggio sono state compiute a danno di organizzazioni di ricerca correlate con lo sviluppo dei vaccini. Nello specifico settore della **Sanità**, il 55% degli attacchi a tema Covid-19 è stato perpetrato a scopo di cybercrime, ovvero per estorcere denaro; con finalità di "Espionage" e di "Information Warfare" nel 45% dei casi. Gli attacchi registrati nel 2020 sono stati classificati anche in base ai loro differenti livelli di impatto, sulla base di una valutazione dei danni dal punto di vista geopolitico, sociale, economico (diretto e indiretto) e di immagine. Nel 2020 gli attacchi rilevati e andati a buon fine hanno avuto nel 56% dei casi **un impatto "alto" e "critico"**; il 44% è stato di gravità "media".

Tra i settori colpiti da attacchi cyber gravi negli ultimi dodici mesi, spiccano (in ordine decrescente): "**Multiple Targets**": 20% del totale. Si tratta di attacchi realizzati in parallelo verso obiettivi molteplici, spesso indifferenziati, che vengono colpiti "a tappeto" dalle organizzazioni cyber criminali, secondo una logica "industriale". Gli attacchi verso questa categoria di obiettivi sono tuttavia in calo del 4% rispetto al 2019; **Settore Governativo, Militare, Forze dell'Ordine** e **Intelligence**, che hanno subìto il 14% degli attacchi a livello globale; **Sanità**, colpita dal 12% del totale degli attacchi; **Ricerca/Istruzione**, verso cui sono stati rivolti l'11% degli attacchi; **Servizi Online**, colpiti dal 10% degli attacchi complessivi. Sono cresciuti, inoltre, gli attacchi verso Banking & Finance (8%), Produttori di tecnologie hardware e software (5%) e Infrastrutture Critiche (4%).
Abbiano inoltre registrato nel corso degli ultimi dodici mesi un incremento di attacchi veicolati tramite l'abuso della **supply chain**, ovvero tramite la compromissione di terze parti, il che consente poi a criminali e spie di colpire i contatti (clienti, fornitori, partner) dell'obiettivo, ampliando notevolmente il numero delle vittime e passando più facilmente inosservati. Nel 2020 gli attacchi cyber sono stati messi a segno prevalentemente utilizzando **Malware** (42%), tra i quali spiccano i cosiddetti **Ransomware** - una tipologia di malware che limi-

ta l'accesso ai dati contenuti sul dispositivo infettato, richiedendo un riscatto - utilizzati in quasi un terzo degli attacchi (29%), la cui diffusione è in significativa crescita (erano il 20% nel 2019), sia in termini assoluti che in termini di dimensioni dei bersagli e di ammontare dei danni. Seguono le "tecniche sconosciute" (in riferimento alle quali prevalgono i casi di Data Breach, per il 20%), mentre **Phishing & Social Engineering** continuano ad essere la causa di una buona parte degli attacchi (15% del totale); si registra inoltre negli ultimi dodici mesi una crescita degli attacchi sferrati per mezzo di vulnerabilità note (+ 10%), precedentemente in calo (-29% nel 2019 rispetto al 2018).

Ci siamo avvalsi anche quest'anno dei dati relativi agli attacchi rilevati dal **Security Operations Center (SOC) di FASTWEB**, che ha analizzato la situazione italiana sulla base di oltre 36 milioni di eventi di sicurezza.
Data la nuova crescita del fenomeno Ransomware, pubblichiamo un'analisi specialistica sul **Ransomware in Italia** e sugli attacchi mirati "double extortion", a cura di TG Soft.
Segue un'analisi sull'**Email Security** e sui trend italiani, a cura di Libraesva.

Anche in questa edizione riportiamo uno studio nuovamente realizzato da ricercatori dell'Università degli Studi di Bari e di Exprivia sullo **stato della cybersecurity nel sud d'Italia**.
L'analisi degli attacchi in Italia è poi completata dalle rilevazioni e segnalazioni della **Polizia Postale e delle Comunicazioni**.

Presenteremo a questo punto l'abituale capitolo dedicato al settore FINANCE, con un'analisi sugli "**Elementi sul Cyber-crime nel settore finanziario in Europa**", a cura di IBM ed un contributo inedito del CERT di Banca d'Italia.
Quest'anno abbiamo aggiunto un capitolo sulla **Supply Chain Security**, che comprende anche un contributo sulla maturità delle organizzazioni in Italia, a cura dell'**Osservatorio Cybersecurity & Data Protection della School of Management del Politecnico di Milano**.

Questi saranno infine i temi trattati nella sezione FOCUS ON:
- "**Ahi Ahi Ahi IoT!**", di Alessandro Vallega e Roberto Obialero.
- "**Attacchi e minacce alle Infrastrutture Critiche Italiane**", a cura di Fortinet.
- "**La metà dei CISO italiani crede che la guerra informatica sia una minaccia imminente per le loro aziende**", a cura di Bitdefender.
- "**La sicurezza dei dati Cloud nel 2020**", a cura di Netwrix.
- "**Business Continuity & Cyber Security: la necessità di un approccio convergente**", di Federica Maria Rita Livelli.

Panoramica dei cyber attacchi più significativi del 2020 e tendenze per il 2021

Introduzione alla decima edizione

In questa prima sezione del Rapporto CLUSIT 2021, giunto ormai al suo decimo anno di pubblicazione, analizziamo i più gravi cyber attacchi noti avvenuti a livello globale (Italia inclusa) negli ultimi 8 semestri[1] e li confrontiamo con l'analisi degli attacchi noti degli ultimi 12 mesi. Da quando nel lontano 2011 abbiamo iniziato a svolgere questa raccolta di "incidenti notevoli" di dominio pubblico abbiamo individuato, classificato e valutato quasi **12.000**[2] attacchi avvenuti tra il gennaio 2011 e il dicembre 2020 (dei quali **1.871** nel 2020).
A partire da questa significativa mole di dati proviamo a fornire un'interpretazione ragionata sull'evoluzione delle minacce cibernetiche nel mondo ed a delineare le tendenze in atto, volutamente espressa con un taglio divulgativo, in modo da risultare fruibile al maggior numero possibile di lettori.

Considerazioni sul campione

Per quanto le nostre analisi ed i relativi commenti si riferiscano ad attacchi *andati a segno*, che hanno cioè superato tutte le difese in essere provocando danni importanti (e non ad attacchi tentati e/o bloccati), il nostro campione è necessariamente *parziale* rispetto al numero degli attacchi gravi avvenuti nel periodo in esame.
Questo accade sia perché *un buon numero* di aggressioni non diventano *mai* di dominio pubblico, oppure lo diventano *ad anni di distanza* (solitamente quanto più gli attacchi sono sofisticati), sia perché in molti casi è interesse delle vittime non pubblicizzare gli attacchi subiti, se non costretti dalle circostanze o da obblighi normativi particolari[3].

Inoltre la natura giornalistica delle fonti pubbliche utilizzate per realizzare questo studio (notizie ricavate da testate specializzate ed agenzie di stampa online, blog, post su social media etc.) introduce inevitabilmente un *bias*[4] nel campione, all'interno del quale sono certamente

---

1 Confrontando i dati degli ultimi 4 anni, in questo caso dal 2017 al 2020

2 11.959 per la precisione

3 In merito a quest'ultima fonte di *disclosure obbligatoria* dobbiamo rilevare che, nonostante l'entrata in vigore del Regolamento GDPR e della Direttiva NIS, nel 2020 non abbiamo rilevato (come ci saremmo aspettati) un aumento significativo di attacchi gravi di pubblico dominio verso bersagli europei, il che alla luce dell'aumento degli attacchi gravi registrati a livello globale nel 2020 (+12% rispetto al 2019) appare statisticamente improbabile, portandoci a concludere che una quota significativa di questi attacchi *non siano ancora emersi*, nonostante gli obblighi di notifica vigenti.

4 https://it.wikipedia.org/wiki/Bias_(statistica)

meglio rappresentati gli attacchi più visibili, cioè solitamente quelli realizzati per finalità *cyber criminali* (o di *hacktivism*, anche se ormai in quantità residuale) rispetto a quelli derivanti da attività di *cyber espionage* ed *information warfare*, che per natura emergono più difficilmente.

In sintesi, considerato che il nostro campione è realizzato esclusivamente a partire da fonti aperte, e che al loro interno alcune classi di incidenti (tipicamente quelli potenzialmente più gravi) sono sistematicamente sottorappresentate, è plausibile supporre che questa analisi dipinga uno scenario *meno critico rispetto all'effettiva situazione sul campo*.

Origini ed evoluzione di questa analisi

Quando nell'ormai preistorico 2011 abbiamo iniziato questa ricerca, poi pubblicata nella prima edizione del Rapporto Clusit del 2012, definendo (ingenuamente, in retrospettiva) il 2011 come "l'Annus Horribilis della sicurezza informatica", gli scenari erano radicalmente diversi e gli impatti geopolitici e socioeconomici delle minacce cibernetiche rappresentavano ancora un problema relativamente minore, suscitando interesse e preoccupazione solo tra pochi esperti di ICT Security[5].
Lo scopo originario per il quale 10 anni fa è nato questo lavoro era dunque di elevare la consapevolezza del pubblico italiano rispetto all'evoluzione delle minacce cibernetiche, nell'ipotesi (poi dimostratasi drammaticamente esatta) che il problema sarebbe inevitabilmente degenerato con grande rapidità negli anni successivi, e che la pressoché totale mancanza di sensibilità in materia fosse *una delle principali ragioni* del peggioramento degli scenari.

Questa finalità rimane ancora oggi centrale, ma data la criticità della situazione che si è venuta a creare nel frattempo, e considerati i rischi sistemici, esistenziali che oggi incombono sulla nostra *civiltà digitale* a causa della crescita straordinaria delle minacce cibernetiche, siamo convinti che innalzare l'awareness del pubblico non sia più sufficiente, e che questa analisi debba continuare ad evolversi, trasformandosi da una semplice cronaca ragionata degli attacchi noti più significativi in un vero e proprio strumento di lavoro e di supporto decisionale.
Per questa ragione dal 2017 abbiamo introdotto un *indice della gravità degli attacchi analizzati*, classificandoli in base a tre livelli crescenti di "*Severity*", il che ci consente di realizzare inediti confronti e di offrire interessanti spunti di riflessione a coloro che si occupano di *threat modeling*, di *cyber risk management* e di *cyber strategy*, sia a livello aziendale che istituzionale, grazie ad una migliore "fotografia" dei rischi attuali resa possibile da questo ulteriore elemento di valutazione.

[5] Giova qui ricordare che all'epoca i rischi "cyber" non erano nemmeno menzionati all'interno del ***Global Risk Report*** del World Economic Forum, mentre dal 2019 sono assurti al primo posto per impatto e probabilità di accadimento, insieme ai disastri naturali ed agli effetti globali del ***climate change***.

Sempre nell'ottica di trasformare questa analisi in uno strumento di lavoro, a partire dal Rapporto Clusit 2022 introdurremo una nuova metodologia di classificazione, in particolare per quanto riguarda le vittime[6], in modo da rendere questi dati più facilmente confrontabili ed integrabili con altre fonti.

2021, "Rompere l'assedio"

Anche quest'anno il quadro che emerge dai dati è sconfortante: il 2020 è stato l'anno *peggiore di sempre* in termini di evoluzione e crescita delle minacce "cyber" e dei relativi impatti, evidenziando un trend persistente di aumento degli attacchi, della loro gravità e dei danni conseguenti.
Per sintetizzare in una frase il nostro giudizio in merito alla situazione, tre anni fa abbiamo commentato che il 2017 aveva rappresentato un "salto quantico" nei livelli di cyber-insicurezza globali, nel 2018 abbiamo insistito affermando che fossimo ormai giunti a "due minuti dalla mezzanotte" e infine nel 2019 abbiamo utilizzato l'espressione degli antichi cartografi "hic sunt leones", a significare di essere ormai giunti su un altro pianeta, in una terra incognita e pericolosa, popolata da mostri.
Quest'anno abbiamo deciso di non utilizzare alcuna frase ad effetto per commentare l'anno precedente, quanto piuttosto di provare ad immaginare cosa ci riservi il futuro se non invertiamo urgentemente la rotta.

I trend in sintesi

Osservando la situazione dal punto di vista quantitativo, la crescita degli attacchi gravi di pubblico dominio nel triennio 2018- 2020 è stata del **20%** (da 1.552 a 1.871).
La crescita registrata nel triennio 2015-2017 era stata "solo" del +11% (da 873 a 1.127), ovvero *nell'ultimo triennio il tasso di crescita del numero di attacchi gravi è quasi raddoppiato rispetto al triennio precedente*. Non solo, la Severity media di questi attacchi (indice che abbiamo introdotto dal 2017) è contestualmente peggiorata, agendo da moltiplicatore dei danni.
Al di là degli aspetti quantitativi, dal punto di vista qualitativo lo studio di diverse migliaia di attacchi degli ultimi 3 anni (5.093, quasi metà del totale del campione di 11.959 attacchi analizzati dal 2011) ci fa comprendere che si è prodotto un *cambiamento epocale* nei livelli globali di cyber-insicurezza, causato dall'evoluzione rapidissima degli attori, delle modalità, della pervasività e dell'efficacia degli attacchi. E' molto importante che si comprendano le implicazioni di questo fatto: il Cybercrime, il Cyber Espionage e l'Information Warfare del 2020 non sono certamente più quelli del 2015, anche se continuiamo ad utilizzare le stesse denominazioni.
Come previsto, nel 2020 si sono realizzate appieno le tendenze più pericolose già indivi-

[6] Per categorie merceologiche standard, in base a tassonomie riconosciute a livello internazionale.

duate a partire dal 2017-2018 (e proseguite nel 2019), che avevamo descritto come "l'anno del trionfo del malware, degli attacchi industrializzati realizzati su scala planetaria contro bersagli multipli da gruppi cybercriminali organizzati che guadagnano miliardi, dell'alterazione di massa della percezione e della definitiva discesa in campo degli Stati come attori di minaccia".
Queste dinamiche nell'ultimo triennio hanno causato conseguenze molto concrete, da un lato spingendo sempre più soggetti (statuali e non) ed entrare nell'arena, accelerando la "corsa agli armamenti" in atto ed esacerbando il livello dello scontro, e dall'altro impattando in modo ormai inequivocabile sulla società civile (singoli cittadini, istituzioni ed imprese), che sta *cambiando* in conseguenza di questa enorme pressione negativa (tipicamente non in meglio). Siamo cioè di fronte a fenomeni che per natura e dimensione ormai travalicano *costantemente* i confini dell'IT e della stessa cyber security, ed hanno impatti profondi, duraturi e sistemici su ogni aspetto della società, della politica, dell'economia e della geopolitica.
Per fare un esempio eclatante della *mutazione sostanziale dello spettro delle minacce cyber* avvenuta negli ultimi 3 anni, il Cybercrime, pur rappresentando senz'altro un problema enorme e facendo la parte del leone nel nostro campione dal punto di vista quantitativo (anche per le ragioni esposte nel capitolo precedente), ormai dal punto di vista qualitativo (ovvero della Severity, secondo la nostra analisi) è paradossalmente diventato *un rischio secondario,* nel senso che ormai ci troviamo a fronteggiare *quotidianamente* minacce *ben peggiori* (in particolare Espionage e Information Warfare), nei confronti delle quali le contromisure disponibili sono particolarmente inefficaci.

Sotto assedio

Dai tempi del "salto quantico" (nel 2017) gli attacchi gravi che abbiamo rilevato sono aumentati del **66%** (in 4 anni), e i danni globali causati dalle minacce cibernetiche rappresentano ormai una cifra enorme, pari se non superiore al PIL italiano (a seconda degli elementi considerati e di come vengono calcolati)[7].
Come esperimento mentale ipotizziamo che nel prossimo quadriennio il tasso di crescita dei danni non acceleri ulteriormente (come purtroppo i trend fanno sospettare) e rimanga costante, con una media del 15% all'anno. In questo scenario "neutro", nel 2024 i danni globali generati dalle varie tipologie di minacce cyber saranno complessivamente quasi il doppio di quelli attuali, cioè nell'ordine di grandezza del PIL della Germania, ovvero un quinto del PIL dell'Unione Europea. Detto diversamente, più di 500 dollari a testa all'anno per ogni essere umano (neonati e centenari inclusi), anche se ovviamente i danni saranno molto più concentrati nei paesi avanzati. Per l'Italia, in questo scenario, nel 2024 le perdite

[7] Per esempio questo report di McAfee stima 945 miliardi di dollari di perdite dovute al solo cybercrime, senza quindi considerare il furto di intellectual property dovuto ad attività di cyber intelligence economica, nè i costi legati alle conseguenze delle operazioni di psyops realizzate tramite fake news e disinformazione, con finalità politiche interne e geopolitiche https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf

potrebbero essere nell'ordine di grandezza dei 20-25 miliardi di euro[8].
Questi stime ad alto livello, per quanto impressionanti, naturalmente non possono rendere l'idea di quanto una singola azienda, una pubblica amministrazione o perfino una nazione possano ormai essere danneggiate se colpite direttamente da un cyber attacco, perchè ancora oggi, finchè non avviene un singolo incidente grave, risulta difficile comprendere la scala e la pericolosità di questo costante "dissanguamento" planetario, che continua silenziosamente ogni giorno dell'anno, sempre ed ovunque, 24 ore al giorno.
A ciò va aggiunto il fatto che, in base al report già citato, a fronte di 945 miliardi di dollari di danni generati dal solo cybercrime nel 2020 (erano 600 miliardi nel 2018)[9], nello stesso anno la spesa globale in ICT security è stata di 145 miliardi di dollari (di cui 1,5 miliardi in Italia)[10], ovvero che per ogni dollaro investito in sicurezza dai difensori gli attaccanti abbiano causato (considerando solo gli attacchi realizzati con finalità cybercriminali) 7 dollari di perdite.
Se stessimo analizzando gli esiti di un conflitto tradizionale, un'asimmetria di questo genere indicherebbe che i difensori stanno perdendo la guerra, anzi che le stanno prendendo di santa ragione, cosa che in modo più sotterraneo (ma per nulla metaforico) sta accadendo anche nel dominio cibernetico (non solo a livello di forze armate ed organizzazioni di intelligence, ma a tutti i livelli della società, coinvolgendo e danneggiando tutti, dai singoli cittadini alle nazioni).
E' anche ragionevole supporre che se/quando i danni raggiungessero i livelli ipotizzati, molti soggetti (in particolare quelli dotati di minori risorse) potrebbero essere dissuasi dal fare ulteriori investimenti in tecnologie digitali, generando un effetto boomerang del quale, complice anche la pandemia in atto, iniziano a sentirsi gli effetti.
Una situazione già molto grave che diventerà insostenibile da qui a metà decade, mettendo in discussione i benefici economici della rivoluzione tecnologica ed organizzativa in atto.
Le cause (e le responsabilità) sono molteplici e molto complesse, derivando da innumerevoli fattori, e pertanto non possono essere trattate in questa sede, ma la risposta non può che essere quella di aumentare sensibilmente gli investimenti in ICT Security (da una media del 2,5% del budget ICT[11] ad almeno il 10%, nel prossimo quadriennio) e di introdurre rapidamente tutte le agevolazioni e gli incentivi necessari perchè questo possa accadere, trattandosi di un importante rischio per la sicurezza del Paese.

---

8 Applicando per difetto la nostra stima di 500 USD di danni per abitante.

9 E' importante notare che, mentre numericamente gli attacchi sono aumentati del 20%, i danni nello stesso periodo sono aumentati del 57%.

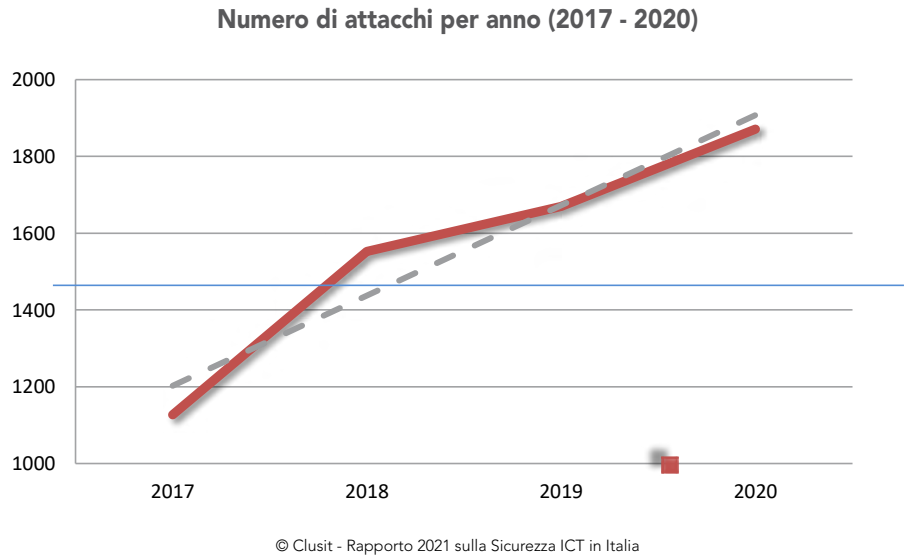
10 Cifra insufficiente, considerato che rappresenta circa l'1% della spesa mondiale in ICT Security, a fronte di un PIL italiano pari al 1,75% di quello mondiale.

11 A titolo di esempio, in base al NIS Investment Report dell'ENISA di dicembre 2020, il gap di investimento (in funzione della spesa ICT) tra realtà europee ed americane è in media del 41%. L'Italia investe in media il 50% in meno degli USA in ICT Security, in proporzione alla spesa ICT. Ciò detto, anche i livelli di investimento americani risultano comunque insufficienti a contrastare efficacemente le minacce cibernetiche attuali https://www.enisa.europa.eu/publications/nis-investments

In sintesi auspichiamo con forza che *già a partire dal 2021* si mettano in campo le risorse necessarie a rompere l'assedio. Il trend attuale deve essere assolutamente invertito, aumentanto in modo significativo gli investimenti in sicurezza cibernetica (di tutti i tipi ed a tutti i livelli), pena un aumento dei danni tale da innescare prima un rallentamento e poi una stagnazione, se non una decadenza, della nostra c.d. "società digitale".
Lo sforzo che dovrà essere messo in campo per recuperare il terreno perduto, ed evitare di innescare dinamiche negative irreversibili (a livello micro e macro) rispetto allo sviluppo del digitale ed alla distribuzione dei suoi benefici è chiaramente *enorme*. Non possiamo però rimandare oltre e, soprattutto, non abbiamo alternative.

Analisi dei principali cyber attacchi noti a livello globale del 2020

In questa prima sezione del Rapporto CLUSIT 2021, come di consueto, proponiamo una dettagliata panoramica degli incidenti di sicurezza più significativi avvenuti a livello globale nel 2020, confrontandoli con i dati raccolti nei 3 anni precedenti[12].
Lo studio si basa su un campione che al 31 dicembre 2020 è costituito da **11.959** attacchi noti di particolare gravità avvenuti nel mondo (inclusa l'Italia) dal primo gennaio 2011 (di cui **5.093** dal 2017), ovvero che hanno avuto un impatto significativo per le vittime in termini di perdite economiche, di danni alla reputazione, di diffusione di dati sensibili (personali e non), o che comunque prefigurano scenari particolarmente preoccupanti. Di questi **1.871** sono avvenuti nel 2020 (**+12%** rispetto al 2019, **+ 20%** rispetto al 2017). Il numero di attacchi rilevati nel 2020 segna una differenza del **+29%** rispetto alla media degli attacchi per anno del triennio precedente (1.449), visualizzata con una linea blu orizzontale nel grafico seguente.

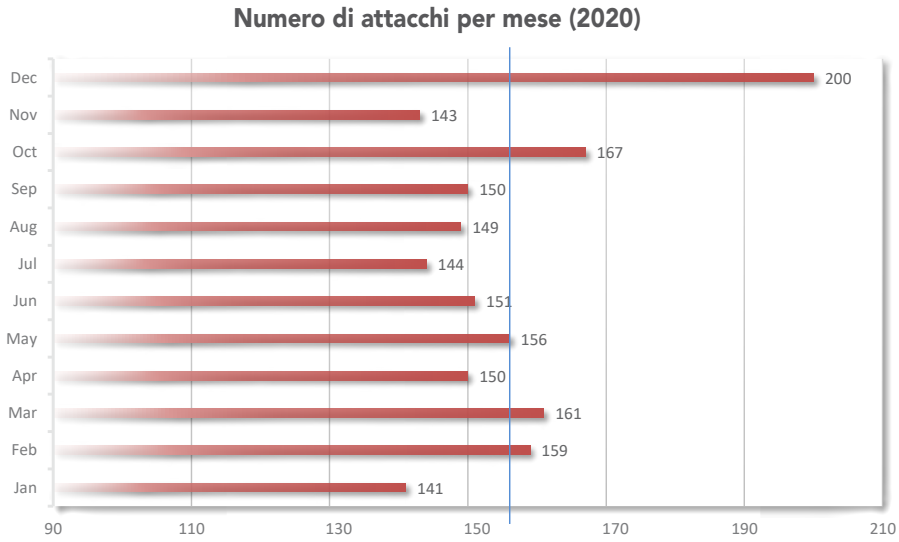


© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia

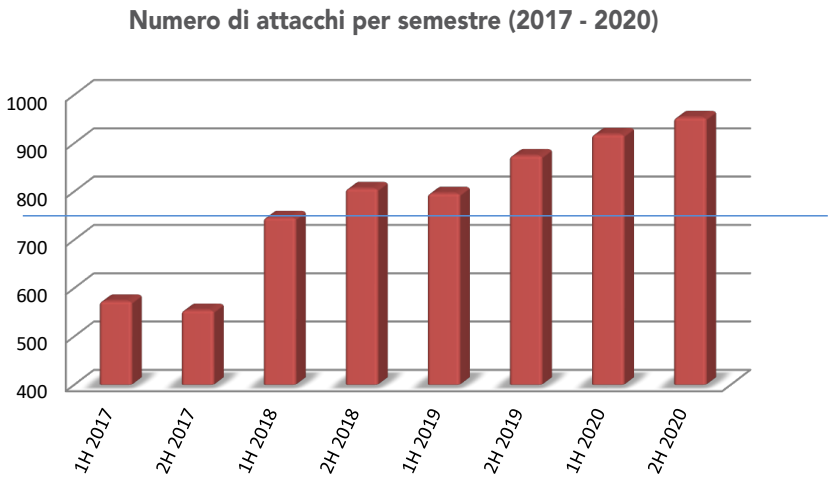
[12] pur avendo iniziato questa ricerca nel 2011, oggi ha poco senso fare confronti con gli anni precedenti al 2017. Da qui in avanti, per comodità di consultazione ed omogeneità dei criteri di classificazione degli attacchi, presentiamo il confronto solo dei dati degli ultimi 4 anni, rimandando alle edizioni precedenti del Rapporto Clusit per i dati relativi al periodo 2011-2016.

Anche quest'anno, per definire un cyber attacco come "grave" abbiamo impiegato gli stessi criteri di classificazione già applicati ai dati del periodo 2014-2019, più restrittivi rispetto ai criteri che avevamo applicato negli anni 2011-2013.

Nel 2020 abbiamo registrato in media **156 attacchi gravi al mese** a livello globale (rispetto ad una media di 94 al mese nel 2017, e di 120 al mese nel triennio 17-19). Il picco massimo mensile di sempre si è avuto nel dicembre 2020 (200 attacchi). Oltre a dicembre, i mesi peggiori nel 2020 sono stati febbraio, marzo ed ottobre.



Questa la distribuzione degli attacchi registrati nel periodo 2017-2020, suddivisi per semestre. La linea blu orizzontale rappresenta la media semestrale del triennio 2017-2019 (725):



© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia

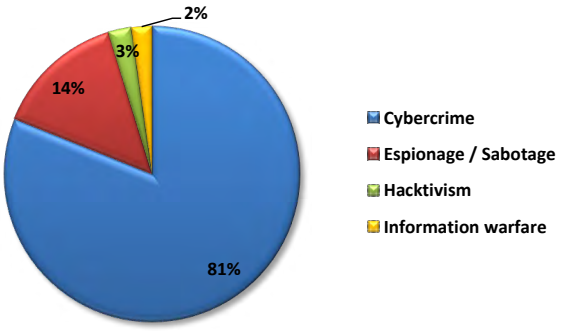
Le tre tabelle seguenti rappresentano una sintesi dei dati che abbiamo raccolto e analizzato. Come in passato abbiamo evidenziato nella colonna più a destra le tendenze osservate.

Distribuzione degli attaccanti

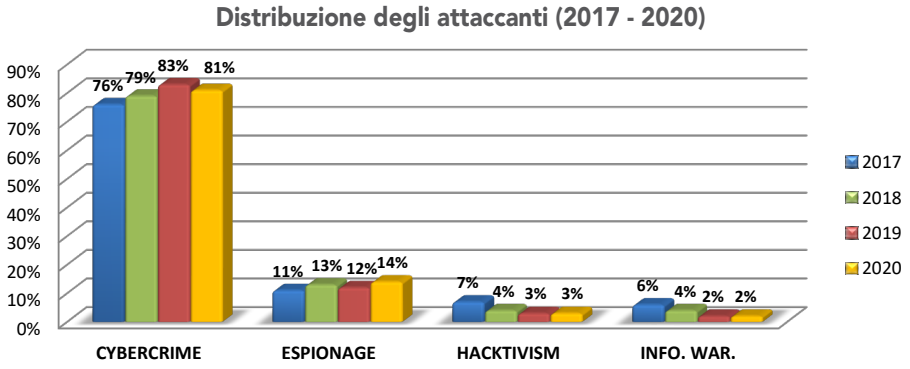
ATTACCANTI PER TIPOLOGIA	2017	2018	2019	2020	2020 su 2019	Trend 2020
Cybercrime	857	1232	1383	1517	9.7%	↗
Hacktivism	79	61	48	47	-2.1%	↗
Espionage / Sabotage	129	203	204	266	30.4%	↑
Cyber warfare	62	56	35	41	17.1%	↑
Espionage / Sabotage + Cyber Warfare	191	259	239	307	28.5%	↑
TOTALE	1127	1552	1670	1871	+12%	

Complessivamente, rispetto al 2019, il numero di attacchi gravi che abbiamo raccolto da fonti pubbliche per il 2020 cresce del +**12%**. In termini assoluti, nel 2020 la categoria "Cybercrime" fa registrare il numero di attacchi più elevato degli ultimi 10 anni, con una crescita del **+77%** rispetto al 2017 (1.517 contro 857) e del **+9,7%** rispetto al 2019.
Dal campione emerge chiaramente che, mentre le attività riferibili ad attacchi della categoria "**Hacktivism**" diminuiscono ancora (**-2,1%**) rispetto al 2019, nel 2020 sono in ulteriore aumento gli attacchi gravi compiuti per finalità di "**Cyber Espionage**" (**+30,4%**) e quelli appartenenti alla categoria "Cyber Warfare" (**+17,1%**).
Va sottolineato che, rispetto al passato, oggi risulta più difficile distinguere nettamente tra "Cyber Espionage/Sabotage" e "Cyber Warfare": sommando gli attacchi di entrambe le categorie, nel 2020 si assiste ad aumento del **28,5%** rispetto all'anno precedente (307 contro 239).

Tipologia e distribuzione degli attaccanti (2020)



Già nel 2017 il Cybercrime si era confermato la prima causa di attacchi gravi a livello globale (76%), salendo al 79% dei casi analizzati nel 2018. Nel 2019 tale percentuale era l'83%, mostrando una tendenza inequivocabile. Nel 2020 tale percentuale si attesta all'**81%**.

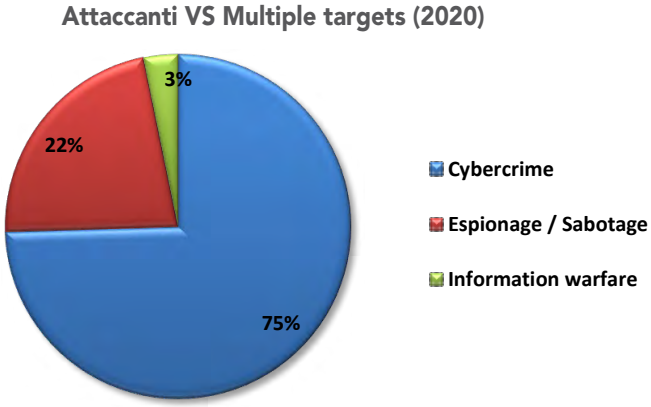


© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia

Per quanto riguarda le attività di Espionage (anche considerando la scarsità di informazioni pubbliche in merito) la loro percentuale rispetto al totale degli attacchi rilevati nel 2019 passa dal 12% al **14%**, mentre l'Information Warfare rimane apparentemente stabile al **2%**. Nel 2020 queste due categorie sommate valgono il **16%** degli attacchi noti totali (ma hanno una Severity più alta della media, vedi poi).

Distribuzione degli attaccanti rispetto alle categorie più colpite

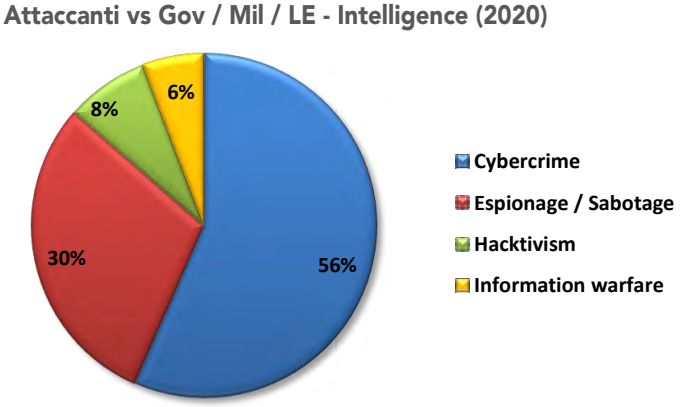
Dal punto di vista della distribuzione degli attaccanti che le hanno prese di mira, le quattro categorie di vittime più colpite nel 2020 mostrano differenze molto significative, il che conferma che ogni categoria di bersagli ha un suo particolare *threat landscape* dal quale deve proteggersi, e che (di conseguenza) non esistono soluzioni universali ma anzi, ogni settore dovrebbe schierare un mix specifico di soluzioni difensive.



© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia

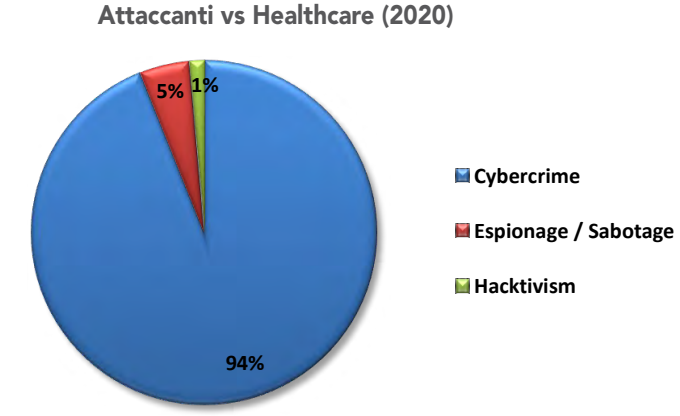
La distribuzione degli attaccanti verso la categoria "Multiple Targets" (che da diversi anni ormai è quella più numerosa) ricalca la distribuzione generale, con un lieve decremento della componente cyber criminale rispetto al totale (dal 81% al 75%), dovuto al fatto che a compiere attacchi contro bersagli multipli in parallelo è ormai anche una consistente fetta di attori con finalità di espionage (22% contro il 14% generale).

Significativamente diversa la distribuzione degli attaccanti verso il settore Governativo. La diversa composizione percentuale degli attaccanti incide anche fortemente sul tipo di tecniche di attacco utilizzate verso le diverse categorie di vittime (vedi oltre). Interessante notare che mentre la quota di attacchi compiuti per finalità cybercriminali contro questo settore è significativamente più bassa rispetto a quella generale (56% contro 81%), la componente riferibile a Espionage è il doppio (30% contro 14%), mentre gli attacchi realizzati per finalità di Hacktivism sono addirittura il triplo, così come quelli con finalità di Information Warfare.

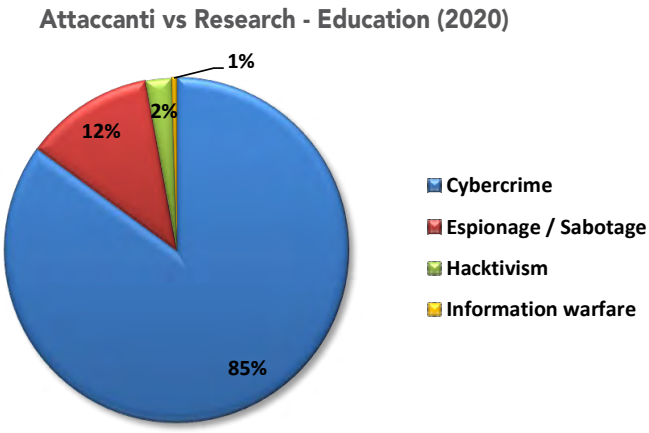


© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia

Ancora diversa la distribuzione degli attaccanti che hanno colpito il settore "Healthcare", prevalentemente con finalità cybercriminali, in particolare estorsioni (ransomware) e furti di dati personali, da utilizzare per compiere ulteriori attacchi. La componente Espionage passa dal 3% del 2019 al 5% del 2020, a riprova delle numerose attività di intelligence che hanno interessato la categoria (con particolare interesse verso lo sviluppo di vaccini per il *SARS-CoV-2*) nel corso dell'anno.



© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia



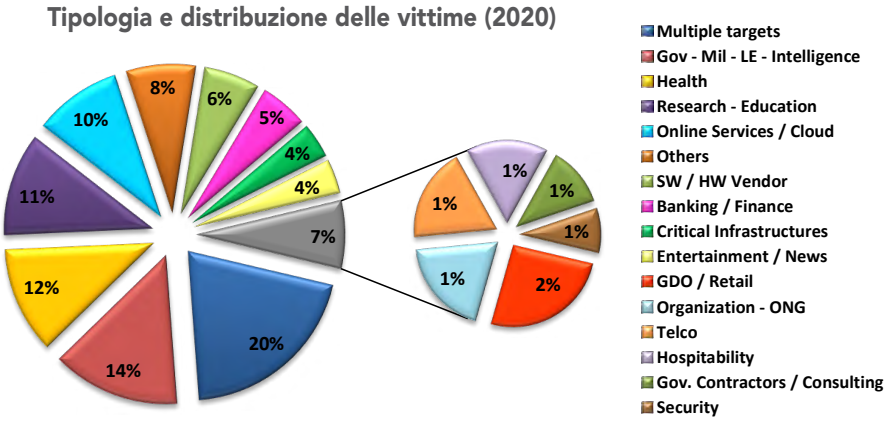
Per la categoria "Research/Education" la distribuzione degli attaccanti è ancora diversa: da un lato si notano i numerosissimi attacchi ransomware verso scuole ed università, dall'altro l'attività di espionage condotta verso centri di ricerca, in particolare quelli dedicati alla preparazione di terapie per contrastare il Covid-19.

Distribuzione delle vittime per tipologia

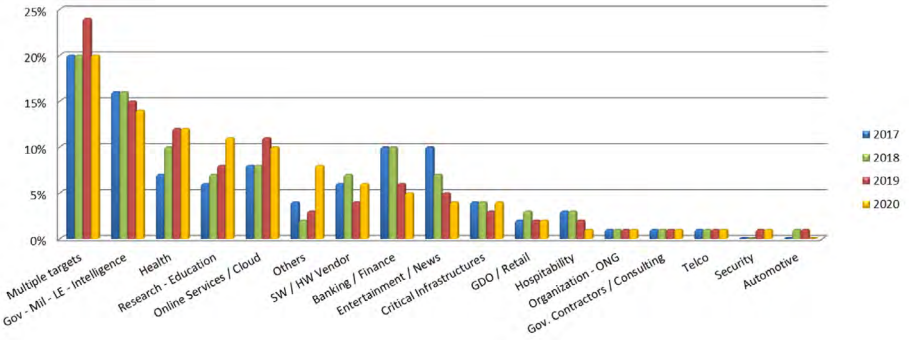
VITTIME PER TIPOLOGIA	2017	2018	2019	2020	2020 su 2019	Trend 2020
Institutions: Gov - Mil - LEAs - Intelligence	179	252	247	258	4.5%	↗
Multiple targets	222	304	395	374	-5.3%	↗
Health	80	159	203	215	5.9%	↗
Banking / Finance	117	157	100	97	-3.0%	↗
Online Services / Cloud	95	129	186	177	-4.8%	↗
Research - Education	71	109	141	207	46.8%	↑
Software / Hardware Vendor	68	109	70	113	61.4%	↑
Entertainment / News	115	102	83	69	-16.9%	↓
Critical Infrastructures	40	57	50	70	40.0%	↑
Hospitability	34	45	27	22	-18.5%	↓
GDO / Retail	24	39	37	35	-5.4%	↗
Others	40	30	53	140	164.2%	↑
Org / ONG	8	18	17	26	52.9%	↑
Gov. Contractors / Consulting	6	14	11	16	45.5%	↑
Telco	13	11	18	25	38.9%	↑
Automotive	4	9	10	8	-20.0%	↓
Security Industry	11	4	17	12	-29.4%	↓
Religion	0	3	2	5	150.0%	↑
Chemical / Medical	0	1	3	2	-33.3%	↓
TOTALE	1127	1552	1670	1871	+12%	

Nel 2020 le categorie più colpite sono state **Multiple Targets** (374 attacchi, **-5,3%** rispetto al 2019), **Government** (258 attacchi, **+4,5%**), **Healthcare** (215 attacchi, **+5,9%**) e **Research/Education** (206 attacchi, **+46,8%**). Queste quattro categorie sommate rappresentano il **77%** delle vittime totali all'interno del nostro campione.
Interessante sottolineare l'aumento di attacchi singoli verso la categoria "Others"

(**+164,2%**), nonostante molti di questi attacchi rientrino solitamente nella categoria "Multiple targets". Ciò è dovuto ad un aumento di *attacchi mirati* verso nuove categorie di bersagli non esplicitamente classificate nella nostra tassonomia, che anche per questo motivo amplieremo dalla prossima edizione.
All'interno della categoria "Multiple Targets", che numericamente costituisce un quinto degli attacchi registrati, sono compresi attacchi verso vittime appartenenti a *tutte le altre categorie, colpite dallo stesso attacco in parallelo*, a dimostrazione del fatto che gli attaccanti sono sempre più aggressivi e conducono operazioni su scala sempre maggiore, con una logica "industriale", che prescinde sia da vincoli territoriali che dalla tipologia dei bersagli, puntando solo a massimizzare il risultato economico.
Degno di nota anche l'aumento degli attacchi verso le categorie "Critical Infrastructures" (**+40%**), "Software/Hardware vendor" (**+61,4%**) e "Gov Contractors & Consulting" (**+45,5%**) rispetto al 2019.



Attacchi per categoria di vittima (2017 - 2020)



© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia

Tramite questo grafico si può apprezzare facilmente l'evoluzione delle minacce rispetto alle categorie di vittime nel periodo 2017-2020.

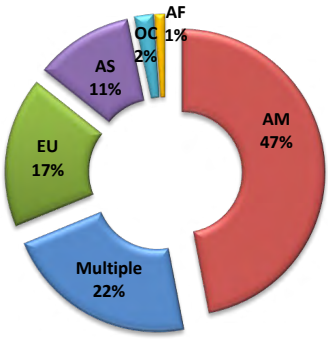
Distribuzione delle vittime per area geografica

La classificazione delle vittime per nazione di appartenenza viene qui rappresentata su base continentale.

Nel 2020 rimangono stabili le vittime di area americana (dal 46% al **47%**), mentre gli attacchi verso realtà basate in Europa aumentano (dal 11% al **17%**), così come quelli rilevati contro organizzazioni asiatiche (dal 9% al **11%**).

Percentualmente diminuiscono invece gli attacchi gravi verso bersagli geograficamente distribuiti su scala globale (categoria "Multiple"), dall'31% del 2019 al **22%** del 2020.

Appartenenza geografica delle vittime per continente (2020)



© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia

Distribuzione delle tecniche di attacco

TECNICHE DI ATTACCO PER TIPOLOGIA	2017	2018	2019	2020	2020 su 2019	Trend 2020
Malware	446	585	729	783	7.4%	↑
Unknown	277	408	317	372	17.4%	↑
Known Vulnerabilities / Misconfigurations	127	177	127	184	44.9%	↑
Phishing / Social Engineering	102	160	291	289	-0.7%	↗
Multiple Techniques / APT	63	98	65	95	46.2%	↑
Account Cracking	52	56	86	85	-1.2%	↗
DDoS	38	38	23	34	47.8%	↑
0-day	12	20	30	23	-23.3%	↓
Phone Hacking	3	9	1	3	200.0%	↑
SQL Injection	7	1	1	3	200.0%	↑
TOTALE	1127	1552	1670	1871	+12%	

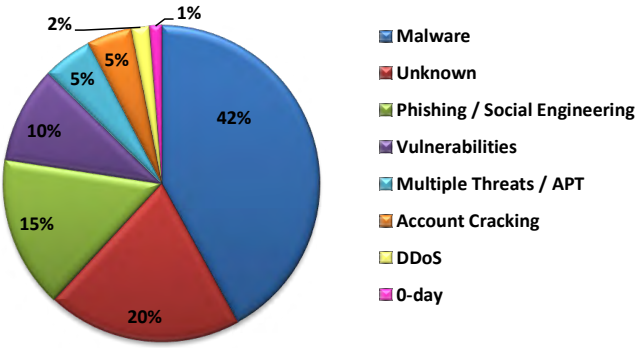
Per la quarta volta dal 2011, nel 2020 le tecniche sconosciute (categoria "Unknown") sono al secondo posto, aumentando del **17,4%** rispetto al 2019, superate solo dalla categoria "Malware", stabile al primo posto, che cresce ulteriormente del +**7,4%** e rappresenta da sola il **42%** del totale.

Al terzo posto la categoria "Phishing/Social Engineering", che rimane stabile rispetto al 2019 e rappresenta il **15%** del totale. Una quota crescente di questi attacchi basati su Phishing si riferisce a "BEC scams"[13], che infliggono danni economici sempre maggiori alle loro vittime. Al quarto posto la categoria "Know Vulnerabilities", utilizzata con successo nel 10% dei casi e in crescita del **44,9%** rispetto al 2019.

Tutte le altre tipologie di tecniche di attacco sommate rappresentano nel 2020 il **13%** del totale. Tra queste, notevole l'incremento percentuale delle categorie "DDoS" (**+47,8%**) e "Multiple Techniques/APT" (**+46,2%**), mentre appaiono in diminuzione gli attacchi realizzati sfruttando vulnerabilità "0-Day" (**-23,3%**).

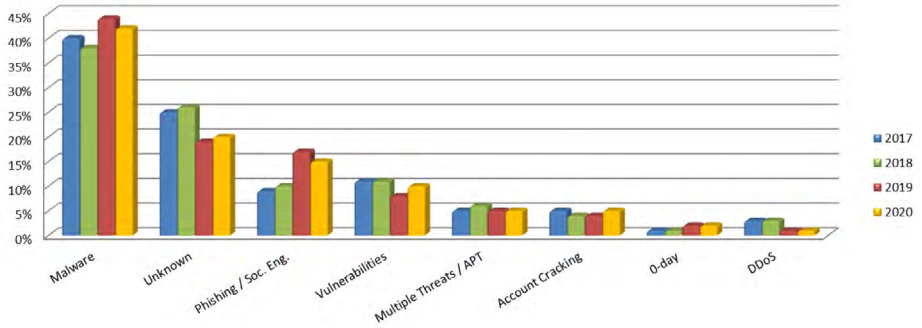
[13] https://en.wikipedia.org/wiki/Business_email_compromise

Tipologia e distribuzione delle tecniche di attacco (2020)



© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia

% Attacchi per tecniche di attacco (2017 - 2020)

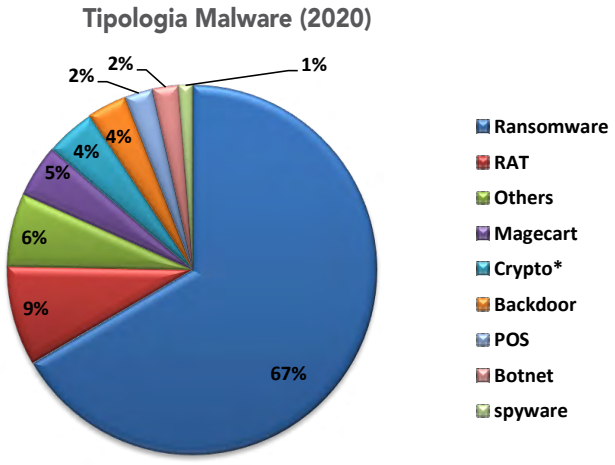


© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia

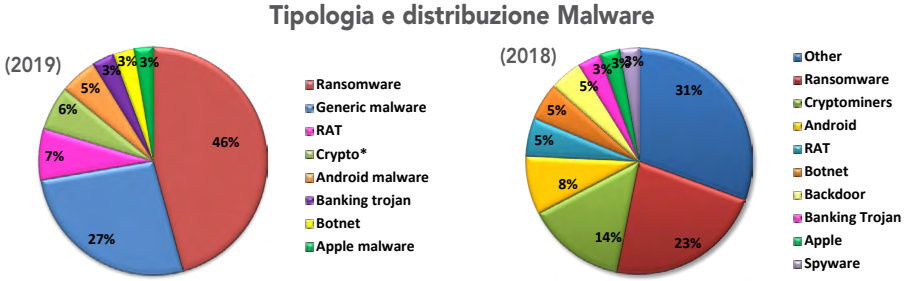
IIn sostanza si conferma anche nel 2020 una tendenza inequivocabile e molto pericolosa: gli attaccanti possono fare affidamento sull'efficacia del Malware "semplice", prodotto industrialmente a costi decrescenti in infinite varianti, su Vulnerabilità note e su tecniche di Phishing / Social Engineering relativamente semplici, per conseguire la gran maggioranza dei loro obiettivi. Questo dato è evidenziato dalla polarizzazione delle tecniche d'attacco, tale per cui ormai le prime 4 categorie (su un totale di 10) rappresentano l'**87%** del campione.

Analisi delle principali categorie di malware

Dato che la categoria "Malware" si conferma per il terzo anno di fila la più numerosa, anche per il 2020 presentiamo un'analisi di dettaglio relativa alle tipologie di malware osservate nel nostro campione, confrontandola con l'anno precedente:



© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia



© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia

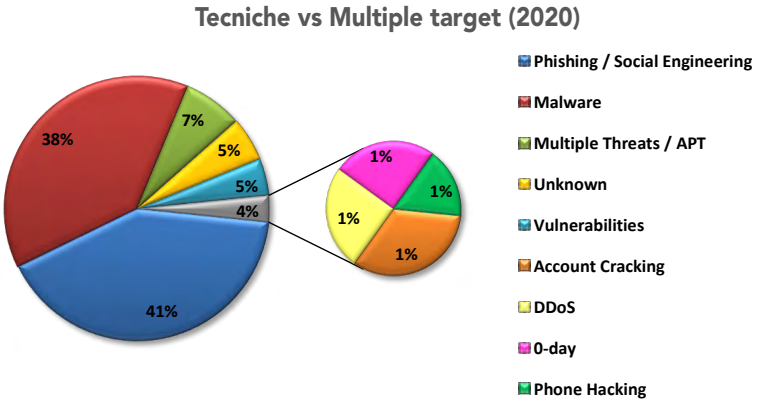
Dai grafici si possono osservare alcuni fenomeni interessanti, tra questi che i Ransomware, che rappresentavano nel 2019 quasi la metà del totale (erano un quarto nel 2018) nel 2020 sono il 67%.

D'altra parte i Cryptominers sono diminuiti dal 14% del 2018 al 4% del 2020.

La categoria "Others/Generic Malware", che era al primo posto nel 2018 con il 31% del totale ed era ancora al 27% nel 2019, si è ridotta al 6% nel 2020, il che indica una maggiore concentrazione degli attaccanti sulle famiglie di malware più efficaci e redditizie.

Distribuzione delle tecniche di attacco utilizzate contro le prime quattro categorie di vittime

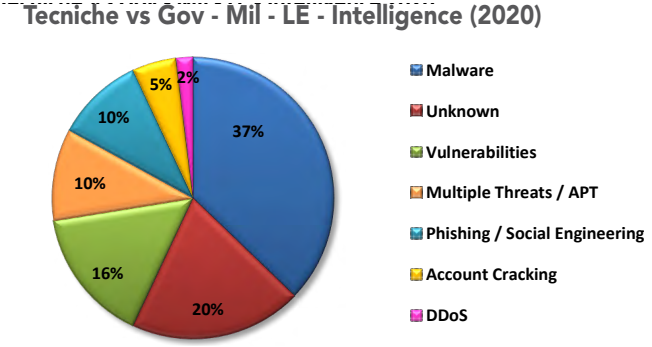
Si può osservare chiaramente come la distribuzione percentuale delle tecniche di attacco mostri variazioni importanti a seconda della tipologia di bersaglio (il che deriva non solo dal fatto che le vittime sono molto diverse tra loro, ma anche dalla diversa natura e dagli obiettivi dei rispettivi attaccanti), a ulteriore riprova del fatto che, in assenza di un threat model puntuale, mettere in campo mitigazioni generiche non rappresenta la migliore allocazione delle risorse disponibili.



© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia

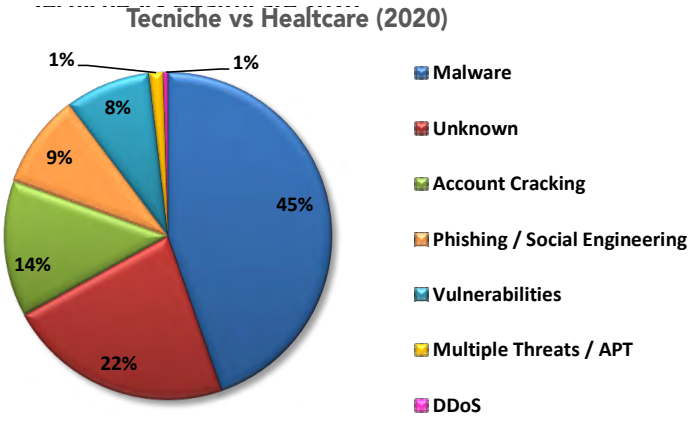
Nel caso degli attacchi industrializzati su larga scala il Phishing rappresenta la tecnica più usata, seguito dal Malware e in misura molto minore da APT e Tecniche sconosciute.

Nel caso del settore Gov invece prevale il Malware, seguito da Tecniche sconosciute, Vulnerabilità note, APT e Phishing.



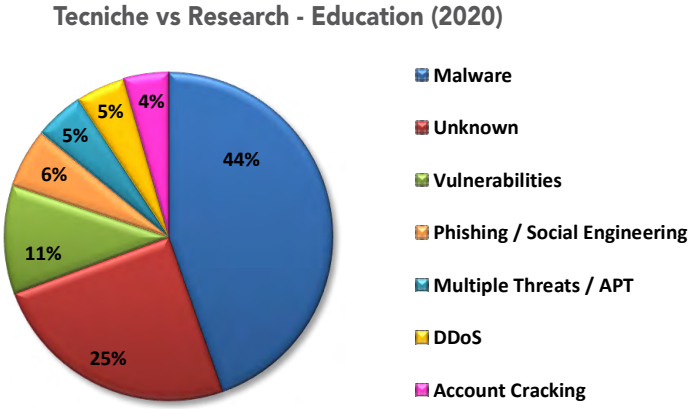
© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia

Nel caso di Healthcare prevalgono le Tecniche sconosciute a pari merito con Malware, seguite da Phishing e Vulnerabilità note.



© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia

Infine nel caso di Research / Education prevale il Malware, seguito da Tecniche sconosciute, Vulnerabilità note e Phishing.

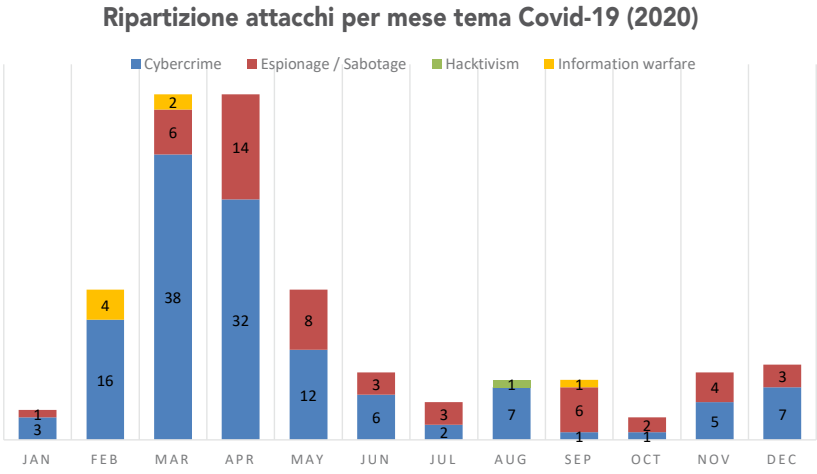


© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia

Analisi degli attacchi a tema "Covid-19"

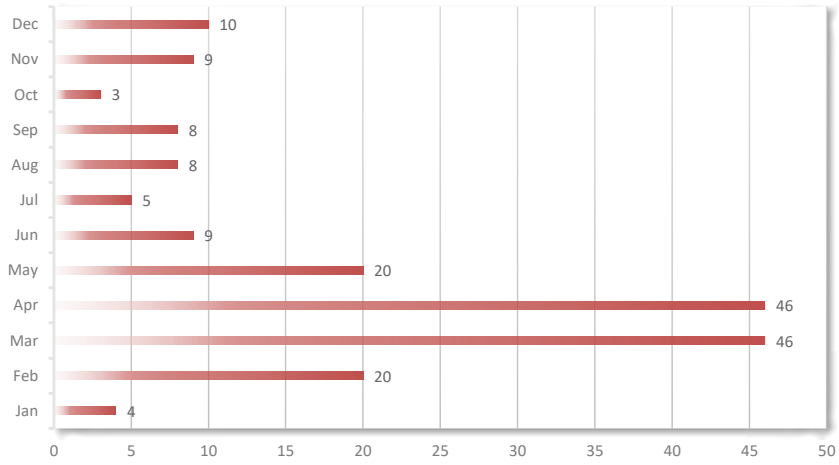
La pandemia da SARS-CoV-2 ha avuto, e sta avendo tuttora, notevoli impatti a livello sanitario, sociale, economico e lavorativo per miliardi di persone e milioni di organizzazioni a livello globale.
Data la criticità di questo momento storico, che tra le altre cose ha costretto individui ed organizzazioni a ripensare profondamente le proprie abitudini ed i propri processi organizzativi, ed a modificarli in corsa, l'argomento "COVID-19" è stato inevitabilmente sfruttato da vari attori ostili a supporto delle proprie operazioni e del conseguimento dei propri obiettivi. Questo a dimostrazione, ove ve ne fosse ancora bisogno, dell'estrema pragmaticità degli attaccanti, che reagiscono con estrema rapidità e non perdono alcuna opportunità per massimizzare i loro risultati, senza preoccuparsi delle possibili ricadute, dirette ed indirette.
In questo caso, oltre a provocare danni in conseguenza degli attacchi compiuti, gli attaccanti hanno anche favorito la diffusione di *fake news* ed alimentato la grande confusione che si è venuta a creare intorno a questa grave emergenza planetaria.

Ciò premesso, nell'analizzare **1.871** attacchi gravi emersi nel corso del 2020, ne abbiamo classificati **188** come direttamente riferibili al tema COVID-19 (ovvero il **10%** rispetto al totale del campione), tenendo anche conto che questi attacchi sono stati realizzati prevalentemente tra febbraio e maggio, con picchi a marzo e aprile, come si evince chiaramente dai due grafici seguenti.



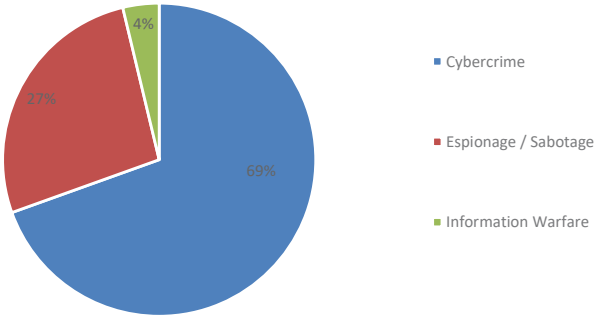
© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia

Attacchi per mese tema Covid-19 (2020)



Contrariamente a quanto si potrebbe pensare, per quanto riguarda gli **attaccanti**, il tema COVID-19 non è stato cavalcato solo da cyber criminali (tipicamente in associazione con campagne di Phishing o di Malware), ma anche da altre categorie di attaccanti, in particolare per finalità di Espionage e di Information Warfare, per conseguire obiettivi molto diversi tra loro.

Tipologia e distribuzione degli attaccanti tema Covid-19 (2020)

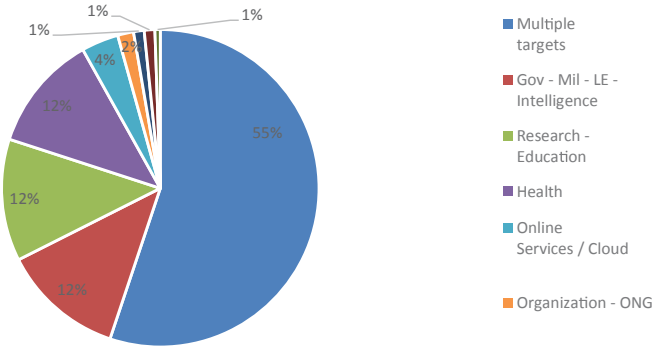


Dal grafico si evince infatti che il tema COVID-19 è stato sfruttato in percentuale proporzionalmente molto maggiore da parte degli attaccanti con finalità di tipo "**Espionage**"

e "**Information Warfare**" (**31%**), in particolare nei confronti di organizzazioni coinvolte nella ricerca sui vaccini, rispetto al nostro campione complessivo, nel quale questi soggetti sono risultati responsabili "solo" del 16% degli attacchi.

Per la stessa ragione, mentre gli attacchi compiuti per finalità **cyber criminali** nel nostro campione complessivo sono stati l'81%, quelli a tema COVID-19 sono il **69%** del totale.
Anche per quanto riguarda la distribuzione percentuale delle **vittime** di questi attacchi si osservano interessanti variazioni rispetto ai valori complessivi del campione.

Tipologia e distribuzione dei target tema Covid-19 (2020)



© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia

In particolare, il **55%** di vittime afferenti alla categoria "**Multiple targets**" (che nel campione complessivo rappresentano il 20% del totale) fa chiaramente intuire la natura di questi attacchi, principalmente basati su tecniche di Phishing e Social Engineering, e strutturati per colpire rapidamente il maggior numero di persone ed organizzazioni, in parallelo.

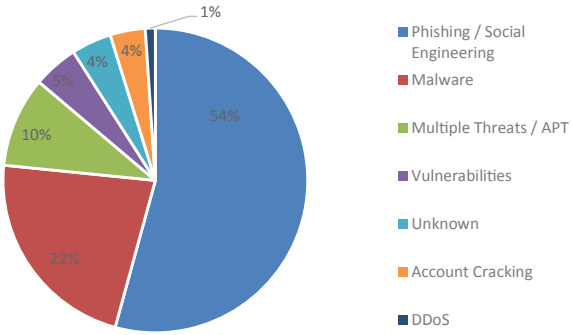
È interessante anche sottolineare il **12%** di attacchi verso la categoria di bersagli "**Gov**", quasi tutti di natura Espionage (con però alcuni casi gravi di BEC scam[14], portati a segno da cyber criminali nelle prime fasi concitate di approvvigionamento di presidi di sicurezza, p.es mascherine, creando danni considerevoli).
Altrettanto grave anche il **12%** di attacchi verso la categoria "**Research / Education**" dove sono state prese di mira organizzazioni ed università coinvolte nella ricerca e nello sviluppo di vaccini anti Covid-19.

Infine, un altro **12%** ha visto il **settore sanitario** vittima di diverse tipologie di attacchi che hanno sfruttato il tema Coronavirus, principalmente Ransomware e Phishing.

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

Per quanto riguarda invece la distribuzione delle **tecniche** utilizzate per attacchi a tema COVID-19, come detto in precedenza, si tratta principalmente di campagne basate su "**Phishing / Social Engineering**" (**54%**) e su "**Malware**" (**22%**). Una percentuale significativa (**10%**) riguarda la categoria "**Multiple Threats / APT**", che nel campione generale invece rappresentano il 5% dei casi.

Tipologia e distribuzione delle tecniche tema Covid-19 (2020)

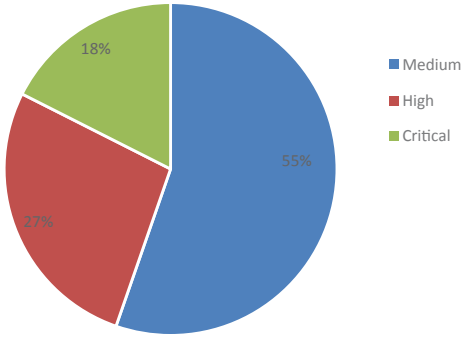


© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia

Infine, per quanto riguarda la **Severity** degli attacchi del nostro campione che rientrano in questo gruppo, è interessante notare come in media sia più bassa di quella del campione generale, nel quale gli impatti di tipo "**High**" e "**Critical**" sommati rappresentano ben il 56%, mentre qui sono il **45%**.

È ragionevole pensare che questa dinamica sia dovuta da un lato alla grande prevalenza di Phishing generico, che mediamente non causa impatti di livello alto e critico, e dall'altro al fatto che anche gli attaccanti abbiano dovuto improvvisare e adattarsi in corsa alla situazione, risultando nel complesso (relativamente parlando) meno incisivi, e dunque dannosi, del consueto.

Distribuzione severity tema Covid-19 (2020)



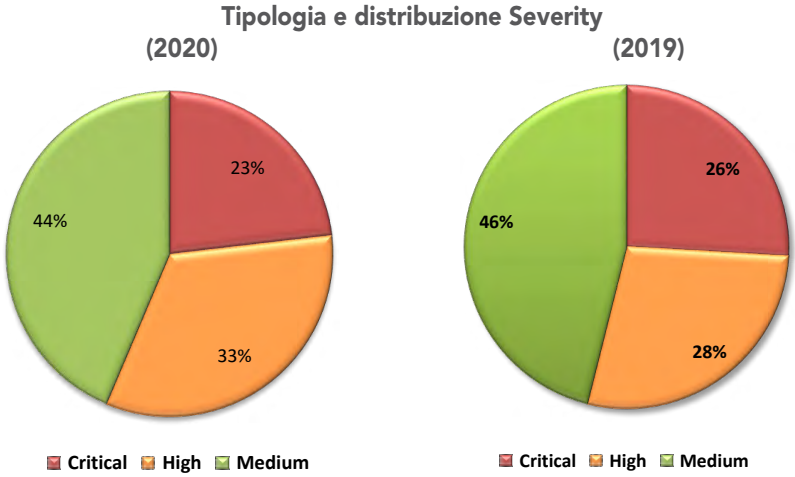
© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia

Concludendo, considerato che la pandemia è tuttora in corso, appare evidente la necessità di prestare particolare attenzione al fenomeno, e di investire nella sensibilizzazione degli utenti rispetto a questo problema, onde evitare ulteriori danni.

Analisi della "Severity" degli attacchi

Come anticipato nell'introduzione di questa analisi, anche per il 2020 presentiamo una valutazione della Severity degli attacchi analizzati.
Per distinguere tra attacchi di differente natura e pericolosità all'interno del campione abbiamo definito tre macrocategorie o livelli di **impatto** (considerato che stiamo comunque analizzando un campione di incidenti tutti definiti come "gravi"): Medio, Alto e Critico.
Va premesso che questo genere di analisi si scontra inevitabilmente con la scarsità di informazioni dettagliate di dominio pubblico relative ai singoli incidenti, e che pertanto deve considerarsi una stima ad alto livello.

Le variabili che contribuiscono a comporre la valutazione dell'impatto per ogni singolo attacco analizzato sono molteplici ed includono: impatto geopolitico, sociale, economico (diretto e indiretto) e di immagine.
Per il campione 2020, l'analisi degli impatti stimati ci presenta questo quadro generale:

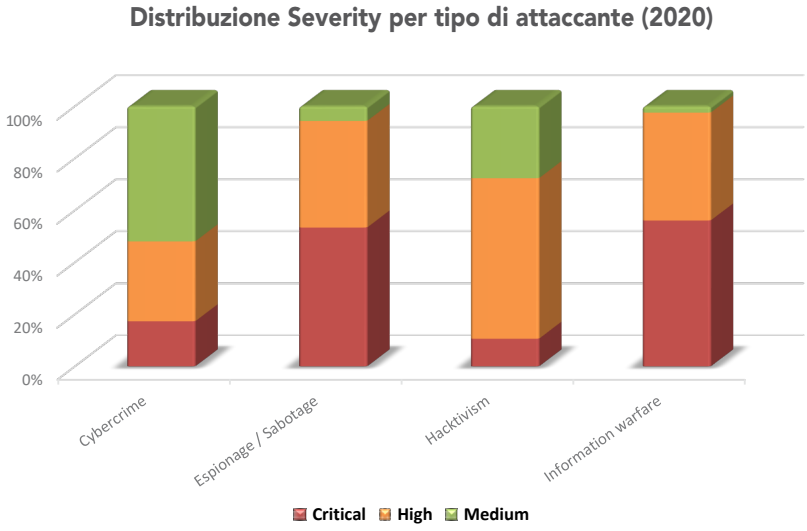


© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia

Interessante confrontare i risultati della stessa analisi relativi al 2019:

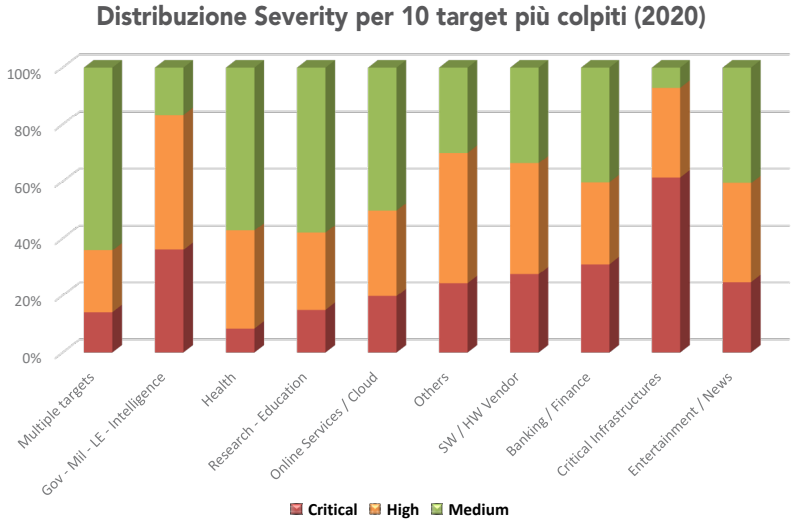
Nel 2020 gli attacchi con impatto "Medio" rappresentano il **44%** del totale (erano il 39% nel 2018 ed il 46% nel 2019), quelli di livello "Alto" il **33%** (erano 33% nel 2018 e il 28% nel 2019) e quelli di livello "Critico" quasi un quarto con il **23%** (erano il 28% nel 2018 ed il 26% nel 2019).
Anche nel 2020 quindi il numero di attacchi di livello "Critical" e "High" supera il 50% del totale (**56%**), in leggero aumento rispetto al 54% del 2019. L'aumento è principalmente dovuto alla crescita degli attacchi di livello "Alto".

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



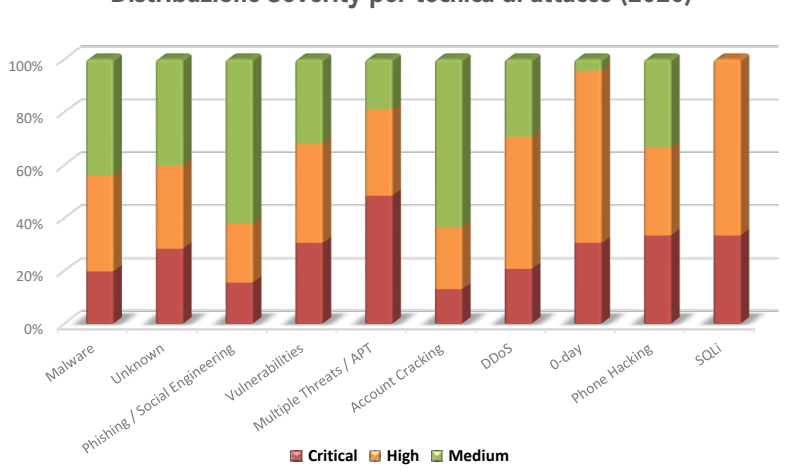
© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia

Non sorprende che il maggior numero di attacchi classificati come "Critici" riguardino le categorie di attaccanti "Espionage" ed "Information Warfare", mentre la prevalenza di attacchi con impatto di tipo "Medio" e (in misura minore) "Alto" riferiti ad attività cybercriminali si spiega con la necessità, per questi soggetti, di rimanere relativamente sottotraccia, guadagnando sui grandi numeri più che sul singolo attacco (tranne casi particolari).
Interessante anche notare come l'Hacktivism, pur in grande diminuzione, presenti un'ampia percentuale di attacchi con impatto di tipo "Alto" ed abbia un valore medio della Severity peggiore rispetto alla categoria Cybercrime (pur essendo numericamente molto meno rappresentato nel campione).



© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia

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



© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia

Gli attacchi con impatto più critico sono quelli realizzati tramite APT e 0-day (quindi più sofisticati e stealth, spesso con motivazioni geopolitiche e finalità di Espionage e Information Warfare), e quelli portati a segno sfruttando "vulnerabilità note" o "tecniche sconosciute".

In percentuale gli attacchi con impatto "Critico" realizzati tramite Malware sono meno di quelli realizzati tramite Vulnerabilità note o con tecniche sconosciute, mentre prevalgono gli impatti di tipo "Alto" nel caso di attacchi condotti tramite 0-day, Account Cracking, DDoS e Unknown.

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

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

Introduzione e visione d'insieme

Anche quest'anno, Fastweb ha contribuito a fotografare la situazione del cybercrime in Italia fornendo un'analisi dei fenomeni più rilevanti elaborata dal proprio Security Operations Center (SOC), attivo 24 ore su 24.

La pandemia di COVID-19 e il mutamento degli stili di vita ha impattato in modo rilevante sulle dinamiche del cybercrime, generando alcuni fenomeni in controtendenza rispetto al 2019.

Dall'analisi sull'infrastruttura di rete di Fastweb, costituita da oltre 6,5 milioni di indirizzi IP pubblici su ognuno dei quali possono comunicare centinaia di dispositivi e server attivi presso le reti dei clienti, si sono registrati oltre 36 milioni di eventi di sicurezza, in netta flessione rispetto agli eventi rilevati per il Report 2019

La flessione è iniziata principalmente **dopo il primo trimestre del 2020**, in corrispondenza con il lockdown e la remotizzazione del lavoro di molte imprese. L'esposizione di alcune tipologie di servizi (SMB Server Message Block, RDP Remote Desktop Protocol, Telnet…) si è ridotta del 18% rispetto al 2019. Analizzando il solo mese di marzo 2020 è stata registrata addirittura una diminuzione di questo indicatore del 63%. La maggior consapevolezza dei rischi legati agli attacchi informatici in periodo di pandemia ha spinto dunque le aziende ad innalzare i propri livelli di protezione dotandosi di strumenti tecnologici, come ad esempio firewall o VPN per garantire la continuità operativa. Tali strumenti da un lato hanno consentito ai dipendenti l'accesso da remoto alle reti virtuali aziendali, dall'altro ad avere una maggiore protezione perimetrale e una conseguente riduzione della superficie di attacco.

Questa novità, sicuramente positiva, ha spinto i criminali informatici a spostare la loro attenzione verso un punto più debole della catena ovvero verso l'endpoint, il pc del dipendente. Si è infatti notata una crescita del numero di attacchi indirizzati ai PC personali (85.000), che sono raddoppiati rispetto allo stesso periodo del 2019, dove si registravano 45.000 infezioni. Questo fenomeno è spiegabile considerando che, durante il periodo di emergenza, molte aziende non sono riuscite a dotare i propri dipendenti di laptop aziendali, con conseguente utilizzo di dispositivi personali, solitamente maggiormente vulnerabili a malware e virus.

Un'ulteriore evidenza, del fatto che il cybercrime è in qualche modo evoluto verso tipologie di attacchi più efficaci durante questo periodo di lavoro da remoto, è anche data dal trend degli eventi DDoS (Distributed Denial of Service) registrati.

Il volume degli attacchi DDoS infatti ha toccato i 7 Tbps, in fortissima crescita anche rispetto al mese peggiore dello scorso anno dove si attestava al massimo a 1.8 Tbps.
In particolare, si è notato un forte innalzamento dei volumi nei mesi del primo e secondo lockdown (marzo 2.2 Tbps, aprile 3.3 Tbps, maggio 5 Tbps, ottobre e novembre circa 6.5Tbps) per poi tornare negli altri mesi a valori in media con l'anno precedente. Lo spostamento del business verso internet ha spinto i cybercriminali ad incrementare questa tipologia di attacchi tesa principalmente a rendere indisponibili i siti di grandi aziende, anche chiedendo un riscatto, e delle Pubbliche Amministrazioni.
In conclusione, è importante evidenziare come la "nuova normalità" che stiamo tutti affrontando ha cambiato profondamente il modo di interagire, di lavorare, di vivere in società, ma ha anche portato il cybercrime ad un adattamento e ad un inasprimento degli attacchi sulla rete, asset fondamentale e irrinunciabile proprio in relazione al periodo attuale.
Nei paragrafi a seguire il dettaglio dei fenomeni rilevati.

Dati analizzati

I dati raccolti dal Security Operations Center di Fastweb sono stati arricchiti, analizzati e correlati con l'aggiunta di quelli forniti da organizzazioni esterne come ad esempio la Shadowserver Foundation, fonte autorevole in merito all'evoluzione delle botnet e dei relativi malware. Inoltre, sono stati considerati eventi e segnalazioni dei principali CERT nazionali e internazionali.
I dati sugli attacchi di distributed denial of dervice, sono stati ricavati da tutte le anomalie DDoS rilevate dalle tecnologie di Fastweb per il contrasto di questo tipo di attacchi. Allo stesso modo, le informazioni relative alle principali tipologie di minacce riscontrate, sono state raccolte da piattaforme interne utilizzate per attività di Incident Management.
È importante sottolineare che tutti i dati, prima di essere analizzati, sono stati automaticamente aggregati e anonimizzati per proteggere la privacy e la sicurezza sia dei clienti sia di Fastweb stessa.

Tipologia di malware e di botnet

La composizione dei malware e botnet che interessano le macchine appartenenti all'AS di Fastweb ha avuto una leggera flessione rispetto alla precedente rilevazione dell'anno 2019. Infatti quest'anno sono state individuate 220 famiglie di software malevoli (+33% rispetto all'anno precedente).
Andromeda raggiunge il 43% delle minacce riscontrate. A livello di comportamento questa è una piattaforma che è utilizzata per distribuire una galassia di varianti di malware (80 famiglie circa) tra cui ransomware, trojan bancari, robot spam, malware antifrode e altro ancora. Ciò che ha reso Andromeda un prodotto estremamente interessante è stata la sua natura modulare.
Un primo modulo, per poche centinaia di dollari consente di acquistare il plug-in keylogger per leggere i dati della tastiera della vittima oppure, per una cifra poco superiore, il plug-in Formgetter, con il compito di acquisire i dati inviati dal browser web del computer infettato.

Al secondo posto troviamo invece QSnatch. Questo malware ha iniziato ad essere presente a fine 2019 e durante tutto il 2020 ha avuto un forte impatto raggiungendo addirittura il 32% delle minacce riscontrate.
Tale malware che si diffonde sulle unità NAS (network-attached storage) prende il controllo completo del dispositivo ed è in grado di bloccare patch e aggiornamenti software. Ancora non è noto come sarà utilizzata questa nuova arma, anche se i ricercatori pensano che potrà essere usata per campagne di tipo DDoS o per la generazione abusiva di criptovalute come bitcoin (criptomining).
Infine, si è rilevata una piccola percentuale di software malevoli (0,08%) che non sono ancora stati catalogati e di cui non si conoscono tutti i dettagli.

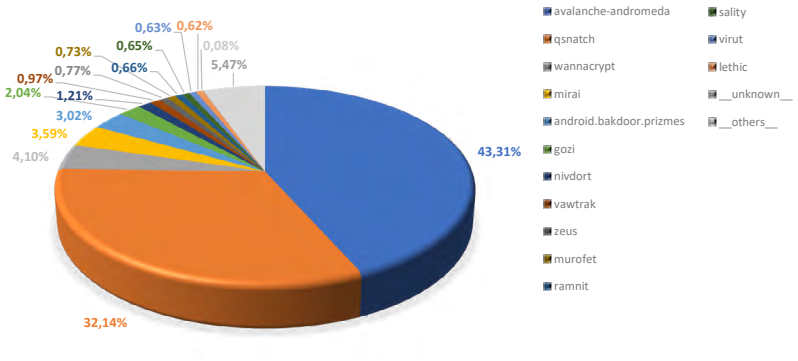


Figura 1 - *Analisi dei Malware rilevati (Dati Fastweb relativi all'anno 2020)*

Andamento temporale

Il grafico di **Figura 2** mostra la diffusione temporale degli host infetti e parte di botnet per l'anno 2020. Come si può notare, il trend continua a crescere e anche nel 2020 si conferma in forte ascesa.
Da evidenziare il picco di circa 8000/9000 host infetti durante i mesi di febbraio/maggio in corrispondenza del primo lockdown, sintomo del fatto che l'aumento del business sul digitale ha avuto come effetto un aumento complessivo delle minacce.

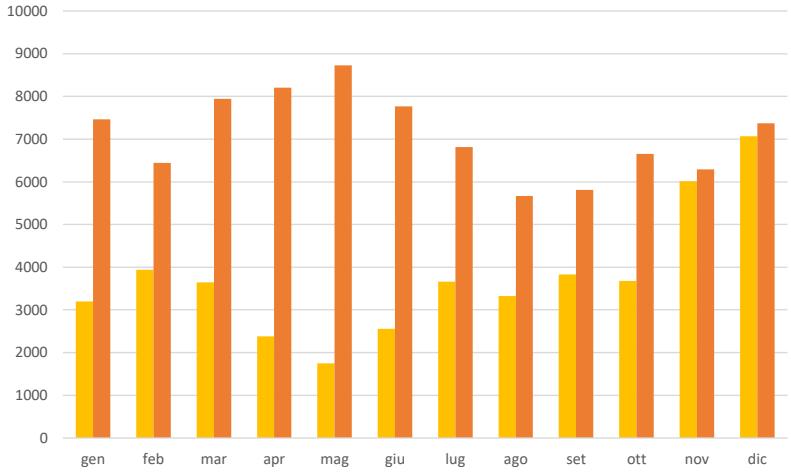


Figura 2 - *Distribuzione temporale del numero di Malware rilevati (Dati Fastweb relativi all'anno 2019/2020)*

Principali famiglie di malware e botnet

Analizzando i trend temporali delle varie tipologie di malware si nota una prima metà dell'anno con un trend in crescita, durante i mesi estivi si evidenza un calo e infine l'ultima parte dell'anno è caratterizzata da una crescita del numero di infezioni da malware con una prevalenza per le infezioni legate a Andromeda e QSnatch.

È importante evidenziare come, gli altri malware abbiano avuto un impatto percentuale più marginale (ma comunque rilevante) relativi a minacce note e diffuse da tempo come Wannacrypt e Mirai.

Per quanto concerne le tipologie di attacco zero-day il trend è stato abbastanza costante e in forte calo rispetto al 2019 anche se, secondo quanto rilevato da Fastweb nel tempo, la tipologia, la potenza e l'efficacia di tali attacchi sono comunque da non sottovalutare.

Tali tipologie di attacchi sono infatti più pericolose della media perché non rilevabili da sistemi di protezione tradizionali che necessitano il rilascio di signature per essere identificati (ad esempio gli antivirus).

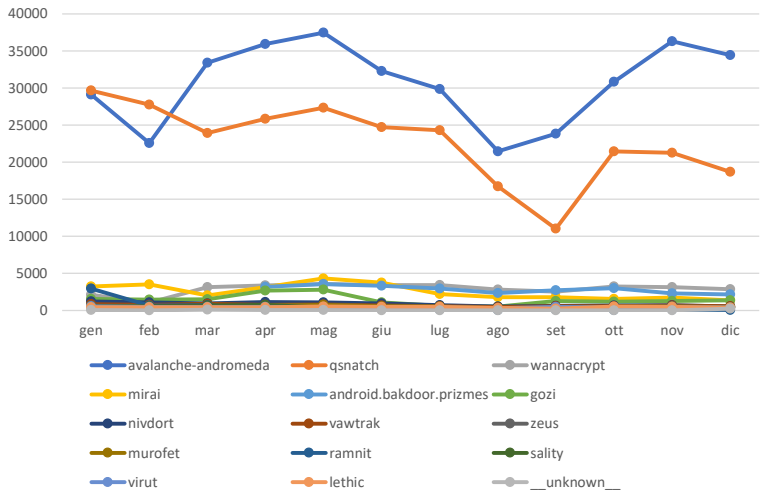


Figura 3 - *Rilevazione mensile dei Malware (Dati Fastweb relativi all'anno 2019)*

Distribuzione geografica dei centri di comando e controllo dei malware

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

Quest'anno oltre l'80% dei centri di C&C relativi a macchine infette appartenenti all'AS di Fastweb si trovano negli Stati Uniti. Tale dato è in leggero calo rispetto all'anno scorso (-2 p.p.) ma comunque resta elevato. Questo principalmente dovuto alla altissima presenza di datacenter/server farm che si concentrano negli Stati Uniti. Al secondo posto, con l'5% circa dei centri di comando e controllo si trova la Germania.

Conseguentemente perdono efficacia le logiche di difesa basate sulla provenienza geografica degli attacchi, perché le organizzazioni cyber-criminali impiegano indirizzi IP distribuiti opportunisticamente in reti che generano grandi volumi di traffico legittimo.

Non è pertanto rilevante da dove proviene l'attacco ma come proteggersi. Risulta quindi necessario attuare meccanismi di protezione che si basino su tecnologie all'avanguardia e centri di competenza specifici come ad esempio l'utilizzo di Security Operation Center o personale specializzato.

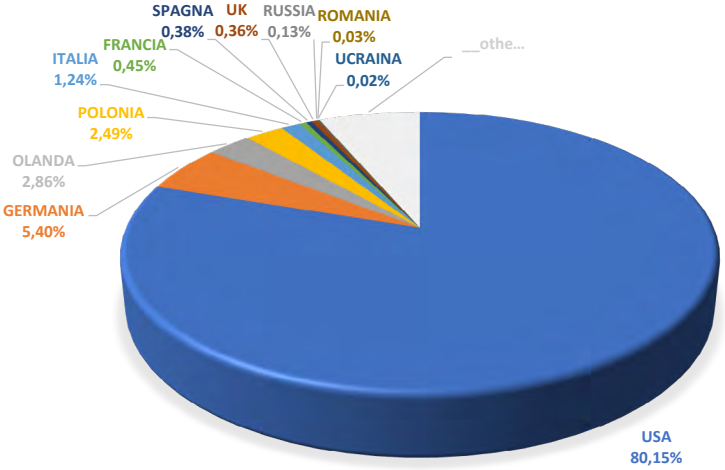


Figura 4 - *Dislocazione dei centri di Comando e Controllo (Dati Fastweb relativi all'anno 2019)*

Attacchi DDOS (Distributed Denial of Service)

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

Alcuni attacchi hanno come target una particolare applicazione o servizio, ad esempio Web, SMTP, FTP, etc., altri invece mirano a mettere fuori uso completamente il server o, addirittura, un'intera rete. Gli attacchi DDoS (distributed denial of service) amplificano la portata di tali minacce. Un attacco DDoS viene infatti realizzato utilizzando delle botnet, ovvero decine di migliaia di dispositivi (non più solo computer di ignari utenti), in grado di generare richieste verso uno specifico target con l'obiettivo di saturarne in poco tempo le risorse e di renderlo indisponibile.

Naturalmente gli effetti di un attacco DDoS possono essere devastanti sia a causa della potenza che possono esprimere, ma anche per le difficoltà insite nel poterli mitigare in tempi rapidi (se non attraverso la sottoscrizione di uno specifico servizio di mitigation).

Il mercato dei DDoSaaS (DDoS as a service) è cresciuto ed il costo del servizio si aggira sui 5-10$ mese per botnet in grado di erogare un attacco di 5-10 minuti ad oltre 100Gbps.

Quanti sono stati gli attacchi DDOS nel 2020?

Nel 2020 sono state rilevate circa 15.000 anomalie riconducibili a possibili attacchi DDoS diretti verso i Clienti Fastweb (in linea con quanto rilevato rispetto all'anno 2019).

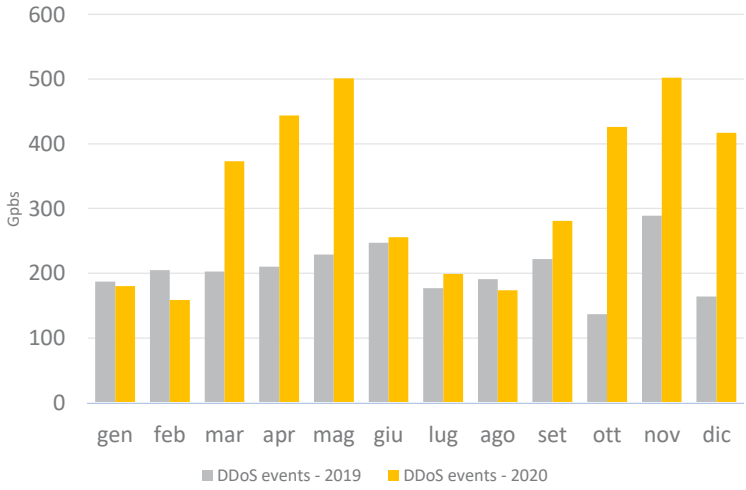


Figura 5 - *Distribuzione mensile delle anomalie DDoS (Dati Fastweb relativi all'anno 2019/2020)*

Quali sono i settori più colpiti

In merito all'analisi della distribuzione dei target degli attacchi DDoS sono stati individuati i settori merceologici maggiormente colpiti da questo tipo di attacchi.
Come si evince dal grafico successivo, il fenomeno riguarda senza esclusione un esteso numero di settori, tra i quali i più esposti risultano essere il mondo del finance/insurance e il mondo dei servizi che sono obiettivo nel 54% dei casi, a seguire il mondo della pubblica amministrazione, quindi i service provider e il mondo dei media (**Figura 6**).

Il volume degli attacchi DDoS

Il grafico seguente rappresenta il volume degli attacchi DDoS durante l'anno. La piattaforma di mitigation utilizzata per la protezione dei clienti, gestisce ogni mese attacchi che occupano una banda variabile tra i 2 Tbps e gli 8 Tbps, in fortissima crescita rispetto all'anno precedente.
Come si può notare il trend è influenzato da picchi, in corrispondenza dei periodi di lockdown dovuti all'emergenza COVID19 (**Figura 7**).

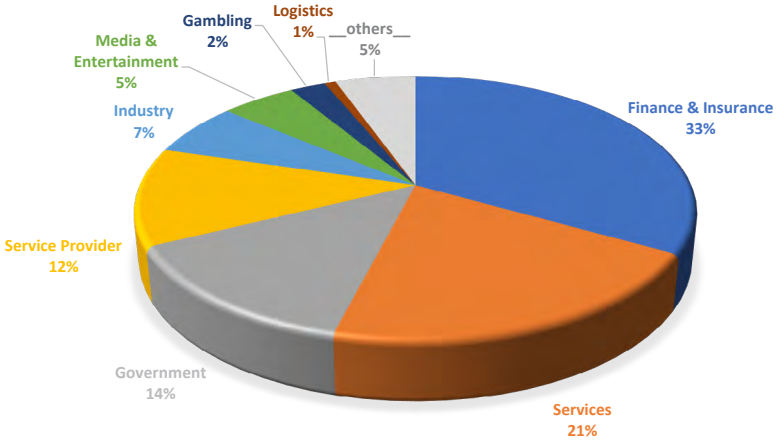


Figura 6 - *Target di possibili attacchi DDoS (Dati Fastweb relativi all'anno 2020)*

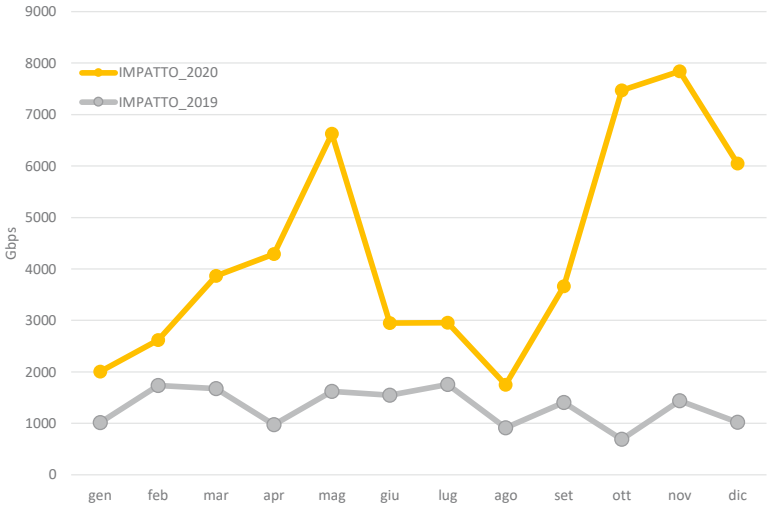


Figura 7 - *Banda totale mensile impegnata negli attacchi DDoS (Dati Fastweb relativi all'anno 2019/2020)*

Di seguito invece viene riportata la distribuzione della banda media di un attacco DDoS nel 2020.

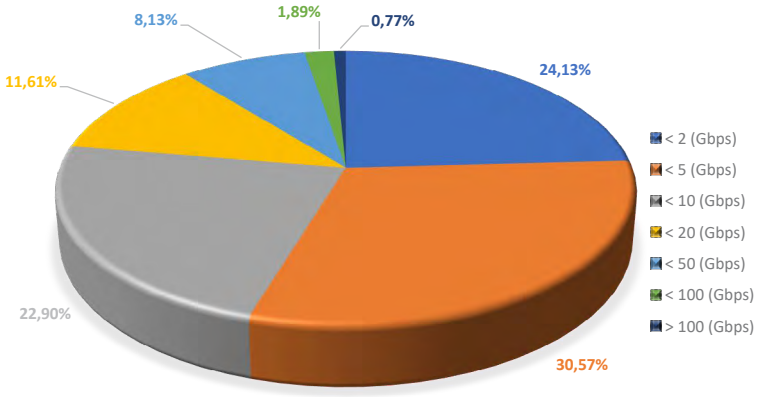


Figura 8 - *Distribuzione della dimensione di un attacco DDoS (Dati Fastweb relativi all'anno 2020)*

Qual è la durata di un attacco DDoS?

Le tecniche di attacco DDoS e i relativi metodi di mitigazione si evolvono nel tempo. Nel corso degli anni, con il consolidamento delle tecniche di difesa, la durata degli attacchi è mediamente diminuita. Anche quest'anno tale trend è confermato, risulta quindi evidente come ci sia una crescente consapevolezza da parte delle vittime degli attacchi e come queste ultime investano per garantire alla propria azienda la protezione da attacchi di tipo DDoS.

Si è osservato che quest'anno circa il 93% degli attacchi è durato meno di 3 ore, mentre i rimanenti casi sono principalmente riconducibili a diversi tentativi effettuati in sequenza ravvicinata. È importante però evidenziare che solo una piccola parte degli attacchi dura oltre le 24 ore consecutive. Rispetto all'anno precedente non si notano particolari differenze, soprattutto se si considerano gli attacchi di piccola durata.

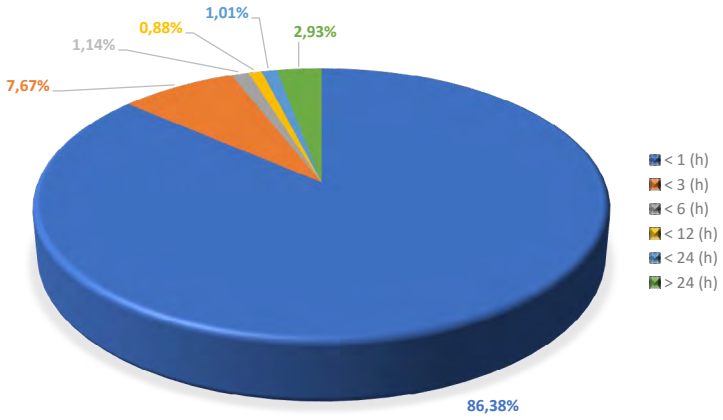


Figura 9 - *Durata dei possibili attacchi DDoS (Dati Fastweb relativi all'anno 2020)*

Tecniche di attacco utilizzate

Le tecniche di attacco utilizzate possono essere diverse, nel 2020 sono state tre le principali tipologie ricorrenti rilevate, con una prevalenza di attacchi di tipo "IP Fragmentation" (17% del totale) e "DNS amplification" (15% del totale).

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

Il secondo e il terzo attacco più diffuso sfruttano invece una tecnica che permette di fare "rimbalzare" il traffico su server DNS o NTP impropriamente configurati. Grazie a questo "rimbalzo" e alle caratteristiche dei servizi DNS e NTP, l'attaccante ottiene il doppio scopo di nascondere i propri indirizzi IP (e quindi la propria identità e collocazione geografica) e di moltiplicare la portata dell'attacco: per ogni megabit di banda immesso dall'attaccante, la vittima riceve da 30 a 50 megabit di traffico indesiderato nel caso della DNS amplification e ben 500 megabit nel caso della NTP amplification.

L'amplificazione del traffico è ciò che consente all'attaccante di rendere irraggiungibile il sito (o servizio) della vittima, saturandone la banda disponibile.

Infine, è da evidenziare come gli attacchi combinati (tecnica mista) siano aumentati sensi-

bilmente, dal 40% del 2019 al 52% del 2020. Tale fenomeno è indice del fatto che attacchi diversificati hanno maggiore probabilità di essere efficaci a causa della loro maggiore complessità per gestire la controparte difensiva.

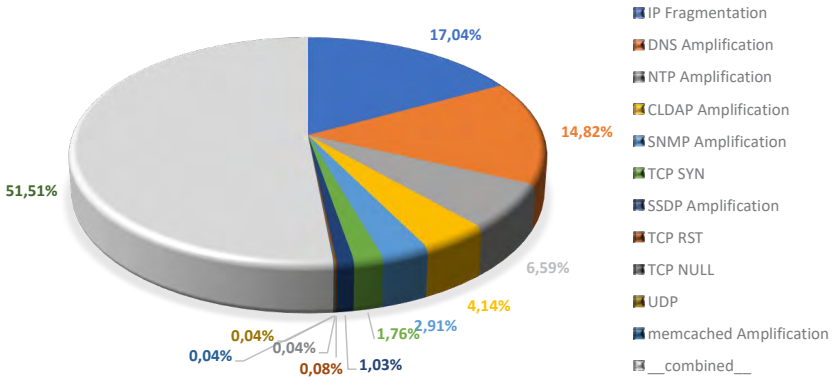


Figura 10 - *Tipologie di attacchi DDoS (Dati Fastweb relativi all'anno 2020)*

Ulteriori vulnerabilità

Servizi critici esposti su Internet

In questo paragrafo viene messo in evidenza il numero di dispositivi che espongono servizi direttamente su Internet privi anche di livelli minimi di protezione. Ciò significa che questi host sono facilmente attaccabili e esposti a rischi elevati di compromissione.

I dati del 2019 riportano circa 53.000 macchine che espongono servizi critici direttamente su Internet con un decremento rispetto all'anno scorso di circa il 18%. Come anticipato, si ritiene che questo fenomeno sia dovuto al fatto che le aziende hanno incrementato le linee difensive di base installando e configurando firewall per abilitare lo smartworking e garantire l'accesso ai dati da remoto.

Al primo posto troviamo Telnet, protocollo utilizzato per la gestione di host remoti, accessibile da riga di comando. Al secondo posto RDP utilizzato per la connessione remota ad un PC. Un attaccante potrebbe sfruttare questo protocollo per prendere il controllo completo della macchina.

Di rilievo è anche la quantità di macchine che espongono Netbios e SMB, quest'ultimo utile per la condivisione di file e stampanti nelle reti locali ma che se esposto su internet può essere utilizzato per accedere ai documenti e file condivisi.

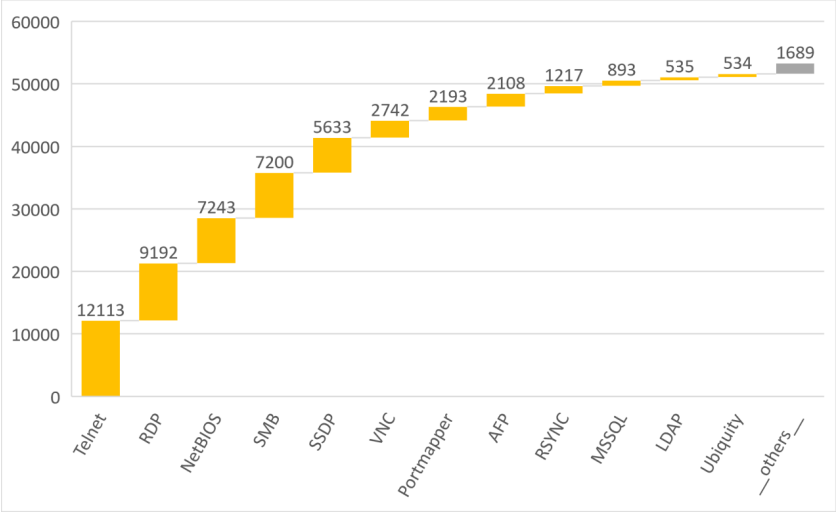


Figura 11 -*Servizi esposti direttamente su Internet (Dati Fastweb relativi all'anno 2020)*

Blocklist

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

Esistono diversi motivi per cui si può essere inseriti nelle liste di blocco, di seguito vengono analizzati i principali:

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

Dalle rilevazioni effettuate si è notato che circa 4.700 IP sono stati inseriti almeno una volta nelle blocklist durante il 2020. Il dato è in sensibile calo rispetto al 2019 dove si erano registrate oltre 7.300 azioni di blocklisting. Il grafico di seguito rappresenta le città maggiormente colpite.

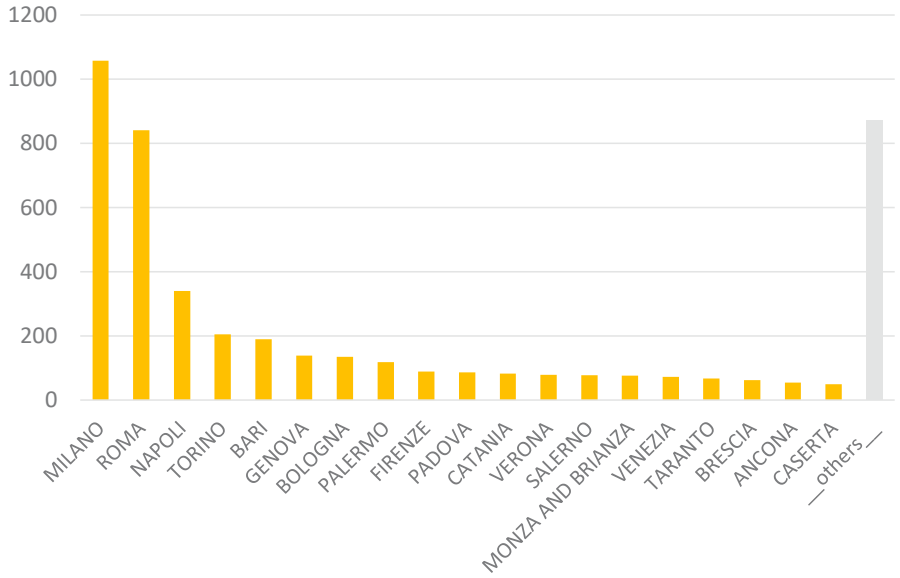


Figura 12 - *Host in Blacklist per città (Dati Fastweb relativi all'anno 2020)*

Ransomware 2020 in Italia – Dalla pesca a "strascico" agli attacchi mirati double extortion… ma non solo

[A cura di Enrico e Gianfranco Tonello, TG Soft]

Nel 2020, anche in Italia, i Ransomware, malware in grado di cifrare i file di dati con l'obiettivo di richiederne un riscatto in denaro generalmente attraverso pagamenti in crypto valute (BTC Bitcoin o altre), per raggiungere l'obiettivo ed eludere i sistemi di difesa di cui gli enti ed imprese si sono progressivamente muniti, hanno iniziato anche ad esfiltrare i file di dati delle vittime minacciandone la diffusione pubblica.

I ransomware fino a qualche tempo fa si "limitavano":
- a cifrare i file di dati;
- a tentare di cancellare i file di ripristino dei più comuni sistemi di backup se, erano, in qualche modo accessibili;
- alla cancellazione delle copie Shadow.

L'obiettivo era quello di costringere la malcapitata vittima al pagamento del riscatto per ottenere la chiave di de-cifratura dei file e riconquistarne l'accesso.

Già dal 2019, o forse prima, si sono iniziati a vedere attacchi ransomware che, oltre a cifrare i file, ne facevano 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.
Questa tecnica di "doppia" estorsione viene oggi chiamata **double extortion**.

Tutto questo per indurre la vittima a pagare il riscatto non solo per la decifratura, ma anche (e soprattutto) per evitare di vedere i propri dati aziendali, contabilità, dati della clientela, progetti, segreti industriali e quant'altro diventare di pubblico dominio. Questa situazione oltre al danno d'immagine, nel caso di diffusione di dati personali e ancora di più se sensibili, può essere sanzionata pesantemente dal Garante Privacy in attuazione al GDPR che, è bene ricordarlo, possono arrivare fino al 4% del fatturato aziendale WW (World Wide) fino ad un massimo di 20 milioni di €.

Le modalità di attacco Ransomware più comuni

Come già noto, nel passato, gli attacchi Ransomware avvenivano principalmente sfruttando l'ingegneria sociale dove attraverso una "semplice" comunicazione via e-mail i cyber malfattori tentavano di far cadere il malcapitato ricevente nella loro trappola. Questa metodologia è andata scemando nell'ultimo periodo, prediligendo l'attacco mirato ad importanti aziende.

I vettori di infezione dei ransomware nel 2020 sono stati i seguenti:
1. Campagna Malspam per attacchi massivi:
   a. aprire un allegato dove da questo si scatenava nell'immediatezza la cifratura dei file;
   b. cliccare su un link che portava all'esecuzione di un file dal quale si attivava il processo di cifratura malevolo.
2. Navigazione su siti compromessi
3. Attacchi mirati:
   a. accesso via RDP (Remote Desktop Protocol).
4. Vulnerabilità della rete aziendale.

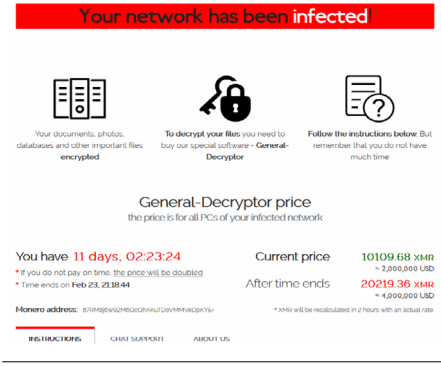
Già nel 2017 si erano iniziati a vedere attacchi un po' più sofisticati che, non solo attraverso le e-mail e la "complicità" di un utente disattento, procedevano attaccando PC o Server esposti sul Web ove fossero presenti vulnerabilità non "patchate" sfruttandole per inoculare malware. Attraverso lo spostamento laterale si propagavano poi nella rete locale per cifrare il maggior numero di computer possibili.
Un'altra metodologia utilizzata in quegli anni è stata la "Supply Chain" che attraverso aggiornamenti di software legittimi veicolavano malware.
Tra gli esempi più noti ricordiamo WannaCry (2017 vulnerabilità EternalBlue) e il ransomware NotPetya (aggiornamento software MEDoc e vulnerabilità EternalBlue), attribuito al governo della Russia.

Oltre a questo i cyber ricattatori si sono mossi andando ad utilizzare tecniche ancora più sofisticate e, seppur continuando con la "pesca" a strascico, hanno intuito che per poter cercare di ottenere riscatti elevati era necessario procedere con attacchi mirati, certamente più complessi, ma che se andati a segno potevano portare a richiedere riscatti ben più corposi. Non più "solamente" qualche centinaia o migliaia di €uro in crypto valuta ma arrivando anche a richiedere centinaia di migliaia di €uro/U$D fino ai casi più estremi, superando il milione di dollari/euro soprattutto nel caso di esfiltrazione di dati.

Due casi recentissimi di attacchi sferrati con il medesimo ransomware #**REvil** aka #**SodinoKibi** praticamente in contemporanea:
(1) attacco via RDP (Remote Desktop Protocol) di sola cifratura file ai danni di un'azienda italiana, che ha visto richiedere:
   - poco più di 963 XMR {Monero} che al cambio del 12/02/2021 corrispondevano circa 200mila U$D / 165mila € se pagato entro le prime 48 ore;
   - riscatto che poi raddoppia passando a quasi 1927 XMR {Monero} che, al cambio del 12/02/2021, equivalevano a 400mila U$D / 330mila €!

(2) attacco ai danni di un'azienda francese con sedi operative anche in Italia che, oltre a cifrare i file di dati segnala, nella richiesta di riscatto anche l'esfiltrazione degli stessi. Il riscatto richiesto è di 2 milioni di dollari che raddoppierà a 4 milioni dopo il 23 febbraio.

(1) *Riscatto Sodinokibi solo cifratura file Fonte: CRAM di TG Soft*



(2) *Riscatto Sodinokibi cifratura+esfiltrazione file - Fonte: CRAM di TG Soft*

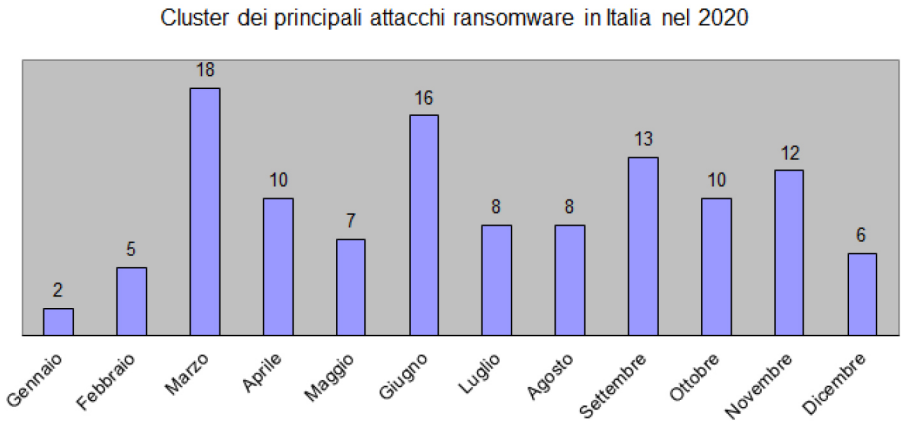
Come si può notare si tratta di due attacchi avvenuti con lo stesso ransomware, ma su due aziende diverse. Il riscatto richiesto, seppur rimanendo importante e raddoppiando dopo una certa data, nel caso della sola cifratura, l'importo richiesto è dell'ordine di qualche centinaia di migliaia di dollari (200/400mila U$D) mentre nel caso di doppia estorsione (double extortion: cifratura + esfiltrazione di dati) la richiesta di riscatto è superiore di un ordine di grandezza passando da qualche centinaia di migliaia di dollari a Milioni di dollari (da 2 a 4 Milioni di U$D).

I Ransomware circolanti in Italia nel 2020

Anche nel 2020, come nei primi mesi del 2021 i Ransomware non hanno mollato la presa "mixando", come detto, campagne di malspam indifferenziate sull'utenza ed attacchi specifici mirati sfruttando gli accessi RDP maldestramente lasciati esposti o vulnerabilità della rete aziendale.

Classificazione dei più importanti attacchi ransomware in Italia

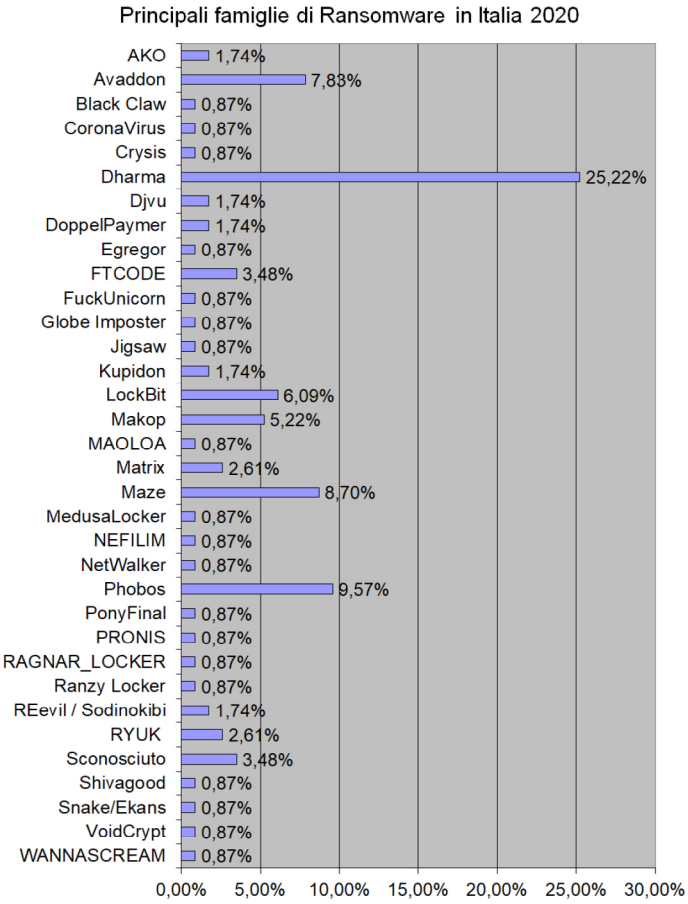
Sono stati verificati e classificati non meno di 115 cluster di attacchi ransomware sia di sola cifratura come anche di esfiltrazione dati (double extortion).



Fonte: Centro Ricerche AntiMalware #CRAM di TG Soft Cyber Security Specialist

Dall'analisi del grafico dei Cluster per mese possiamo notare che vi è un picco nel mese di marzo quando in fretta e furia, a causa dell'emergenza epidemiologia Covid-19, molte aziende sono state costrette, causa provvedimenti governativi (DPCM) che hanno introdotto il *lockdown*, a mettere in tutto o in parte in SMART Working / Lavoro Agile molti dipendenti.

Lo SMART Working / Lavoro Agile ha, di fatto, "autorizzato" i dipendenti ad utilizzare i propri computer fissi o portatili personali che, a causa della vetustà e/o del poco manutenzionamento o per la mancanza di software di protezione aggiornati essendo collegati via internet ai computer della rete aziendale sono diventati, in molte occasioni, la porta d'ingresso di questi attacchi.



**Sconosciuto ➔ Casi di attacchi ransomware, le cui vittime non hanno reso nota la tipologia del ransomware da cui sono stati colpiti. Fonte: Centro Ricerche AntiMalware #CRAM di TG Soft Cyber Security Specialist.*

Come si evince dal grafico sono non meno di trentaquattro le famiglie/tipologie di ransomware distinte che sono state utilizzate per attacchi agli utenti italiani di cui una di queste tipologie è, quasi certamente, di realizzazione italiana o di re-ingegnerizzazione italiana. Si tratta del ransomware FuckUnicorn scoperto/utilizzato nel secondo trimestre 2020. Questo esemplare "autoctono" ha sfruttato l'emergenza epidemiologica Covid-19 per sferrare i suoi attacchi.

Dharma è il ransomware che è stato utilizzato maggiormente dai cyber criminali per attaccare l'utenza italiana. Più di ¼ degli attacchi è avvenuto utilizzando questo agente patogeno.
Phobos, che viene considerato il successore di Dharma in particolare negli attacchi in modalità RDP è stato utilizzato in poco meno del 10% degli attacchi.
Maze, con il suo 8,70% conquista la terza piazza che, visto che si tratta di un ransomware utilizzato per lo più per attacchi mirati di cifratura+esfiltrazione dati (double extortion) è un "ottimo" risultato.
Avaddon, con il suo 7,83% si piazza solo in quarta posizione ma, visto che viene utilizzato con varie modalità di diffusione sia attraverso campagne Malspam come anche per attacchi mirati è ipotizzabile che, nel 2021, possa recuperare qualche posizione.
LockBit, con il suo 6,09% guadagna la quinta posizione.

Ransomware 2020 in Italia ➔ primo trimestre 1 gennaio – 31 marzo

In questo trimestre [3] [4] [5] si è rilevata una flessioni di attacchi ransomware di **Ryuk** [6] e **FTCode** [7] molto attivi nel 2019. Sebbene, dal mese di gennaio fino a circa metà febbraio siano continuate le campagne di malspam di Emotet con la veicolazione anche di **Trickbot**, quest'ultimo però non ha attivato lo stadio dell'attacco ransomware di **Ryuk**.

A parziale compensazione di queste "mancanze" sono stati registrati attacchi di nuovi attori nel mondo dei ransomware:
- **AKO** riconducibile ad una variante di **MedusaLocker**
- **PrOnIs**, molto probabilmente deriva da "**0p3nSOurc3 X0r157**"
- **CoronaVirus**
- **Jigsaw**

In questa prima parte dell'anno sono stati riscontrati cluster di attacchi che hanno visto l'utilizzo dei seguenti ransomware:

- Phobos	- AKO	- PrOnIs	- Dharma	- FTCode
- MedusaLocker	- Jigsaw	- Ryuk	- CoronaVirus	- Maze

Nel trimestre gli attacchi ransomware sono stati sferrati attraverso le modalità:
- RDP (Remote Desktop Protocol) [8];
- Drive-By-Download.

Segnaliamo che gli attacchi **RDP** avvenuti a gennaio che hanno permesso un accesso abusivo al sistema per eseguire direttamente il ransomware, nello specifico i cyber criminali hanno utilizzato nella maggior parte dei casi **Phobos** che deriva e sta raccogliendo l'eredità di **Dharma** il quale aveva la peculiarità di essere uno dei preferiti dai cyber malfattori negli attacchi **RDP**.
In marzo rispetto a febbraio si rileva un aumento degli attacchi via RDP.

L'incremento degli attacchi è probabilmente riconducibile al lockdown causato dal Covid-19 che ha comportato un maggiore utilizzo del protocollo RDP, esponendo l'infrastruttura aziendale a rischi di attacchi attraverso gli accessi esterni permettendo ai cyber criminali attacchi ransomware diretti.
Per la massiva offensiva degli attacchi via **RDP**, in marzo, i cyber criminali hanno utilizzato **RYUK, Phobos, Dharma** e **MedusaLocker.**
Per gli attacchi double extortion il **Maze** ha rivendicato l'attacco ad un'importante azienda meccanica lombarda.

Ransomware 2020 in Italia ➔ secondo trimestre 1 aprile – 30 giugno

In Italia i principali attacchi ransomware [11] [12] [13] sono giunti da:

- REvil aka Sodinokibi	- Makop	- Dharma	- LockBit
- FuckUnicorn	- Kupidon	- Avaddon	- Maze

Le principali new entry sono state: **Makop, LockBit** e **Avaddon.**

Prosegue il trend di progressivo incremento degli attacchi via RDP, dovuto al lockdown causato dall'emergenza epidemiologica Covid-19 che, come già segnalato, ha obbligato molti italiani a lavorare da casa, lasciando esposti gli accessi esterni della rete aziendale ad attacchi.
I cyber malfattori, in questo trimestre, per gli attacchi RDP hanno preferito utilizzare **Dharma**. A maggio, in Italia, a dare man forte a Dharma negli attacchi RDP si è notato anche l'utilizzo del ransomware **LockBit**.
Inoltre, sembrerebbe che gli autori di **LockBit** si siano affiliati a quelli del **Maze** per condividere le loro piattaforme di data leak. La richiesta di riscatto del LockBit varia dalla tipologia della vittima, con riscatti richiesti da 1600 U$D in su.

Il nuovo ransomware **Avaddon** [9] ha utilizzato diversi vettori d'infezione per attaccare l'utenza italiana:

- **Phorpiex** (worm, che si è diffuso in Italia attraverso campagne di malspam a giugno). Le vittime infettate entrano a far parte della botnet Phorpiex, che ha diffuso il ransomware Avaddon;
- **Campagne malspam dirette**. Il 30 giugno Avaddon è stato distribuito con una campagna malspam diretta che aveva per oggetto "*Notifica (A2QCS) ufficiale riguardanti possibili violazioni*", con allegato un documento Excel che scaricava direttamente il ransomware.

Un'altra new entry tra i ransomware che hanno attaccato l'Italia nel mese di giugno è **Kupidon.**
Gli attacchi di Kupidon analizzati sono avvenuti via RDP. Il riscatto richiesto era di 1200 $ (dollari USD) in BTC (Bitcoin). La gang dei cyber criminali è probabilmente di origine russa dall'indirizzo email (yandex.ru) visibile nella loro home page.

Per quanto riguarda l'utenza italiana colpita da attacchi double extortion (cifratura & esfiltrazione file), il ransomware **Maze** ha rivendicato gli attacchi a:

- Studio di Architettura e Design
- Primaria Società di costruzioni generali

Nello stesso periodo, a livello mondiale, Maze ha colpito grandi produttori elettronici come LG e Xerox.
A giugno due grandi società italiane, primaria società energetica e primaria società produttrice di calzature, sono state colpite da attacchi informatici.
La società del settore energetico è stata attaccata domenica 7 giugno dal ransomware **Snake/Ekans**, che in precedenza aveva colpito la multinazionale giapponese Honda.

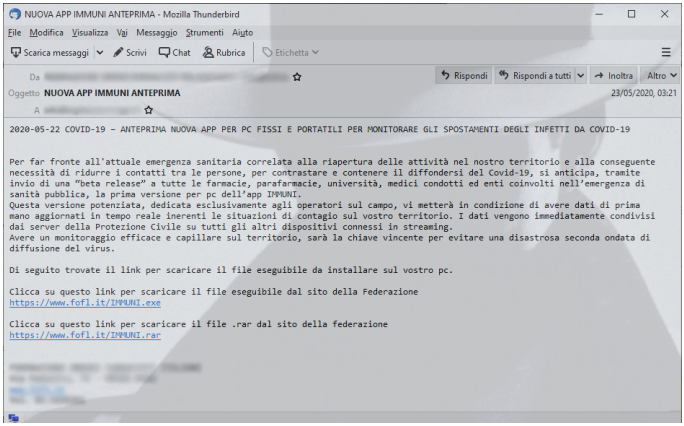
Per quanto riguarda l'attacco subito dalla primaria società del ramo calzaturiero, che è avvenuto domenica 14 giugno, non sono state rilasciate informazioni sulla tipologia di ransomware utilizzato.

FUCKUNICORN – Il ransomware italiano

Il 23 maggio 2020 è stata avviata una campagna malspam in italiano con oggetto "**NUOVA APP IMMUNI ANTEPRIMA**".
Il messaggio invitava ad installare nel proprio PC l'app IMMUNI da un link presente all'interno del messaggio, per far fronte all'attuale emergenza epidemiologica del Covid-19.
Il link in realtà scaricava il ransomware denominato **FUCKUNICORN**.

In figura la nuova immagine dello sfondo cambiata dal ransomware **FUCKUNICORN** al termine della cifratura

Fonte: Centro Ricerche AntiMalware #CRAM di TG Soft Cyber Security Specialist



Mentre il Ransomware cifra i file viene mostrata all'utente la seguente schermata di una mappa raffigurante l'infezione da Covid-19:
Il malware contiene diversi indicatori che fanno ipotizzare che la realizzazione del Ransomware sia italiana.

Il riscatto richiesto è di 300 Euro, da versare in cryptovaluta BitCoin.

"La lunga serpe sul bastone di Asceplio si è ribellata, ed una nuova era sta per sopraggiungere! Questa è la vostra possibilità per redimervi dopo anni di peccati e soprusi. Sta a voi scegliere. Entro 3 giorni il pegno pagare dovrai o il fuoco di Prometeo cancellerà, i vostri dati così come ha cancellato il potere degli Dei sugli uomini. Il pegno è di solamente 300 euros, da pagare, con i Bitcoin al seguente indirizzo: 195naAM74WpLtGHsKp9azSsXWmBCaDscxJ dopo che pagato avrai, una email mandarci dovrai. xxcte2664@protonmail.com il codice di transazione sarà la prova. Dopo il pegno pagato riceverai la soluzione per spegnere il fuoco di Prometeo. Andare dalla polizia o chiamare tecnici a niente servirà, nessun essere umano aiutarti potrà."

Contenuto del file del riscatto

Ransomware 2020 in Italia ➔ Terzo trimestre 1 luglio – 30 settembre

Nel terzo trimestre 2020 [14] [15] [16], gli attacchi ransomware continuano ad utilizzare differenti vettori d'infezione (RDP, navigazione su siti compromessi e campagne malspam).

Sono stati monitorati gli attacchi dei seguenti ransomware:

- Globe Imposter
- Black Claw
- LockBit
- DoppelPaymer
- Matrix
- Phobos
- Crysis
- Makop
- WannaScream
- Avaddon

La maggior parte dei ransomware identificati nel 3° trimestre sono stati veicolati attraverso il desktop remoto (RDP) dopo aver guadagnato un accesso abusivo al sistema.

A luglio hanno fatto la loro comparsa in Italia due nuovi ransomware denominati:

- Black Claw
- WannaScream

Gli attacchi di **Black Claw** analizzati sono avvenuti attraverso intrusione via RDP.
Il ransomware durante la cifratura ai file aggiunge l'estensione ".bclaw".
WannaScream utilizza un'infrastruttura di tipo RaaS (Ransomware-as-a-Service) e all'interno della sua configurazione troviamo il parametro "SOLDIER" che contiene l'ID dell'attaccante. Nel sample analizzato l'attaccante era identificato con la sigla "M-k".

A luglio anche la società ENAC (Ente Nazionale per l'Aviazione Civile) è stata colpita da un attacco ransomware. L'attacco molto probabilmente è avvenuto a partire da venerdì 10 luglio e ha colpito alcuni server dell'Ente Nazionale per l'Aviazione Civile, come indicato in un tweet del 12 luglio. Il sito è stato ripristinato parzialmente alle sue funzionalità solamente dal 17 luglio, circa una settimana dopo l'attacco subito.

Ad agosto il gruppo cyber criminale di **REvil** (aka **Sodinokibi**) [10] ha colpito un'azienda italiana distributrice di ricambi auto del modenese chiedendo un riscatto di 125.000 dollari per non far partire l'asta dei dati esfiltrati.

Nel mese di settembre è stata individuata una campagna di malspam atta a veicolare il ransomware della famiglia Avaddon. La campagna di malspam con oggetto "*È stata presentata una citazione a carico della Sua società, in merito a una fattura non dichiarata*", si spacciava come proveniente dall'Agenzia delle Entrate e conteneva un link malevolo che reindirizzava la vittima verso un finto portale dell'Agenzia delle Entrate.

Nel 3° trimestre il gruppo cyber criminale del **Maze** ha attaccato diverse società italiane alle quali, oltre ad operare la cifratura dei file ha effettuato esfiltrazione dati dandone notizia nel loro sito di data leak:

- S.p.A. lombarda distributrice di dispositivi medici
- S.p.A. lombarda leader pressofusione leghe di zinco
- Primaria Fondazione Culturale veneta
- S.r.l. campana gestione rifiuti
- S.p.A. piemontese produttrice film per imballaggi alimentari
- S.p.A. piemontese ramo alimentare distributrice formaggi grattugiati
- Società altoatesina specialista ICT e telecomunicazioni

Nel 3° trimestre DoppelPaymer ha rivendicato l'attacco informatico ad una S.p.A. campana Multiutility fornitrice di energia e telefonia con esfiltrazione di documenti riservati.

A settembre non sono finiti gli attacchi ransomware in Italia.
S.p.A. veneta leader mondiale dell'occhialeria è stata costretta a bloccare la produzione per l'intera giornata del 21 settembre a causa di un attacco del ransomware NEFILIM. Università laziale è stata colpita da un attacco che ha compromesso più di 100 computer.

Ransomware 2020 in Italia ➔ Quarto trimestre 1 ottobre – 31 dicembre

Questo trimestre [17] [18] [19] registriamo un aumento degli attacchi ransomware i principali hanno utilizzato le seguenti tipologie/famiglie:

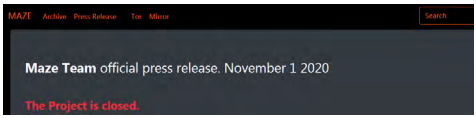
- Dharma
- Avaddon
- VoidCrypt
- RAGNAR_LOCKER
- Makop
- Phobos
- MAOLOA
- Stop/Djvu
- DoppelPaymer
- Ranzy Locker
- ShivaGood
- LockBit
- Matrix
- Egregor

ShivaGood non è un ransomware "nuovo", le prime versione risalgono al 2019.
L'attacco ransomware **Avaddon** questa volta è avvenuto attraverso la navigazione su siti compromessi.
VoidCrypt è stato veicolato attraverso la vulnerabilità della VPN del firewall FortiGate di Fortinet, la quale ha permesso di accedere alla rete locale e quindi di conseguenza ai server tramite RDP.
Gli attacchi attuati dal ransomware **MAOLOA** sono avvenuti attraverso il malware downloader **QakBot** con cui il pc era precedentemente infetto e da cui è stato scaricato il ransomware.
Il ransomware **Stop/Djvu** è stato diffuso attraverso il download di software infetti. La richiesta di riscatto è stata di 490 $.
Anche **Ranzy Locker** è stato diffuso attraverso accesso abusivo via RDP.

Attacchi ransomware double extortion

Il 27 ottobre primaria S.p.A. distributrice di energia è stata colpita da un attacco ransomware con esfiltrazione di dati. A darne notizia è stato il gruppo di cyber criminali di **NetWalker** attraverso un post nel proprio blog nel dark web. Secondo NetWalker avrebbero esfiltrato circa 5 TB di dati.

Il 28 ottobre un'altra S.p.A. italiana multiutility energia e telecomunicazioni è stata colpita da un attacco ransomware con esfiltrazione di dati. A darne notizia questa volta è stato il gruppo di cyber criminali **DoppelPaymer** attraverso un post nel proprio portale nel dark web.



Il mese di novembre inizia con il comunicato stampa di **Maze** che annuncia la chiusura ufficiale del progetto ransomware. Nel comunicato viene rinnegata l'esistenza del cartello Maze e indicato il motivo della chiusura del progetto stesso.

Ad inizio novembre la società italiana tra i leader mondiali del beverage (aperitivi e bevande alcoliche) è stata colpita da un attacco ransomware con esfiltrazione di dati.
A darne notizia questa volta è stato il gruppo di cyber criminali **RAGNAR_LOCKER** attraverso un post nel proprio portale nel dark web.

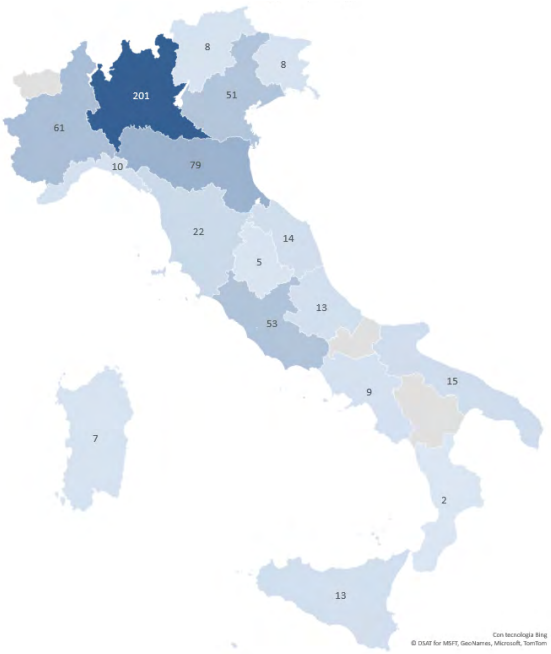
Sempre a novembre il gruppo di cyber criminali di **Egregor** miete un'altra vittima italiana. Si tratta di una coop agricola romagnola che produce ortofrutta biologica.
Il 28 dicembre un'altra società italiana la Snaitech, uno dei principali operatori di gioco legale in Italia, ha annunciato, con un comunicato stampa, di essere stata colpita da un attacco informatico a partire dal 27 dicembre 2020, che ha messo fuori uso il proprio portale.

Vulnerabilità VPN sfruttata per attacchi ransomware

Nel mese di novembre vari cyber criminali hanno pubblicato nei forum del dark web varie liste di IP gestiti dal firewall Fortinet vulnerabili all'exploit CVE-2018-13379.

Il 5 novembre è stato analizzato un attacco ransomware di VoidCript perpetrato sfruttando la vulnerabilità CVE-2018-13379, dove è stato ritrovato un file contenente una lista di 571 IP italiani. In figura la distribuzione geografica di questi IP con target Italia.

Le regioni più colpite sono:
- Lombardia
- Emilia Romagna
- Piemonte
- Lazio
- Veneto



Ditribuzione degli IP per Regione.
Fonte: Centro Ricerche AntiMalware #CRAM di TG Soft

CONCLUSIONI

Il 2020 non è stato solamente un anno difficile a causa della pandemia Covid-19 ma che ha visto i creatori/diffusori di ransomware diventare sempre più agguerriti.
Affinata ormai da anni la corretta implementazione degli algoritmi di cifratura senza particolari errori che non permettono la decifratura senza pagare il riscatto, si sono concentrati sulle tecniche di attacco più efficaci e devastanti dove l'accesso ai PC / Server avviene via RDP o attraverso vulnerabilità della rete aziendale.
L'attacco non si limita alla sola cifratura dei file, ma ne trasferisce una copia per ricattare la vittima anche se questa dovesse essere in grado di ripristinare i file cifrati attraverso, ad esempio, delle copie di backup recenti.
È chiaro che per difendersi da questi attacchi è necessario non solo dotarsi di sistemi di mitigazione che si attivino efficacemente nella fase iniziale dell'attacco e permettano di limitare i danni, ma soprattutto evitare l'esfiltrazione dei dati cioè ridurre le esposizioni di PC e Server agli accessi esterni.

Non è azzardato ipotizzare che il trend-topic degli attacchi ransomware 2021 sarà la double extortion.

Bibliografia

[1] CRAM di TG Soft - *Attacchi #RDP veicolano #Ransomware #REvil aka #Sodinokibi in Italia* - Febbraio 2021
https://twitter.com/VirITeXplorer/status/1360143703906648064?s=1002

[2] CRAM di TG Soft - *Attacco hacker Trigano paralizzata* - Febbraio 2021
https://www.linkedin.com/posts/tg-soft attacco-hacker-trigano-paralizzata-la-activity

[3] CRAM di TG Soft - *Telemetria e statistiche dei virus/malware circolanti in Italia 2020-01* - Febbraio 2020
https://www.tgsoft.it/italy/news_archivio.asp?id=1061

[4] CRAM di TG Soft - *Telemetria e statistiche dei virus/malware circolanti in Italia 2020-02* - Marzo 2020
https://www.tgsoft.it/italy/news_archivio.asp?id=1067

[5] CRAM di TG Soft - *Telemetria e statistiche dei virus/malware circolanti in Italia 2020-03* - Aprile 2020
https://www.tgsoft.it/italy/news_archivio.asp?id=1076

[6] CRAM di TG Soft - *Analisi tecnica del ransomware Ryuk che colpisce le grandi organizzazioni* – Luglio 2019
https://www.tgsoft.it/italy/news_archivio.asp?id=1010

[7] CRAM di TG Soft - *2019W38 Report settimanale => 23-27/09 2K19 campagne MalSpam target Italia* – Settembre 2019 https://www.tgsoft.it/italy/news_archivio.asp?id=1024

[8] CRAM di TG Soft - *Continuano gli attacchi Ransomware con violazione degli accessi RDP* – Agosto 2019
https://www.tgsoft.it/italy/news_archivio.asp?id=1013

[9] CRAM di TG Soft - *2020W26 Report settimanale => 27/06-03/07 2K20 campagne MalSpam target Italia* – Giugno 2020 https://www.tgsoft.it/italy/news_archivio.asp?id=1102

[10] CRAM di TG Soft - *Analisi tecnica del ransomware REvil - Sodinokibi e Threat Intelligence Report* – Giugno 2019 https://www.tgsoft.it/italy/news_archivio.asp?id=1004

[11] CRAM di TG Soft - *Telemetria e statistiche dei virus/malware circolanti in Italia 2020-04* - Maggio 2020
https://www.tgsoft.it/italy/news_archivio.asp?id=1084

[12] CRAM di TG Soft - *Cyber-Threat Report degli attacchi informatici di maggio 2020 in Italia* - Giugno 2020
https://www.tgsoft.it/italy/news_archivio.asp?id=1093

[13] CRAM di TG Soft - *Cyber-Threat Report degli attacchi informatici di giugno 2020 in Italia* - Luglio 2020
https://www.tgsoft.it/italy/news_archivio.asp?id=1103

[14] CRAM di TG Soft - *Cyber-Threat Report degli attacchi informatici di luglio 2020 in Italia* - Agosto 2020
https://www.tgsoft.it/italy/news_archivio.asp?id=1118

[15] CRAM di TG Soft - *Cyber-Threat Report degli attacchi informatici di agosto 2020 in Italia* - Settembre 2020
https://www.tgsoft.it/italy/news_archivio.asp?id=1125

[16] CRAM di TG Soft - *Cyber-Threat Report degli attacchi informatici di settembre 2020 in Italia* - Ottobre 2020
https://www.tgsoft.it/italy/news_archivio.asp?id=1137

[17] CRAM di TG Soft - *Cyber-Threat Report degli attacchi informatici di ottobre 2020 in Italia* - Novembre 2020
https://www.tgsoft.it/italy/news_archivio.asp?id=1149
[18] CRAM di TG Soft - *Cyber-Threat Report degli attacchi informatici di novembre 2020 in Italia* - Dicembre 2020 èhttps://www.tgsoft.it/italy/news_archivio.asp?id=1161
[19] CRAM di TG Soft - *Cyber-Threat Report degli attacchi informatici di dicembre 2020 in Italia* - Febbraio 2021
https://www.tgsoft.it/italy/news_archivio.asp?id=1169

Email security: i trend italiani del 2020

[A cura di Rodolfo Saccani, Libraesva]

Questo report sull'andamento della email security in Italia nel 2020 deriva dall'analisi di un campione di 10 miliardi di email ricevute in Italia dagli apparati di Libraesva. Il campione è rappresentativo del traffico di posta in Italia e comprende tipologie di traffico eterogenee (aziende di ogni dimensione, ISP/MSP, consumer, education, istituzionale, etc).

Un anno movimentato

Il 2020 è stato caratterizzato dalla pandemia di COVID-19 che ha condizionato quasi tutti gli aspetti delle nostre esistenze: lavoro, socialità, abitudini, libertà personali, rapporti interpersonali, emotività, spostamenti, acquisti, eccetera.
La posta elettronica è uno dei principali canali di comunicazione del nostro tempo, è il canale principale in assoluto se consideriamo le attività aziendali. Per noi che ci occupiamo di email security le tracce della pandemia sono rimaste ben visibili nei pattern di comunicazione via posta elettronica.
Le modalità di comunicazione sono cambiate (basti pensare al lavoro da remoto), i contenuti delle comunicazioni hanno visto ondate di argomenti quasi esclusivamente legati all'evento pandemico (soprattutto in concomitanza con i principali provvedimenti restrittivi), gli aspetti legati alla sicurezza, alla privacy, agli attacchi di phishing e alla distribuzione di malware sono stati pesantemente condizionati dalla pandemia. Se vogliamo, l'evento pandemico ha ancora più messo in evidenza la rilevanza del fattore umano nella sicurezza delle comunicazioni elettroniche.

Il COVID-19 ha offerto innumerevoli nuovi spunti per campagne di phishing veicolate via email, spunti che sono stati prontamente colti e utilizzati in campagne malevole.
Ricordiamo che una campagna di phishing efficace è caratterizzata da tre elementi principali: il presentarsi come una fonte autorevole, la capacità di catturare l'attenzione della vittima, quella di instillare un senso di urgenza al fine di indurre a compiere un'azione dannosa come aprire un allegato malevolo, cliccare su un link, fornire credenziali o informazioni confidenziali. Autorevolezza, cattura dell'attenzione, senso di urgenza, call-to-action ... se ci facciamo caso parliamo esclusivamente di leve che agiscono su aspetti affatto tecnici ma legati ai comportamenti umani.
Non è difficile immaginare come un evento eccezionale come quello pandemico con tutto il suo carico emotivo, il flusso continuo di nuove informazioni, il susseguirsi di provvedimenti normativi, i cambiamenti delle modalità di lavoro e delle abitudini di vita, abbia creato un terreno molto fertile per gli autori di campagne di phishing.
Abbiamo monitorato nel corso dell'anno il trend delle comunicazioni relative alla pandemia di COVID-19. Il seguente grafico mostra l'andamento delle mail legittime legate a questo argomento (analisi effettuata attraverso rilevazione di parole chiave presenti nel testo del messaggio).

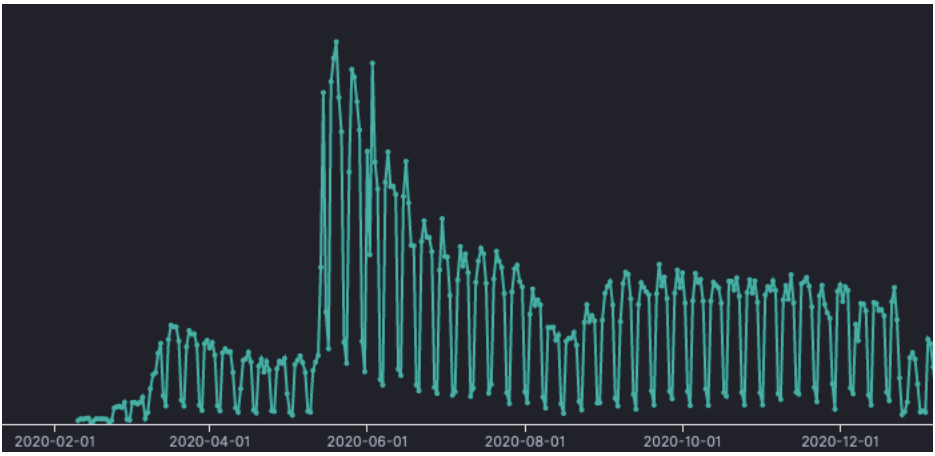


Figura 1 - *Andamento delle mail legittime a tema COVID-19. Fonte: Libraesva*

L'andamento ad inizio anno vede una progressiva crescita di comunicazioni che perdura circa un mese e mezzo e che inizia a decrescere solo dopo il primo lockdown. Segue un grande picco successivo ai primi allentamenti del lockdown. In questo periodo si susseguono incessantemente provvedimenti normativi e disposizioni organizzative. E' del 13 maggio la "legge rilancio" mentre il 15 maggio un decreto delinea il quadro generale all'interno del quale gli spostamenti verranno limitati da ordinanze statali, regionali e comunali. Seguono innumerevoli ordinanze, interpretazioni e chiarimenti oltre a decreti che progressivamente vanno ad autorizzare la ripresa di ulteriori attività. A tutto questo si affiancano informazioni e aggiornamenti sull'andamento della pandemia, sullo stato del sistema sanitario sugli studi clinici che contribuiscono ad una crescente conoscenza del fenomeno.

Indicativamente, in questo periodo il 10% delle nostre mailbox conteneva mail a tema COVID-19. Ricordo che stiamo ancora parlando di comunicazioni legittime, ovvero non malevole, che esplicitamente menzionano la pandemia. E' un indice dell'attenzione che il tema ha avuto nel corso del tempo.

Quello che segue è invece l'andamento delle mail indesiderate a tema COVID-19 che sono state intercettate dai sistemi di filtraggio della posta elettronica. Oltre a mail di spam vero e proprio relative a prodotti e servizi (mascherine, gel, termoscanner, guanti, test antigenici, tamponi, improbabili prodotti anti-covid, servizi finanziari per fronteggiare l'emergenza, eccetera) questo flusso contiene anche mail di phishing e distribuzione di malware che sfruttano l'alto livello di attenzione legato alla pandemia.

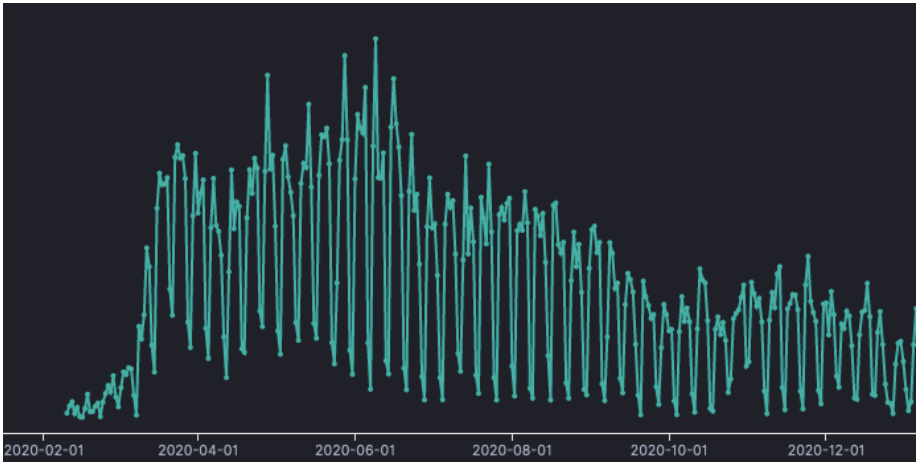


Figura 2 - *Andamento delle mail indesiderate a tema COVID-19. Fonte: Libraesva*

L'andamento delle mail indesiderate è più regolare: nel mese di marzo c'è stata una rapida crescita che poi si è più o meno stabilizzata. Da agosto in poi c'è stata una progressiva lenta decrescita. Questo grafico ci dice che il tema è stato rapidamente adottato da chi intendeva abusarne ed è stato progressivamente abbandonato solo quando ha iniziato a perdere di efficacia.

Quali tattiche sono state utilizzate nelle mail di phishing? Tra le più aggressive abbiamo notato campagne massive di finte mail di licenziamento. La mail, che si spaccia per una comunicazione proveniente dal dipartimento risorse umane, comunica al malcapitato il suo licenziamento in tronco giustificato dall'emergenza COVID. L'esempio di **Figura 3**, nonostante sia scritto in inglese, è stato inviato a numerosi dipendenti italiani di aziende multinazionali.

L'allegato di queste mail è un file html che punta a carpire le credenziali dell'utente (**Figura 4**).

Dear alessandro
Employee Company,

We are deeply saddened to inform you that your term of employment at company has come to an immediate end. Due to the covid-19 epidemic, we have no choice but to end your employment with us.This decision is effective immediately.

Find attached your 2 months salary receipt.

We thank you for your service and we wish it didn't have to end this way.

Sincerely,

Human Resources Manager

cc: ceo@ro

Figura 3 - *Campagna di phishing, finto licenziamento causa COVID. Fonte: Libraesva*

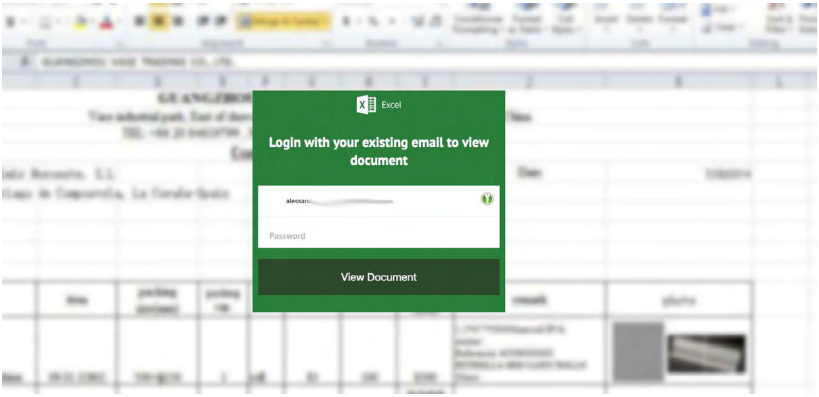


Figura 4 - *Allegato malevolo per carpire credenziali. Fonte: Libraesva*

Naturalmente anche i tentativi di truffa massivi e di bassa qualità sono stati prontamente declinati a tema COVID. Vincite improvvise, donatori inattesi e le classiche truffe "alla nigeriana" hanno adottato le parole chiave legate alla pandemia nel tentativo di guadagnare maggiore visibilità e credibilità.

In occasione dell'espansione delle sue attività, la "Pula alle Uova d'Oro" (una struttura di risparmio e di credito con i suoi partner inglese, europeo, americano) ha lanciato una lotteria a favore di qualsiasi persona fisica giuridica, viva o meno in Africa ma con un indirizzo elettronico, questa lotteria è stata organizzata con l'obiettivo di aiutare il mondo intero a seguito del disastro del CORONAVIRUS (COVID - 19)) che rende triste il mondo intero e promuove i progetti della nostra struttura di risparmio da (la gallina alle uova) d'oro verso altri paesi del continente.

La Tombola è stata supervisionata da un avvocato. Il suo indirizzo e-mail è stato estratto a sorte, definendola il vincitore del terzo premio che rappresenta la somma di 60.000 euro.

Primo premio: una villa duplex in Piazza Haie viva

2° prezzo: una somma di 70.000 euro + 05 computer (Schermo al plasma, Pentium 4)

Terzo premio: una somma di 60.000 euro

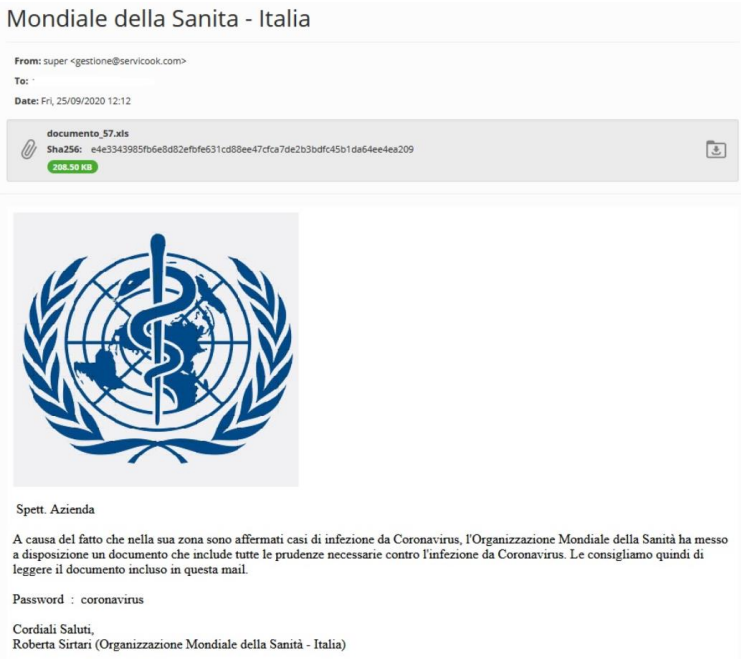
4° prezzo: una somma pari a 25.000 euro + 5 congelatori (Sharp)

Le chiediamo di contattare con urgenza l'avvocato incaricato della supervisione e della consegna dei lotti di questa lotteria alla persona di:

Maestro Junior Debaule,

Figura 5 - *Truffa a tema COVID. Fonte: Libraesva*

Numerose e più subdole le mail che, spacciandosi per organismi istituzionali, come ad esempio l'Organizzazione Mondiale della Sanità, avvisavano di presunti allarmi per la presenza di cluster di contagio nell'area.


Mondiale della Sanita - Italia

From: super <gestione@servicook.com>
To:
Date: Fri, 25/09/2020 12:12

documento_57.xls
Sha256: e4e3343985fb6e8d82efbfe631cd88ee47cfca7de2b3bdfc45b1da64ee4ea209
208.50 KB

Spett. Azienda

A causa del fatto che nella sua zona sono affermati casi di infezione da Coronavirus, l'Organizzazione Mondiale della Sanità ha messo a disposizione un documento che include tutte le prudenze necessarie contro l'infezione da Coronavirus. Le consigliamo quindi di leggere il documento incluso in questa mail.

Password : coronavirus

Cordiali Saluti,
Roberta Sirtari (Organizzazione Mondiale della Sanità - Italia)

Figura 6 - *Campagna di phishing che si spaccia per OMS. Fonte: Libraesva*

Altrettanto diffuse le campagne di phishing legate alla ripresa delle attività produttive con finte email del MEF o di altri organismi istituzionali veicolanti malware.
L'utilizzo di nomi e loghi istituzionali conferisce una percezione di autorevolezza che abbassa le difese, in particolare in un momento in cui la paura e l'emotività sono ancora alte.


Progetto riapertura parziale dell' attivita economica ai fini della ripartenza dell'economia: indicazioni per le attivita

From: conferma <super@economicoppo.casa>

To:

Date: Tue, 17/11/2020 01:55

sviluppo_economico_11_.139.zip

Sha256: 02daac8c4efb72e720fca1836c6c31fddfa9a2771ee1089af122340313d1f1fe

52.01 KB

Ministero dell'Economia e delle Finanze

Oggetto: Progetto riapertura graduale dell'attivita commerciale e produttiva ai fini della ripartenza dell'economia: indicazioni per le attivita

Il ministro dell'economia e delle finanze;

DISPONE URGENTEMENTE ai titolari d'impresa di verificare mediante l'archivio allegato a questa email le ultime modifiche effettuate alle ordinanze e l'eventuale corrispondenza della loro categoria di attivita all'interno dei nuovi elenchi di attivita limitate , ed eventuali modalita associate, allo scopo di gestire le riaperture con un ragionevole anticipo.

(Disposizioni finali)
Le disposizioni del presente decreto producono effetto in data 20/11/2020

Roma, ""17/11/2020""

Figura 7 - *Campagna di phishing che si spaccia per il MEF. Fonte: Libraesva*

Con l'arrivo dell'app Immuni le campagne di phishing hanno incominciato a sfruttare questo nuovo filone. La **Figura 8** è tratta da un sito di phishing che riproduce una finta pagina del Play Store di Google:

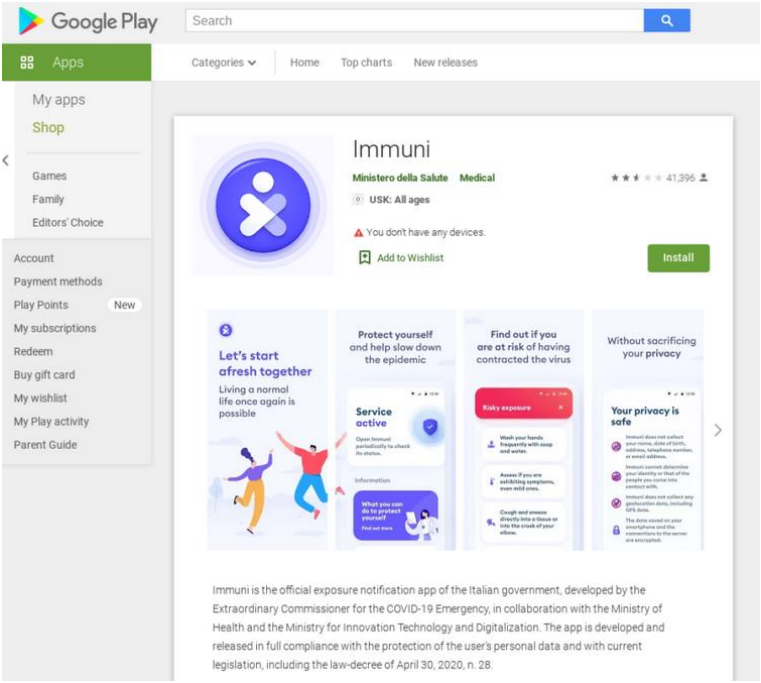


Figura 8 - *Finta app Immuni su un finto Google Play Store. Fonte: Libraesva*

L'anno si è chiuso con l'arrivo del cashback e non potevano mancare campagne di phishing a tema cashback o SPID.

Figura 9 - *Phishing sul cashback di Stato. Fonte: Libraesva*

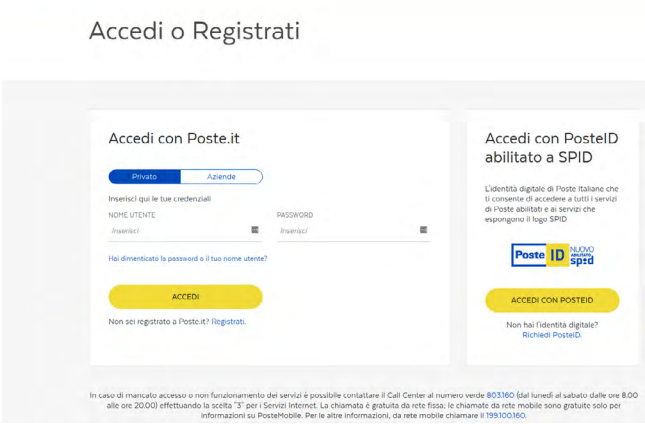


Figura 10 - *Finto sito di Poste Italiane. Fonte: Libraesva*

Anche nelle campagne di email malevole vige una sorta di meccanismo di selezione naturale. Le tecniche che si dimostrano più efficaci vengono copiate si diffondono rapidamente a discapito di quelle meno efficaci. La rapida diffusione delle campagne di phishing a tema COVID-19, in tutte le sue declinazioni, ci ha fornito una misura di quanto sia rilevante il ruolo della componente emotiva e di quanto, a parità di condizioni tecniche, sia il fattore umano a fare la differenza.

L'andamento nel corso dell'anno

Il grafico di **Figura 11** mostra la percentuale di email intercettate dai sistemi di email security sul totale del traffico. Da settembre in avanti la media cala ma si tratta di oscillazioni frequenti e dipendenti da una tale quantità di variabili da non rappresentare in sè un trend particolarmente significativo.

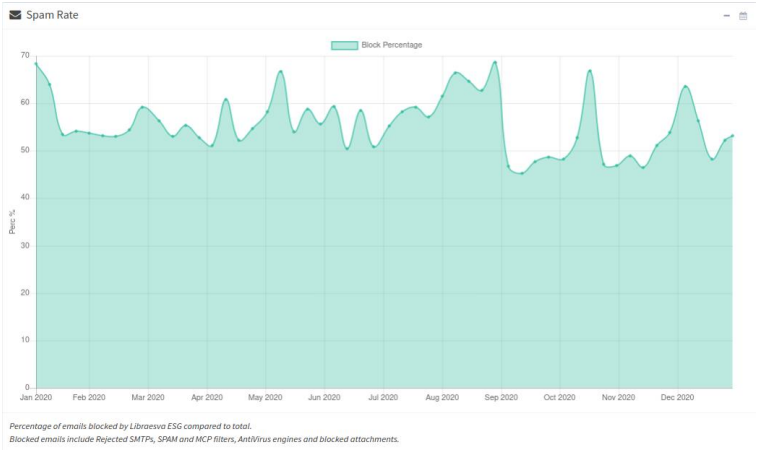


Figura 11 - *Andamento dello spam nel 2020. Fonte: Libraesva*

Malware allegato a messaggi di posta

Già lo scorso anno avevamo rilevato la progressiva perdita di efficacia di sistemi di protezione reattivi, ovvero progettati per intercettare minacce note. Questo approccio (tendenzialmente basato su ricerca di pattern noti) è particolarmente inefficace in presenza di malware polimorfico e nuove varianti, le quali si trovano di fronte a finestre di opportunità di molte ore all'interno delle quali possono transitare senza essere intercettate.

L'approccio proattivo basato sulla rimozione delle istruzioni che abilitano alla realizzazione di un dropper (il codice che installa il malware sul computer della vittima) è l'unico che offre una copertura anche contro nuove varianti e malware polimorfico.

Il grafico di **Figura 12** mostra l'andamento nel corso dell'anno dei sistemi di sandboxing di nuova generazione da noi monitorati. In rosso i file che sono stati bloccati perché riconosciuti come malevoli. In giallo i file che sono stati neutralizzati grazie all'approccio poc'anzi descritto e che non sono stati intercettati dai sistemi reattivi basati su pattern e signature. In verde i file contenenti codice attivo legittimo (come le macro legittime di un file excel).

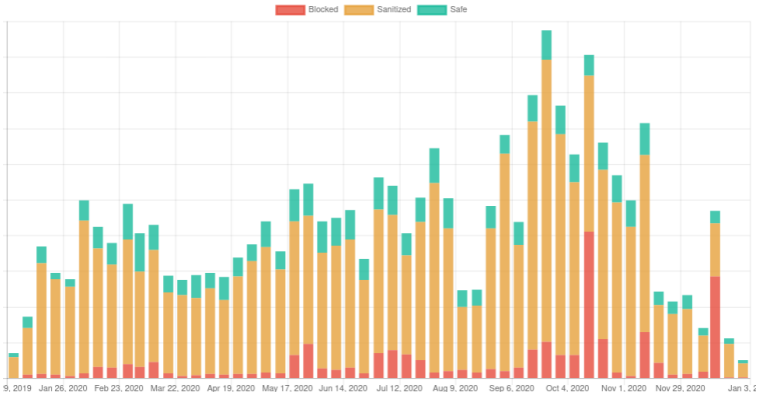


Figura 12 - *Allegati trattati da QuickSand. Fonte: Libraesva*

Nel corso dell'anno abbiamo osservato l'utilizzo di nuove tecniche di realizzazione di dropper. In gennaio ha iniziato a circolare del malware basato su macro in documenti Office che, al fine di eseguire codice senza essere rilevato come malevolo, usava alcune callback VBA (Visual Basic for Applications) che vengono invocate prima di attivare una connessione. Il trucco consiste nell'inserire del contenuto remoto nel documento al fine di indurre Office ad invocare queste macro (il cui nome termina per _onConnecting). Attraverso queste callback è possibile eseguire codice senza invocarlo apertamente, consentendo di svicolare attraverso alcuni sistemi di protezione.

In maggio abbiamo visto un utilizzo smodato (come sempre, una tecnica efficace viene rapidamente copiata da altri attori) delle macro-formule di Office. Si tratta di una vecchissima funzionalità che precede l'introduzione del VBA e di cui quasi nessuno si ricordava più. Un po' come era successo un paio di anni prima con il DDE.

In termini di nuove modalità di attacco degne di menzione, questo è tutto. Si conferma la tendenza prevalente ad affinare le tecniche di attacco e ad aggirare i sistemi di protezione ricorrendo al polimorfismo e ad un grande numero di nuove varianti.

Attacchi attraverso link

E' più facile riuscire a consegnare una mail con un link piuttosto che una mail con allegato un malware, questo è il motivo per cui molti attacchi vengono condotti in questo modo.
I link spesso puntano a siti legittimi che sono stati appena compromessi e che quindi hanno una buona reputazione.

Qual'è la percentuale di email che contiene almeno un link? Il grafico di **Figura 13** mostra questo valore nel corso del 2020.

Figura 13 - *Percentuale di email contenenti almeno un link. Fonte: Libraesva*

Naturalmente tutte le mail che contengono un link ad un sito noto come pericoloso vengono intercettate e bloccate ma, come detto prima, in molti casi si tratta di un link ad un sito legittimo appena compromesso o comunque di un sito non ancora noto come pericoloso. Questo è il motivo per cui è importante che i link vengano verificati anche al momento del click, con un sistema di sandboxing dei link che, visitando prima dell'utente la pagina, blocchi la visita in caso di pericolo.

Quanti sono i link che vengono intercettati da questa ultima rete di protezione? Ce lo dice il grafico di **Figura 14**.

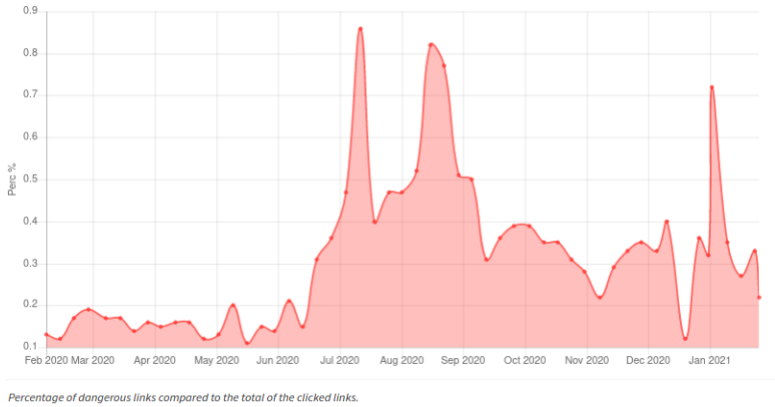


Figura 14 - *Percentuale di click intercettati da UrlSand. Fonte: Libraesva*

Come vediamo si tratta di numeri piccoli, il picco non arriva allo 0.9%. Se in percentuale il valore sembra piccolo, parliamo comunque di diversi milioni di click ciascuno dei quali avrebbe potuto portare ad una compromissione.
Dove sono localizzati i siti a cui puntano questi link malevoli? La mappa di **Figura 15** ci indica la distribuzione.

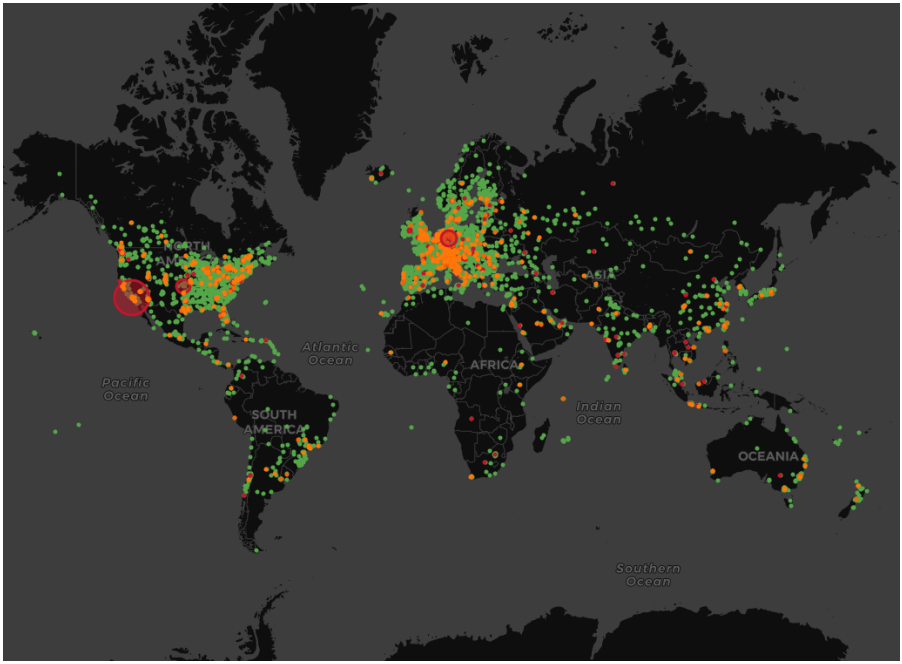


Figura 15 - *Distribuzione geografica siti di malware. Fonte: Libraesva*

Questa è di fatto la distribuzione dei siti che vengono utilizzati per la distribuzione di malware e phishing indirizzati verso utenti italiani.

Conclusioni

Ad oggi le mail malevole sono divenute praticamente indistinguibili dal punto di vista tecnico dalle mail legittime. E' ampiamente diffuso l'abuso di account di posta legittimi (o di servizi commerciali di invio massivo di messaggi di marketing) per l'invio di malware e phishing. Questo rende le mail malevole tecnicamente identiche a quelle legittime. La differenza la fa il contenuto.
D'altro canto intercettare una mail malevola in base alle sue caratteristiche tecniche è più facile che farlo in base al suo contenuto. Estrapolare concetti come "attrarre l'attenzione", "spacciarsi per una fonte autorevole", "fare leva sull'emotività o sull'impulsività" è una sfida

tecnica assai più complessa rispetto al basarsi su elementi tecnici ben più definiti. Questo rende l'email security una disciplina che diviene sempre più specialistica e complessa.

"Artificial Intelligence" e "Machine Learning" sono concetti generici, tutt'altro che nuovi. Sono in uso da decenni in questo settore ma hanno visto una grande evoluzione negli ultimi anni proprio per via di questa tendenza che il settore della email security ha preso: una progressiva riduzione dei "segnali" di ordine tecnico utili a discriminare traffico legittimo da traffico non legittimo e una conseguente crescente rilevanza di "segnali" legati al contenuto. L'ultima evoluzione riguarda un particolare aspetto del machine learning che è legato alla mappatura delle relazioni tra corrispondenti di posta elettronica. Con l'obiettivo di ricostruire qualcosa di più simile possibile al concetto di "fiducia" che nelle conversazioni mediate va perso.

In una conversazione in presenza il volto, il tono della voce, la gestualità veicolano una mole di informazioni enorme. E' principalmente su queste informazioni, oltre che sulla storia della relazione, che inconsciamente stabiliamo il livello di fiducia nell'interlocutore.
Come ricostruire qualcosa di simile al concetto di fiducia in una comunicazione elettronica mediata come quella attraverso la posta elettronica?
Tenendo traccia dello storico e dei pattern di comunicazione tra individui un algoritmo può cercare di stimare l'affinità tra due interlocutori stimando il livello di fiducia. L'analisi dei pattern di comunicazione consente anche di rilevare anomalie e identificare abusi (ad esempio un account takeover) o tentativi di spoofing.
Questa è la prossima frontiera della email security che i vari vendor declineranno, come sempre, ciascuno a modo suo con nomi diversi ("Adaptive Trust Engine" nel caso di Libraesva) e con risultati più o meno efficaci perché non è lo strumento in sé ma il modo in cui lo si utilizza a determinarne l'efficacia.

Stato della cybersecurity nel sud Italia

[A cura di Vita Santa Barletta e Danilo Caivano (Università degli Studi di Bari) e di Luisa Colucci e Domenico Raguseo (Exprivia S.p.a.)]

Introduzione

Il rapporto Clusit 2020 – aggiornamento giugno – ha evidenziato come nel primo semestre del 2020 il numero di attacchi gravi di dominio pubblico siano in crescita del 6,7% rispetto al 2019 (796 contro 850). Ciò è confermato anche dai dati riportati dall'Osservatorio sulla CyberSecurity di Exprivia che registra nell'ultimo anno un incremento del numero di attacchi, incidenti e violazioni di privacy connessi al cybercrime (**Fig. 1**). Un incremento che impatta su diversi settori (**Fig. 2**) e su tutto il territorio nazionale (**Fig. 3**).

Uno scenario che considerando anche gli ultimi eventi pandemici vissuti, tende a crescere. Basti pensare alla trasformazione digitale in corso delle aziende che per sopravvivere devono necessariamente essere "smart". Un termine che negli ultimi mesi è stato utilizzato in diversi contesti e in diverse sfaccettature, ma che non rende sicuramente un'azienda o un dipendente sicuro da attacchi informatici. Anzi, il cambiamento imposto alle aziende per far fronte al periodo di lockdown dovuto al COVID-19 ha reso smart determinate tipologie di attacchi.

Analizzare l'andamento degli attacchi che maggiormente influenzano la percezione delle aziende/enti, permette di delineare non solo linee guida per poter aumentare il livello di sicurezza, ma soprattutto comprendere il problema relativo alla tipologia di vulnerabilità alla quale l'azienda/ente è soggetta.

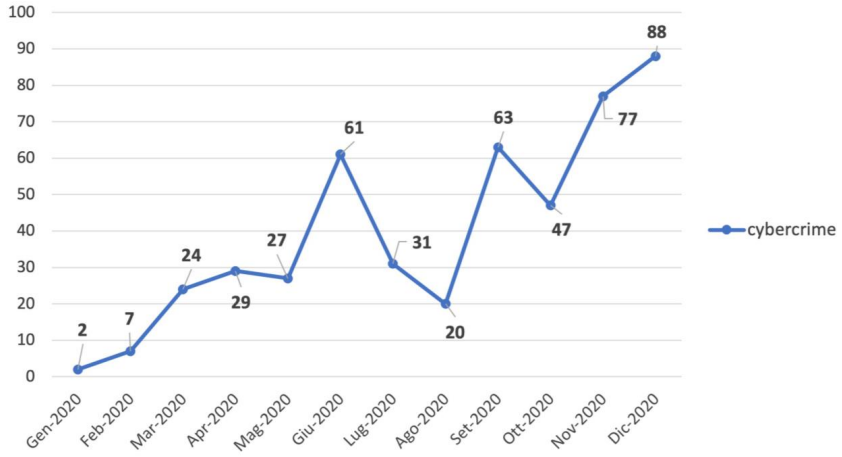


Figura 1 - *Attacchi Cybercrime nel corso del 2020 – Osservatorio Exprivia CyberSecurity*

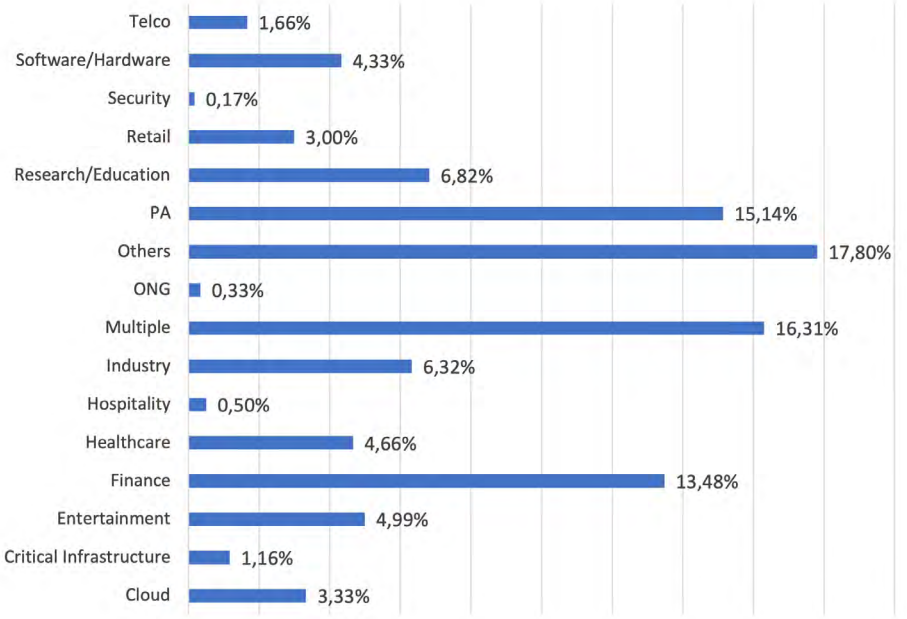


Figura 2 - *Suddivisione per tipologia di vittime - Osservatorio Exprivia CyberSecurity*

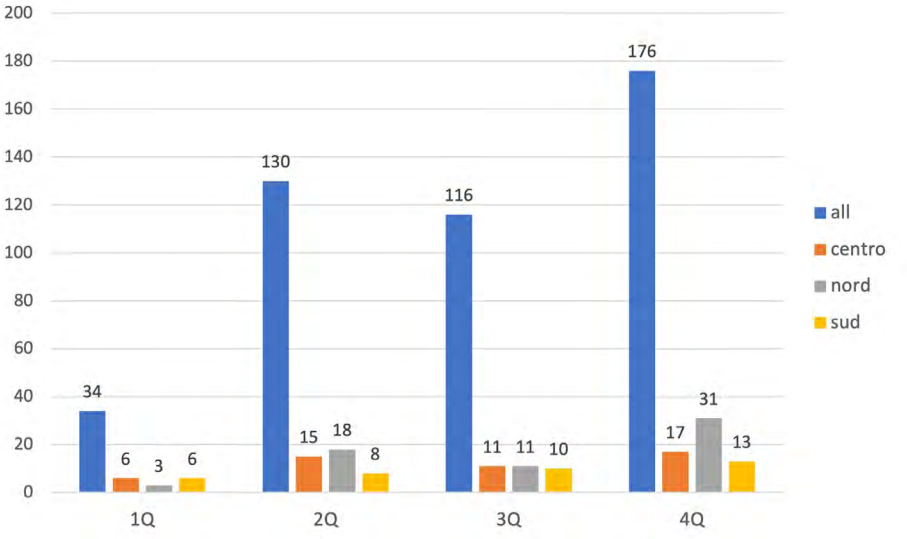


Figura 3 - *Suddivisione attacchi, incidenti e violazioni privacy per aree geografiche - Osservatorio Exprivia CyberSecurity*

Agli attacchi e incidenti va poi aggiunto, per avere uno scenario completo, anche il tema relativo alla violazione della privacy. Non dimentichiamo, infatti, che gli attacchi sono solo una parte del problema. Sempre secondo l'Osservatorio sulla CyberSecurity di Exprivia, le violazioni della privacy rappresentano il 7,11% dei problemi e il 18,51% è rappresentato dagli attacchi che si trasformano in incidenti (**Fig. 4**).

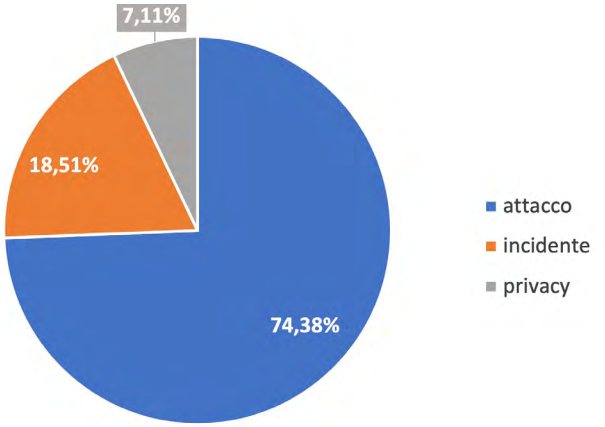


Figura 4 - *Attacchi, incidenti, violazioni di privacy - Osservatorio Exprivia CyberSecurity*

Partendo da tali considerazioni e analizzando i dati dello studio portato avanti nel 2019 sullo stato della sicurezza informatica nel Sud Italia, abbiamo condotto per il 2020 uno studio quali-quantitativo sull'intero territorio italiano.

Obiettivo dello studio

Lo studio è stato realizzato con l'obiettivo di valutare la percezione che le organizzazioni hanno della sicurezza informatica al fine di poter definire strategie di contenimento del rischio applicabili non solo all'infrastruttura IT, ma anche al software utilizzato e all'organizzazione tutta.

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

- regione in cui l'azienda opera;
- tipologia di azienda rispondente;
- attacchi informatici subiti ed eventuali danni rilevati anche durante il periodo del lockdown;
- capacità di difendersi in caso di attacco informatico;
- grado di consapevolezza dei dipendenti circa i rischi conseguenti un attacco;
- conformità a standard e regolamenti in ambito privacy e security.

Al survey hanno risposto 304 aziende/enti. Per la sua promozione e somministrazione sono stati utilizzati differenti canali social, Linkedin, Twitter e Facebook, con lo scopo di massimizzare il numero di soggetti coinvolti e potere così fornire una panoramica ampia del fenomeno. Il survey è accessibile al seguente link https://forms.gle/NjrCt7RmwH9SdJTw8

Analisi dei risultati

Delle 304 risposte raccolte, possiamo notare che il campione che ha aderito allo studio opera in diverse regioni del territorio italiano (**Fig. 5**): Abruzzo, Emilia Romagna, Lazio, Liguria, Lombardia, Marche, Piemonte, Puglia, Sicilia Toscana e Veneto. Inoltre alcune aziende, 24, hanno riportato che forniscono servizi in tutto il territorio nazionale.

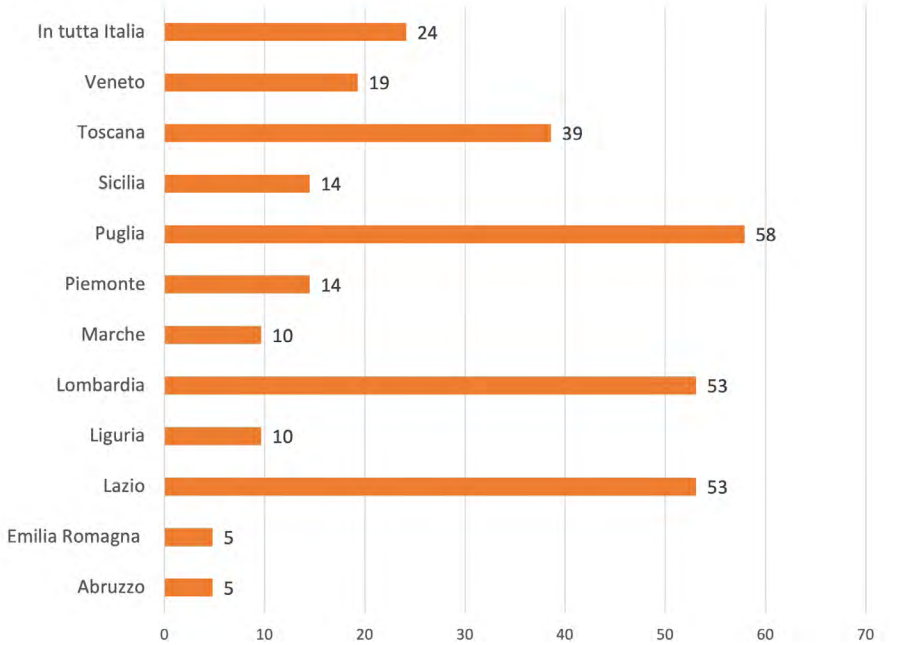


Figura 5 - *Ripartizione del campione intervistato per regione*

Il 52,4% si riferisce a piccole imprese (fino a 50 dipendenti), il 28,3% a medie (da 51 a 250 dipendenti) e il 28,3% a grandi (oltre 250 dipendenti) (**Fig. 6**).

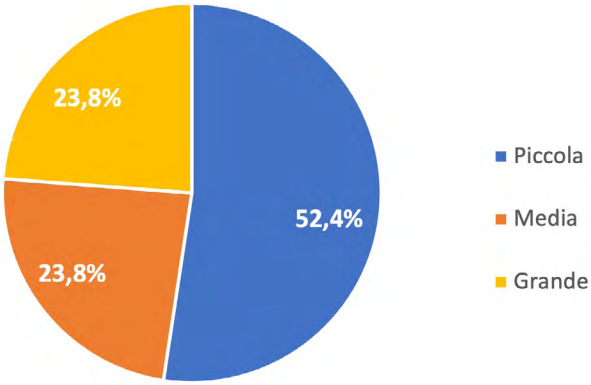


Figura 6 - *Ripartizione del campione intervistato per dimensione*

Il 12,7% del campione è un soggetto pubblico, l'85,7% privato e, infine, il 1,6% a soggetti pubblico-privato (**Fig.** 7).

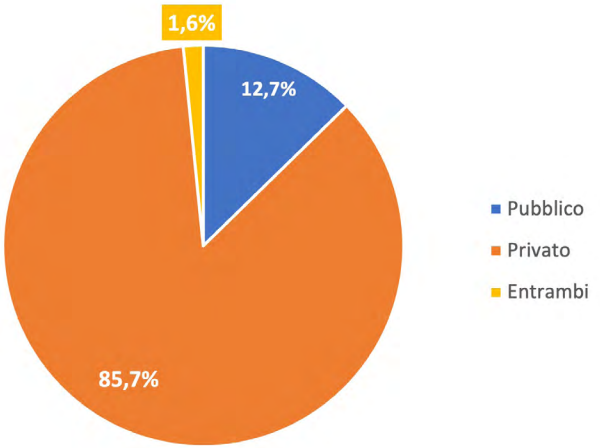


Figura 7 - *Ripartizione del campione intervistato per tipologia*

La **figura 8** presenta invece la distribuzione dei soggetti intervistati per settore di riferimento. Il 33,4% operano nel settore "Consulting e Software/Hardware Vendor" e il 19% in "Research-Education".
Seguono rispettivamente con il 6,3% "Critical Infrastructure", "Manufacturing", "Sanità" e "Servizi Online e Cloud", e con il 3,2% "Governo-Militare" e "ICT". Il 4,8%, invece, opera

in “Studio Ingegneria” e con il 1,6% ciascuno i settori “Automotive”, “Banca e Finanza”, “Comunicazione”, “Estetica”, “Grande Distribuzione e Vendita al dettaglio”, “Osteopatia” e “Turismo”.

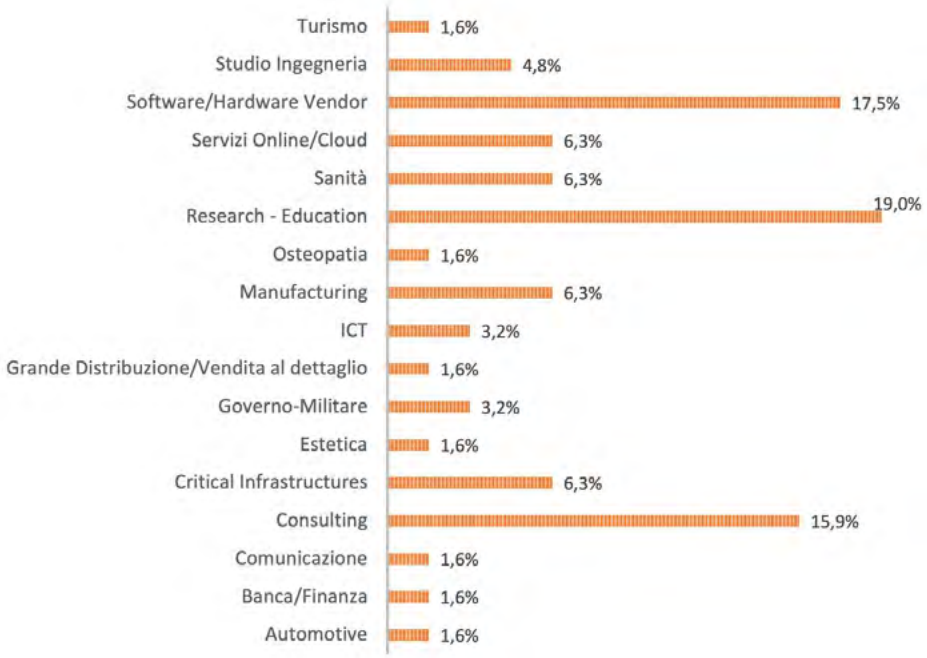


Figura 8 - *Ripartizione del campione intervistato per settore di appartenenza*

Procedendo con l’investigare gli attacchi nel corso del 2020, si ha che il 76,2% del campione ha dichiarato di non essere stato soggetto ad attacchi informatici. Il 23,8%, invece, riporta di aver subito attacchi (**Fig. 9**) ed in particolare il 3,2% afferma che gli attacchi informatici subiti sono relativi al periodo di lockdown a causa del COVID-19. Il 19%, al contrario, ha dichiarato che gli attacchi subiti non hanno nessuna connessione con il periodo di lockdown, ed infine l’1,6% non ha nessuna percezione sulla possibilità che i danni subiti possano essere in relazione al periodo vissuto (**Fig. 10**).

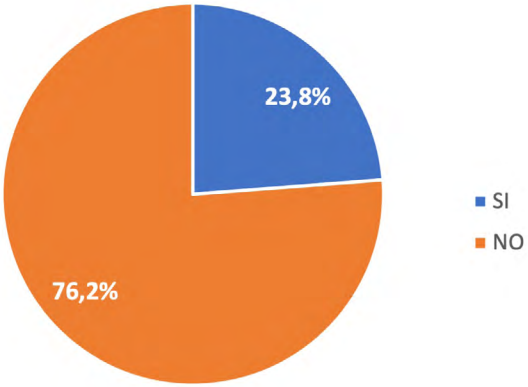


Figura 9 - *Distribuzione dei soggetti vittima di attacchi nel corso del 2020*

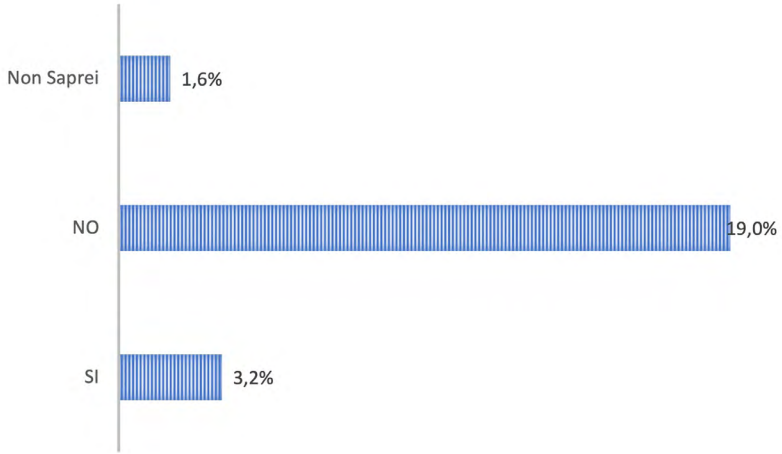


Figura 10 - *Distribuzione dei soggetti vittima di attacchi nel periodo di lockdown a causa del COVID-19*

I danni subiti sono stati valutati trascurabili per il 26,7% dei soggetti coinvolti, bassi per il 13,3%, di media entità per il 40%, e molto alti per il 20% (**Fig. 11**). Nessuno ha valutato con un valore alto l'impatto subito.
La tipologia di danni subiti (**Fig. 12**) risulta essere per il 37,5% riconducibile ad una perdita/esfiltrazione di dati, per il 25% di natura economica, per il 16,7% ad un danno di immagine, il 16,6% di tipo fisico/infrastrutturale e di tempo. Mentre il 4,2% non ha rilevato alcun danno a seguito dell'attacco ricevuto.

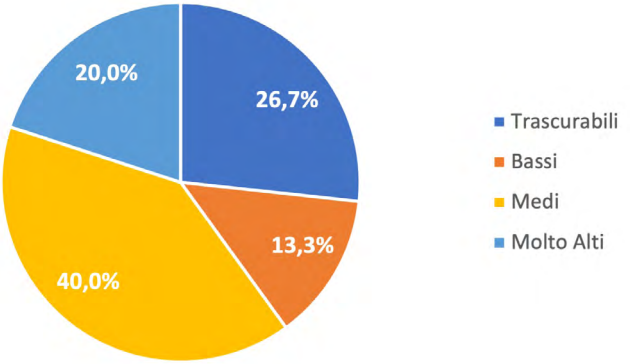


Figura 11 - *L'azienda/ente come valuta i danni subiti*

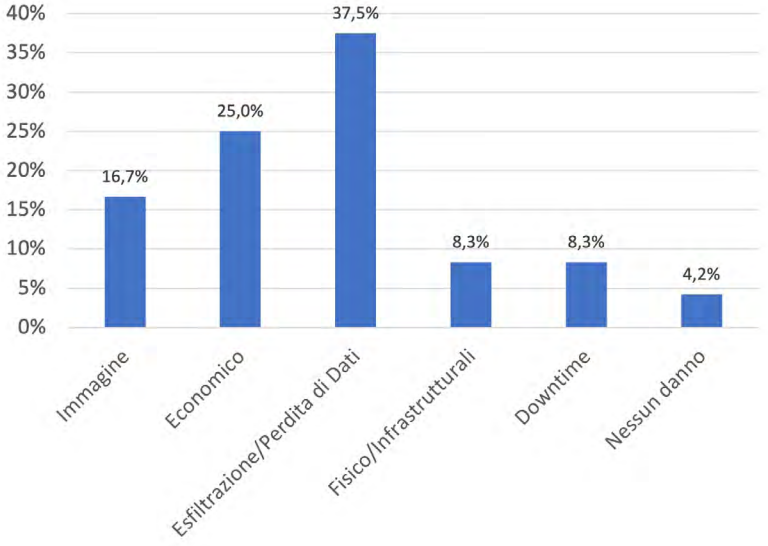


Figura 12 - *Ripartizione del campione per tipo di danni subiti*

Per quanto riguarda la capacità dei soggetti intervistati di difendersi in caso di attacco informatico, il 41,3% si ritengono pienamente in grado di difendersi, il 17,5% sufficientemente capaci, il 41,2% poco o incapace di difendersi (**Fig. 13**).

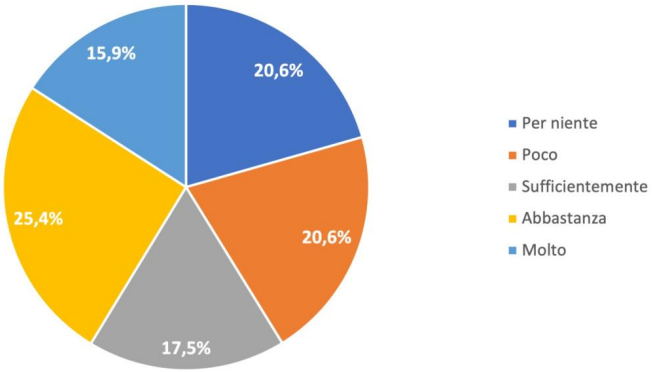


Figura 13 - *Ripartizione del campione per capacità di difesa da attacchi informatici*

La **figura 14** mostra la ripartizione del campione intervistato per grado di conformità a standard e regolamenti in ambito privacy e security. Il 31,7% si dichiara completamente conforme, il 22,2% di esserlo abbastanza. Il 12,7% ritiene di esserlo sufficientemente, il 22,2% poco e il 11,1% per niente. Di conseguenza è possibile affermare che la maggioranza del campione si ritiene conforme a regolamenti e standard in ambito privacy e security.

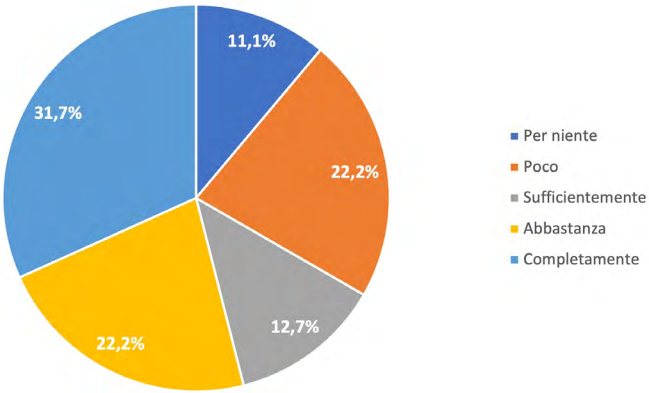


Figura 14 - *Ripartizione del campione intervistato per grado di conformità a standard e regolamenti in ambito privacy e security*

Per quanto concerne la percezione circa la probabilità di un attacco informatico, il 47,6% lo ritiene altamente possibile, il 23,8% sufficientemente probabile. Mentre il 25,4% lo ritiene poco probabile e solo il 3,2% ritiene nulla la probabilità (**Fig. 15**).
Al contempo, per quanto riguarda i dati relativi al grado di consapevolezza dei dipendenti circa i rischi conseguenti ad un attacco informatico (**Fig. 16**), il 19% e il 22,2% dei soggetti intervistati dichiarano rispettivamente una consapevolezza molto alta e abbastanza alta. Il 15,9% sufficientemente consapevole, il 30,2% e il 12,7% invece, poco o per niente consapevoli.

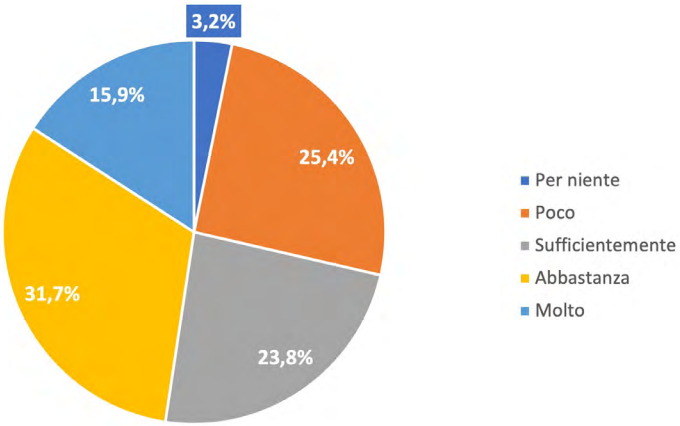


Figura 15 - *Ripartizione del campione intervistato per probabilità di attacco informatico*

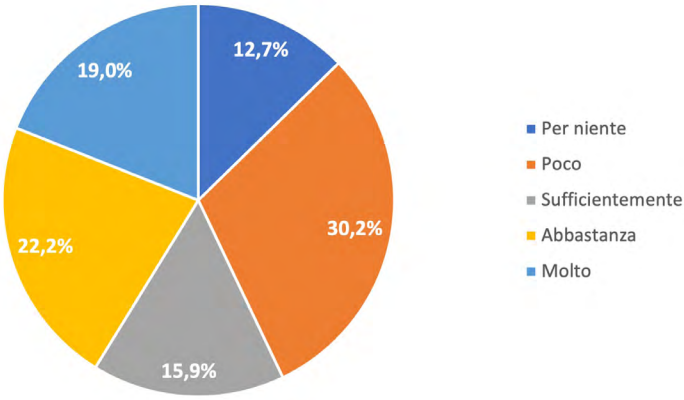


Figura 16 - *Ripartizione del campione intervistato per grado di consapevolezza sui rischi conseguenti un attacco*

Il 54% dei soggetti intervistati dichiara che all'interno della propria azienda si tengono corsi di formazione specifici sulla sicurezza mentre i restanti 46% dichiara di no (**Fig.17**). Analizzando, invece, la percezione del campione circa la necessità di formazione specifica sulla sicurezza informatica, si evince che il 95,2% valuta positivamente la frequenza a corsi, a differenza del 4,8% (**Fig. 18**).

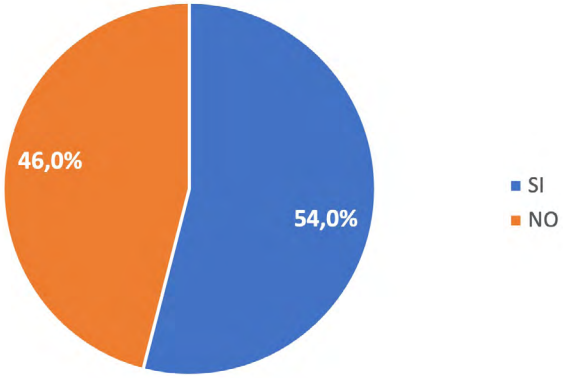


Figura 17 - *Ripartizione del campione intervistato rispetto all'attività formativa svolta sulla sicurezza informatica*

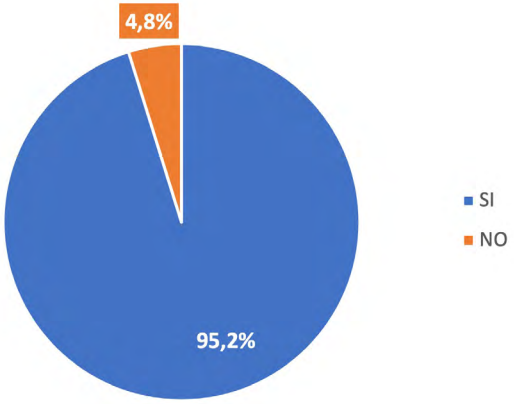


Figura 18 - *Ripartizione del campione intervistato rispetto all'utilità percepita di corsi di formazione sulla sicurezza informatica*

Per quanto riguarda le misure di prevenzioni adottate (**Fig. 19**) dai soggetti intervistati, il 34,6% ricorrono a "Firewall e Data Firewall", il 32,4% ad "Antivirus", il 12,3% a strumenti di "Data Loss Prevention", l'11,7% utilizzano "Intrusion Prevention System e Intrusion Detection System", il 6,1% SIEM, l'1,7% di Penetration Testing Software, ed infine l'1,1% non adotta alcun metodo o strumento o non ne è a conoscenza.

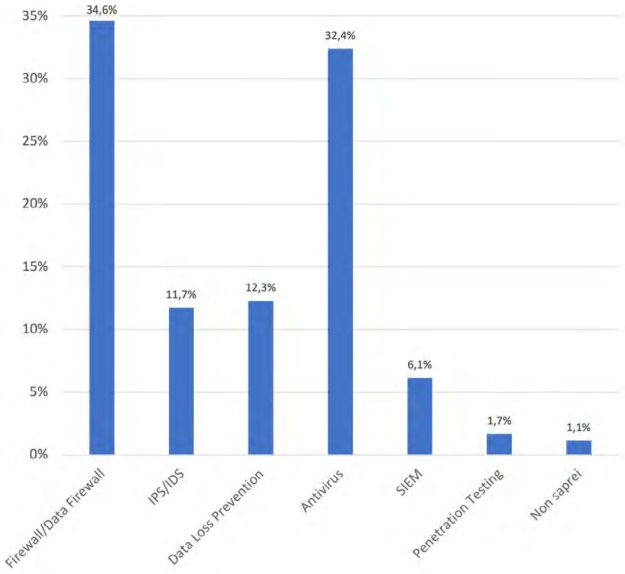


Figura 19 - *Ripartizione del campione intervistato per misure di prevenzione adottate*

Il 44,4% dei soggetti, meno della metà del campione, si preoccupa di verificare i requisiti di sicurezza sia durante la fase di acquisto di software/servizi da terze parti, che all'interno dei termini e condizioni di sottoscrizione dei servizi cloud. Il 55,6%, invece, non opera alcuna verifica (**Fig. 20**).

Conclusioni

Lo studio condotto sullo stato della sicurezza informatica in Italia ha complessivamente coinvolto un campione di 304 aziende/enti. A differenza dello studio condotto precedentemente nel Sud Italia (Report Clusit 2020), notiamo come il campione ha una maggiore distribuzione del campione in diverse regioni e non prevalentemente il Puglia. Ciò sicuramente ci porterà nei prossimi studi ad avere una maggiore percezione di come le diverse realtà nazionali stiano lavorando per far fronte al processo di digitalizzazione che le regioni stanno attuando.

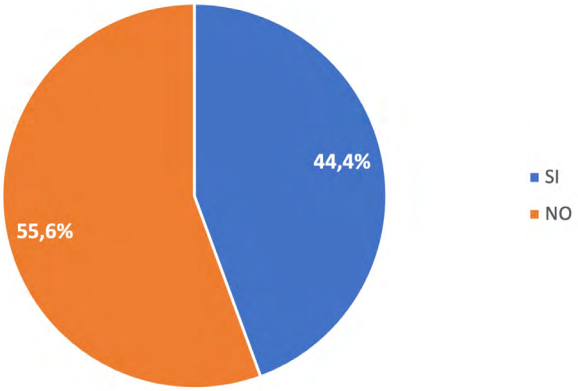


Figura 20 - *Ripartizione del campione intervistato rispetto all'attività di verifica sicurezza in fase di procurement*

Va evidenziato che i risultati, per quanto significativi, vanno interpretati con cautela e certamente in chiave pessimistica. Coloro che hanno partecipato al survey, per le modalità con cui quest'ultimo è stato promosso ed erogato, hanno un livello di alfabetizzazione informatica medio-alto e rappresentano una percentuale modesta di coloro che giornalmente fanno uso inconsapevole di sistemi e tecnologie digitali.
Più della metà dei soggetti intervistati riguarda la piccola azienda (52,4%) con settori estremamente diversificati. Ciò potrebbe riguardare la necessità dei soggetti di aderire a programmi che permettano loro di aumentare il livello consapevolezza sulla sicurezza informatica per poter far fronte al contesto delle minacce informatiche. Basti pensare che più della metà del campione (55,6%) non opera alcuna verifica sui requisiti di sicurezza sia durante la fase di acquisto di software/servizi da terze parti, che all'interno dei termini e condizioni di sottoscrizione dei servizi cloud.
Su 304 aziende, il 23,8% riporta di aver subito attacchi informatici nel corso dell'anno, con una valutazione dei danni medio-alto. Un dato importante visto la maggior parte di loro hanno subito danni economici, di immagine e soprattutto di perdita di dati. Il 41,2%, infatti, non ritiene la sua azienda in grado di difendersi da attacchi informatici. Una percentuale alta e che molto probabilmente nasconde anche l'assenza di capacità nel rilevare un attacco informatico. Infatti tra le misure di prevenzione adottate non emergono nessuna tipologia di esercizi di Red Team e/o Blue Team per poter addestrare il proprio personale a difendersi.
Non a caso il 95,2% dei soggetti ritengono utile la formazione sulla sicurezza informatica. Un risultato che esprime come le aziende/enti stiano cambiando la loro percezione sul livello di consapevolezza sulla sicurezza informatica.

Attività e segnalazioni della Polizia Postale e delle Comunicazioni nel 2020

Nell'anno 2020, la diffusione pandemica da COVID-19 ha comportato profondi mutamenti delle nostre abitudini di vita, modificando in maniera repentina e spesso radicale tutte le nostre attività (dal lavoro per passare allo studio, al tempo libero, ai rapporti sociali), con una rimodulazione delle stesse basata in larga parte sull'utilizzo di internet.

Ciò ha comportato un allargamento della platea degli utenti connessi alla rete (comprendendo anche minori o persone con scarsissime conoscenze informatiche), ed un notevole aumento dei dispositivi connessi.
Se da un lato la società ha quindi compiuto un ulteriore passo in avanti, entrando in maggiore confidenza con le nuove tecnologie, dall'altro lato è stata maggiormente esposta alle insidiose aggressioni da parte della cyber-criminalità.

In questo scenario, l'impegno della Polizia Postale e delle Comunicazioni si è indirizzato verso la prevenzione ed il contrasto di un insieme assai vasto ed eterogeneo 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 Anticrimine Informatico per la Protezione delle Infrastrutture Critiche

Il dato emergente dalle attività del Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche – CNAIPIC - nel periodo di interesse, riferisce come sia gli attacchi diretti alle grandi infrastrutture erogatrici di servizi essenziali (approvvigionamento idrico ed energetico, pubblica amministrazione, sanità, comunicazione, trasporti, finanza sistemica), che gli attacchi apparentemente isolati, diretti a singoli enti, imprese o cittadini, manifestino una dimensione criminale organizzata, essendo ascrivibili all'operato di sodalizi ben strutturati, spesso operanti a livello transnazionale.
Le tipologie di eventi cyber che hanno maggiormente impegnato gli operatori del Centro sono rappresentate dagli attacchi a mezzo malware, soprattutto di tipo ransomware, attacchi DDoS con finalità estorsiva, accessi abusivi con l'intento di carpire dati sensibili, campagne di phishing e, in ultimo, campagne APT (Advanced Persistent Threats), particolarmente insidiosi poiché ricollegabili ad attori malevoli dotati di notevole expertise tecnico e rilevanti risorse.

L'emergenza Covid-19, in particolare, ha offerto a tali sodalizi criminali un'ulteriore occasione per strutturare e dirigere attacchi ad ampio spettro, volti a sfruttare per scopi illeciti la situazione di particolare esposizione e maggior vulnerabilità in cui il Paese è risultato, e

tuttora risulta, esposto.

Nello specifico, alcune delle più rilevanti infrastrutture sanitarie impegnate nel trattamento dei pazienti "Covid" sono state oggetto di campagne di cyber-estorsione volte alla veicolazione all'interno dei sistemi ospedalieri di sofisticati ransomware – concepiti allo scopo di rendere inservibili, mediante cifratura, i dati sanitari contenuti al loro interno - a fronte di richieste di pagamento del prezzo estorsivo, per lo più in cryptovalute (es. Bitcoin), onde ottenere il ripristino dell'operatività.
Il sistema sanitario e della ricerca è stato inoltre bersaglio di diversi attacchi APT, con lo scopo della esfiltrazione di informazioni riservate riguardanti lo stato di avanzamento della pandemia e l'elaborazione di misure di contrasto, specie con riguardo all'approntamento di vaccini e terapie anti-Covid.
Si sono moltiplicati i casi di phishing ai danni di enti ed imprese, veicolati attraverso messaggi di posta elettronica i quali, dietro apparenti comunicazioni di Ministeri, organizzazioni sanitarie e altri enti, relative all'andamento del contagio o alla pubblicazione di misure di contrasto, nascondevano in realtà sofisticati virus informatici in grado di assumere il controllo dei sistemi attaccati (virus RAT) e procedere così all'esfiltrazione di dati personali e sensibili, alla captazione di password di accesso a domini riservati, finanche all'attivazione di intercettazioni audio-video illegali.

Sul piano degli attacchi al sistema produttivo del Paese, si è registrato un generale aumento delle minacce legato all'adozione su larga scala dei modelli di lavoro a distanza, c.d. "smartworking", modelli che se da un lato hanno consentito la prosecuzione di attività essenziali, hanno d'altro canto prodotto una considerevole estensione del perimetro informatico delle aziende, con una conseguente maggior esposizione ad azioni ostili esterne.

Nel delineare l'identità degli autori del reato, il trend legato all'andamento degli attacchi ai danni delle infrastrutture critiche fa registrare, nel complesso, l'emersione di una matrice criminale di natura puramente economica, orientata al conseguimento di profitti illeciti, che si pone in misura oggi prevalente rispetto alle condotte ispirate da ragioni di cyber-hacktivism, ideologicamente o politicamente orientato.
L'azione di contrasto attuata dal CNAIPIC nel corso del 2020, è stata rivolta sia all'attività di contrasto dei reati, sia soprattutto ad assicurare interventi di tipo preventivo e di protezione, incentrati sulla capacità di analisi e di allerta precoce finalizzata alla diffusione, in tempo reale, degli IoC relativi alle minacce in corso, a beneficio dell'interno panorama delle infrastrutture critiche nazionali.

Nell'ambito del progetto legato alla creazione di un Sistema Informativo Nazionale per il Contrasto al Cyber Crime (progetto SINC3 finanziato con fondi ISF) che mira ad estendere la rete di protezione cibernetica anche alle realtà più sensibili del Paese, l'anno in esame ha visto il sostanziale completamento delle attività preparatorie che porteranno nell'anno

2021 all'avvio della piattaforma di condivisione delle informazioni di sicurezza informatica e la contestuale costituzione dei NOSC (Nucleo Operativo Sicurezza Cibernetica) presso i Compartimenti Polizia Postale e delle Comunicazioni sul territorio.
La rilevazione relativa al periodo in esame conferma, in linea generale, l'andamento crescente del numero di attacchi complessivamente verificatisi ai danni delle Infrastrutture critiche del nostro Paese:

ATTIVITÀ C.N.A.I.P.I.C.	Anno 2019	Anno 2020
Attacchi rilevati	147	509
Alert diramati	82484	83416
Persone indagate	59	105
Richieste di cooperazione internazionale in ambito Rete 24/7 High Tech Crime G7 (Convenzione Budapest)	79	69

Dalla tabella si evince che gli attacchi rilevati hanno subito un incremento del 246% con una conseguente crescita delle persone identificate ed indagate.
Tra le attività di polizia giudiziaria più significative si segnala:

Operazione "Data Room"

Il CNAIPIC nell'ambito di una lunga e articolata attività di indagine ha effettuato quella che può essere ritenuta la prima operazione su larga scala volta alla tutela di dati personali trafugati, culminata con l'esecuzione, effettuata con l'ausilio di personale dei Compartimento Polizia Postale e delle Comunicazioni di Roma, Napoli, Perugia e ancona, a 13 ordinanze di custodia cautelare e 7 ordinanze che dispongono l'obbligo di dimora nel comune di residenza ed il divieto di esercitare imprese o ricoprire incarichi direttivi in imprese e persone giuridiche.

Al vertice del sistema due dipendenti infedeli di TIM S.p.A., oltre ai responsabili di alcune società che offrono servizi di call center, avevano messo i piedi una complessa e articolata attività criminale finalizzata al commercio illecito dei dati personali di centinaia di migliaia di utenti di società operanti nella fornitura di servizi essenziali, nel settore telecomunicazioni ed energia.

I 26 indagati complessivi, tutti destinatari di provvedimenti di perquisizione locale e personale, sono stati ritenuti responsabili, a vario titolo ed in concorso tra loro, della violazione aggravata dei reati previsti all'art. 615 ter c.p. (accesso abusivo a sistema informatico), all'art.615 quater c.p. (detenzione abusiva e diffusione di codici di accesso), riguardando le condotte sistemi di pubblico interesse, e della violazione della legge sulla privacy art.

167-bis D. Lgs. 193/2003 (comunicazioni e diffusione illecita di dati personali oggetto di trattamento su larga scala).

Le estrazioni dei dati dai database dei fornitori dei servizi, per come verificato nel corso delle indagini, venivano sistematicamente portate avanti con un volume medio di centinaia di migliaia di record al mese, che gli indagati modulavano a seconda della illecita "domanda" di mercato.
Nel corso delle attività, svolte grazie alla collaborazione di TIM S.p.A. e all'importante apporto della struttura di sicurezza aziendale dell'azienda, è venuto alla luce un complesso "sistema" che vedeva, da un lato una serie di tecnici infedeli procacciare i dati, dall'altro una vera e propria rete commerciale che ruotava attorno alla figura di un imprenditore Campano, acquirente della preziosa "merce", che poi veniva poi piazzata sul mercato dei call center, 13 sono quelli già individuati nella prima fase delle indagini, tutti in area campana, ed oggetto di altrettante attività di perquisizione.

Operazione GLAAKI

Il C.N.A.I.P.I.C., con l'ausilio del Compartimento Polizia postale di Bari, all'esito di una complessa attività tecnica di indagine, ha eseguito una perquisizione locale personale ed informatica nei confronti di un cittadino italiano residente nella provincia di Taranto resosi responsabile dei reati di "detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici" (art. 615 quater c.p.) nonché di diffusione di programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art.615 quinquies c.p.). L'indagine, denominata "GLAAKI", nata grazie ad una collaborazione con una società di threat intelligence, attiva nel settore cyber intelligence, è stata avviata nel febbraio del 2020, in piena emergenza epidemiologica da covid quando questo centro è venuto a conoscenza di una campagna di spear phishing perpetrata attraverso l'invio massivo di email dirette ad ignari cittadini destinatari di un messaggio contenente un allegato malevolo avente ad oggetto proprio le parole "covid-19".

Gli effetti psicologici che la pandemia stava apportando alla socialità nazionale, proprio agli inizi di febbraio 2020 hanno consentito all'hacker di sfruttare al meglio l'ingegnosità del suo attacco informatico.
Con il pretesto, infatti, di fornire aggiornamenti sullo stato di avanzamento del virus, il cyber criminale ha indotto i destinatari delle email ad aprire un allegato infetto, che ha consentito al malfattore di appropriarsi delle credenziali bancarie e dei dati personali delle vittime.
Al fine di indurre le stesse ad aprire l'allegato malevolo, l'hacker, ha utilizzato "nomi di mittenti credibili", ovvero, dopo essere entrato abusivamente all'interno della casella di posta elettronica, ha copiato i contatti della rubrica e, falsificandone l'indirizzo email, ha inviato messaggi contenti il virus a tutti i destinatari che fidandosi dell'attendibilità del mittente l'hanno aperto senza esitare.

Le complesse attività di analisi delle ricorrenze hanno permesso di ricostruire l'infrastruttura informatica del codice malevolo attraverso piccole tracce involontariamente lasciate dall'hacker, ovvero dettagli riferibili ad acronimi di nomi apparentemente insignificanti, utilizzati in fase di registrazione ai servizi internet, che hanno consentito di localizzare il possibile attaccante.

La conferma del complesso quadro investigativo si è avuta solo con l'esecuzione delle perquisizioni informatiche, eseguite da personale altamente specializzato di questo Centro, che hanno permesso di superare le difese create dal cyber criminale, consentito di rintracciare ed isolare il codice malevolo di tipo keylogger, appositamente creato dall'hacker.
La campagna di diffusione del malware in questione ha mietuto numerose vittime approfittando della vulnerabilità emotiva creatasi proprio all'inizio della pandemia.
L'attaccante, tramite l'utilizzo di sofisticate tecniche di social engineering, è riuscito a nascondere tramite l'utilizzo di virtual private network i nodi di collegamento ai server utilizzati per compiere l'attacco. Solo in sede di perquisizione, è stato possibile ricostruire l'intera vicenda ovvero isolare il codice malevolo e recuperare gli accessi agli spazi web utilizzati per immagazzinare i dati fraudolentemente carpiti

C.N.A.I.P.I.C. e convenzioni con le infrastrutture critiche

Nell'ottica di un'efficace condivisione operativa, il Centro ha proseguito la stipula di specifici Protocolli a tutela delle infrastrutture critiche nazionali: al riguardo, nel 2020 sono state sottoscritte **6** nuove convenzioni con le società Borsa Italiana, EFSA (European Food Safety Authority), IREN S.p.A., SACBO Aeroporto di Bergamo, SAIPEM S.p.A., SIOT TAL Oleodotto Transalpino ed il rinnovo dell'accordo convenzionale con la società SIA S.p.A.
Si rappresenta, altresì, che analoghe forme di collaborazione sono state avviate dagli uffici territoriali della Specialità con strutture sensibili di rilevanza locale, sia pubbliche che private, al fine di garantire un sistema di sicurezza informatica capillare e coordinato.

Financial cybercrime

Nel 2020 a causa della pandemia da Covid 19, e del conseguente lockdown come mezzo di contenimento della diffusione del virus, vi è stato un sensibile aumento delle statistiche con riferimento a tutto il cybercrime ed in particolare rispetto al financial.
L'obbligo, oltre che la necessità, di dover permanere in casa ha costretto criminali e vittime ha incrementare l'utilizzo dello strumento informatico.
Com'è noto, l'obiettivo criminale del trafugamento dei dati personali e delle credenziali di accesso a servizi finanziari, utili alla disposizione di pagamenti in frode, è posto in essere dai criminali attraverso massive campagne di phishing.
I due principali metodi di realizzazione di questa tipologia di reato: email contenenti allegati malevoli; l'impiego di siti-clone, sono affiancate ed integrate oggi da altre due modalità che stanno costituendo una vera piaga che affligge i correntisti di tutti gli istituti bancari il "Vishing" e lo "Smishing".

Queste due insidiose varianti del phishing consentono ai malviventi il procacciamento di codici "one-time", token virtuali e password dispositive mediante il ricorso all'insidiosa chiamata "vocale" o attraverso "l'Alias" messaggi ed sms che si vanno a inserire in automatico tra quelli che di solito pervengono dalla nostra banca.

Il tessuto economico-produttivo del Paese continua ad essere oggetto degli attacchi noti a livello mondiale con le espressioni BEC e CEO Fraud.
Le frodi basate sul social engineering hanno avuto un costante incremento perché basati su comunicazioni commerciali a distanza.
I fenomeni di Bec fraud, risultano fortemente influenzati dall'epidemia del Covid-19 sia a causa dell'abbassamento delle difese aziendali, determinato dallo stato di difficoltà psicologica o "logistica" di lavoratori e amministratori, sia dall'aumento su larga scala di processi di smart-working.
Alcune Bec fraud risultano specificamente collegati al tema-Covid, perché relativi direttamente a frodi commerciali nell'acquisto di mascherine e dispositivi sanitari.

Nonostante la difficoltà operativa di bloccare e recuperare le somme provento di frode informatica, soprattutto perché inviate verso paesi extraeuropei (Cina, Taiwan, Hong Kong ed oggi anche il Regno Unito), grazie alla versatilità della piattaforma OF2CEN (On line Fraud Cyber Centre and Expert Network) per l'analisi e il contrasto avanzato delle frodi del settore, nell'anno 2020, la Specialità ha potuto bloccare e recuperare alla fonte, su una movimentazione di **33.186.674,00 €**, ben **20.046.240,00 €**.

La piattaforma in questione, frutto di specifiche convenzioni intercorse mediante ABI con gran parte del mondo bancario, consente di intervenire in tempo quasi reale sulla segnalazione, bloccando la somma prima che venga polverizzata in vari rivoli di prestanome.
Al riguardo, con riferimento al fenomeno del cyber-riciclaggio, di rilievo è la recente operazione internazionale denominata "Emma6", coordinata dal Servizio Polizia Postale e delle Comunicazioni con la collaborazione di 21 Paesi Europei e di Europol, volta a identificare i c.d. "money mules", primi destinatari delle somme provenienti da frodi informatiche e campagne di phishing, che offrono la propria identità per l'apertura di conti correnti e/o carte di credito, sui quali vengono poi accreditate le somme illecitamente acquisite.
L'operazione in parola ha consentito sul territorio nazionale di identificare e denunciare **257** money mules.
Le transazioni fraudolente sono state **744**, per un totale di circa **9** milioni di euro, di cui circa **3.6** milioni euro sono stati bloccati e/o recuperati grazie alla piattaforma per la condivisione delle informazioni denominata "OF2CEN", realizzata appositamente al fine di prevenire e contrastare le aggressioni criminali ai servizi di home banking e monetica.

Truffe on line

In relazione al fenomeno delle truffe on line, nel medesimo scenario caratterizzato dalla diffusione della pandemia, sono state svolte specifiche attività di indagine riguardanti numerosi casi legati alla vendita OnLine di dispositivi di protezione individuale, attività criminale, questa, favorita dalla ricerca pressante di mascherine, guanti, liquidi igienizzanti ed il conseguente proliferare nel web di siti di e-commerce risultati poi fraudolenti.
Tale ambito ha riguardato anche la contraffazione del marchio CE. Infatti sono state individuate numerose partite di materiale, venduto all'ingrosso, proveniente soprattutto dall'estero, riportanti marchi CE contraffatti: tale merce era destinata, in alcuni casi, alla vendita al dettaglio anche attraverso il circuito delle farmacie ignare della contraffazione.

Sono state anche raccolte numerose segnalazioni e avviate altrettante attività d'indagine, inerenti le false raccolte fondi, poste in essere attraverso siti web apparentemente riconducibili ad enti ospedalieri o accreditate da falsi patrocini di Istituzioni o Enti Pubblici (Regioni – Comitati vari).
Il modus operandi dei cybercriminali, facendo leva sul generale e diffuso sentimento di vicinanza della cittadinanza al personale medico ed infermieristico, incessantemente impegnato nella lotta al Covid 19, dava la possibilità di effettuare dei versamenti di denaro e/o bonifici su IBAN legati a conti correnti o carte ricaricabili attivati ad hoc.
L'esito di tali attività investigative ha portato ad indagare **23** persone, **6** Società e al sequestro di **5.000** test rapidi Covid e **2.360** dispositivi di protezione privi delle prescritte certificazioni.
Nel corso del 2020, sono stati trattati complessivamente **93.300** casi e sottoposte ad indagine **3.860** persone.

Nel corso del periodo in esame, è stata implementata l'attività di contrasto al diffuso fenomeno del falso trading online, che ha visto aumentare a dismisura la perdita di ingenti capitali verso Paesi esteri presso i quali l'acquisizione di elementi utili al proseguimento delle indagini risulta particolarmente difficoltosa, sebbene si dia risalto all'azione di cooperazione internazionale attraverso i canali che caratterizzano sia Europol che Eurojust.
Cyber terrorismo
Come noto, nell'ambito della prevenzione e del contrasto al terrorismo internazionale di matrice jihadista ed, in particolare, dei fenomeni di radicalizzazione sul web, il personale della Polizia Postale e delle Comunicazioni effettua costantemente il monitoraggio del web, affiancato da qualificati mediatori linguistici e culturali – messi a disposizione da associazioni senza scopo di lucro – il cui contributo, per la peculiarità della materia e dei relativi contenuti multimediali presenti sulla rete, fornisce un valore aggiunto di fondamentale importanza.

In particolare, la Specialità 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 servizi di comunicazione online di ogni genere.
L'attività, funzionale al contrasto dei fenomeni di radicalizzazione e cyberterrorismo, ha permesso di riscontrare come l'attuale struttura centrale dell'apparato di propaganda del Daesh, con produzione mediatica più o meno costante nel tempo, risulti essere costituita da vari Media Center insistenti nelle province del Califfato che si appoggiano ai c.d. Supporter Generated Content per la diffusione del materiale di propaganda.

Nel dettaglio, anche nel corso del 2020 è stato possibile constatare come tale struttura mediatica abbia continuato a basarsi su una miriade di account, attivati quotidianamente dai supporter del Califfato (anche in forma automatizzata tramite apposite strutture dipendenti dal Daesh e deputate al mantenimento dell'operatività mediatica) con l'obiettivo di divulgare magazine online del Califfato, aggiornamenti sulle attività dei combattenti nei teatri operativi, video, documenti, manuali o pubblicazioni di esponenti di spicco della corrente radicale islamica, infografiche di minaccia etc.

L'adozione di tale modalità operativa per la diffusione della propaganda jhiadista è stata determinata sia dall'incremento dell'azione di rimozione dei contenuti illeciti presenti sulle proprio piattaforme da parte dei maggiori fornitori di servizi Internet (tra i quali Telegram, Facebook, Google, Twitter, etc.), sia per le particolari attività di contrasto attuate dal law enforcement.

In particolare, nel corso del 2020 sono proseguite le attività svolte dal personale del Servizio Polizia Postale e delle Comunicazioni all'interno dei tavoli di lavoro internazionali deputati al contrasto del Cyberterrorismo, con il coordinamento di Europol e con il coinvolgimento di tutte le Forze dell'Ordine degli Stati Membri, nonché dei rappresentanti dei maggiori Internet Service Provider, tra i quali soprattutto Telegram (che è stato il fornitore di servizi online che ha ricevuto la maggior parte delle richieste di rimozione e che ha allontanato dalla propria piattaforma una parte significativa degli attori chiave all'interno della rete di diffusione della propaganda IS).
E ancora, in tale contesto operativo, tra le principali attività svolte nel corso del 2020 dal personale del Servizio Polizia Postale e delle Comunicazioni si evidenzia la partecipazione all'azione denominata "RAD - Referral Action Day on instructional material online" svoltasi il 2 luglio 2020 e promossa da Europol al fine di procedere – tramite la segnalazione ai rispettivi Provider interessati – alla rimozione di ogni tipo di contenuto didattico in formato digitale utilizzato per la pianificazione e realizzazione di attacchi terroristici.

L'Action Day ha coinvolto unità specializzate del Centro europeo antiterrorismo (ECTC) e rappresentanti di 18 Paesi, tra cui 13 Stati membri dell'U.E. e 5 Paesi extra U.E.

L'attività in argomento ha preso di mira i contenuti online creati o utilizzati come materiale didattico per ispirare e commettere attacchi nel contesto del terrorismo di matrice jihadista, nonché dell'estremismo razziale, antagonista e anarchico.

In particolare, appare opportuno evidenziare come i manuali fatti in casa e le guide individuate nel corso dell'operazione costituiscano il principale strumento per la realizzazione di armi devastanti, soprattutto per gli attacchi condotti da attori solitari, ovvero dai gruppi terroristici e dai loro sostenitori.
Durante l'azione, gli esperti della Sezione Cyberterrorismo hanno rilevato, valutato e segnalato i contenuti online, inclusi manuali e tutorials su come preparare e attuare attacchi terroristici, come selezionare gli obiettivi, come utilizzare le armi e costruire bombe. Alcuni dei documenti individuati contenevano anche le istruzioni su come rimanere anonimi online e su come evitare di essere individuati durante la pianificazione di un attacco terroristico.

All'esito delle attività sono state segnalate per la successiva rimozione un numero complessivo di **1.724** url riconducibili a **113** piattaforme web utilizzate per la propaganda jihadista e n. **182** url su **67** piattaforme web nell'ambito dei contenuti riferibili all'area dell'ultradestra e antagonista/anarchica.

Appare evidente, dunque, come il carattere transnazionale delle operazioni di contrasto appena descritte, sia per la natura internazionale del fenomeno che per la stessa struttura della rete, abbia comportato l'imprescindibile attivazione di strumenti di cooperazione sovranazionale che hanno determinato un indiscusso valore aggiunto alle attività di prevenzione messe in atto dalle diverse Forze di Polizia nazionali.
Ed invero, l'analisi effettuata sulla diminuzione del corso del 2020 del numero dei siti e account riconducibili alla propaganda jihadista ha permesso di evidenziare l'importanza delle lavoro svolto dal Servizio Polizia Postale e delle Comunicazioni, quale punto di contatto nazionale dell'Internet Referral Unit (IRU) di Europol, nell'ambito degli "Action Day" che determinato un massiccio "take down" di migliaia di gruppi, canali e account che sono stati oggetto di preventiva segnalazione da parte del law enforcement, in quanto considerati responsabili della pubblicazione del settimanale di propaganda jhiadista al-Naba.

Oltre alle suindicate attività sia preventive, sia di Polizia Giudiziaria connesse al terrorismo di matrice jihadista, la Polizia Postale e delle Comunicazioni ha registrato nel corso degli ultimi anni un notevole incremento nell'ambito del settore della propaganda online legata all'estremismo razzista e xenofobo, riscontrando un trend di forum e discussioni dedicate all'argomento in costante aumento.
In particolare, anche in tale ambito il web rappresenta uno strumento strategico per la diffusione della propaganda delle ideologie estremiste e violente, nonché per il reclutamento di nuovi combattenti, il finanziamento, lo scambio di comunicazioni riservate nella pianificazione degli attentati e di rivendicazione degli stessi.

L'indottrinamento ed il reclutamento, come nel caso del radicalismo jihadista, avvengono sempre sulla rete, attraverso una graduale autoformazione che inizia con la visualizzazione di contenuti diffusi soprattutto nelle board "riservate", diverse dai principali social network. La digitalizzazione delle tecnologie dell'informazione e della comunicazione ha permesso all'antisemitismo 2.0 di riprodursi in modo rapido e multimediale; contenuti contro gli ebrei si trovano sia negli spazi web antisemiti che in siti e social network generalisti, dove vengono pubblicati e condivisi commenti offensivi senza registrare l'intervento dei moderatori. Il web 2.0, dunque, pare aver contribuito a diffondere una sottocultura dove razzismo, intolleranza e antisemitismo sono divenuti socialmente accettabili, specie tra i giovani. La radicalizzazione verbale e l'abbassamento della soglia dei tabù si evidenzia attraverso il linguaggio, la carica di violenza, il sarcasmo razzista. In tale ambiente, la promozione delle teorie cospirative, la demonizzazione degli ebrei/sionisti e dello stato ebraico e l'uso degli ebrei/sionisti come capro espiatorio possono condurre ad una violenza reale contro gli ebrei.

E ancora, l'analisi effettuata sulle modalità utilizzate nel corso degli ultimi attacchi terroristici, in cui si è assistito alla diffusione in diretta streaming delle immagini all'interno di varie piattaforme online, ha determinato un evidente innalzamento del rischio ed un conseguente incremento del livello di attenzione anche nei tavoli di lavoro internazionali.
In particolare, proprio in seno all'E.U. Internet Forum, personale del Servizio Polizia Postale e delle Comunicazioni ha contribuito – unitamente a rappresentanti degli Stati Membri e di Europol, nonché di alcuni delegati delle maggiori compagnie fornitrici di servizi internet (tra le quali Facebook, Google, Microsoft, Telegram, Twitter, Snap, JustPaste.it e Dropbox) – all'elaborazione di un protocollo di crisi dell'Unione Europea finalizzato al contrasto e al contenimento della rapida diffusione virale di contenuti terroristici e di estremismo violento online.

Nel dettaglio, l'adozione del protocollo in argomento, che vede il Servizio Polizia Postale e delle Comunicazioni quale punto di contatto nazionale, ha determinato la predisposizione di un meccanismo, attivo h24 sette giorni su sette, volto a garantire una risposta coordinata e tempestiva ad una crisi terroristica online (intesa come un evento che descrive un danno alla vita o all'integrità fisica) transfrontaliera nel contesto del terrorismo o dell'estremismo violento.
Appare opportuno evidenziare che tale protocollo – attualmente in via di definizione, con un vademecum operativo che verrà rilasciato a breve da Europol, all'esito di numerose riunioni operative – è già stato attivato in via sperimentale proprio nel corso degli ultimi episodi terroristici accaduti in Francia, al fine di contrastare nell'immediatezza la diffusione del video dell'attacco terroristico stesso.
Inoltre, la grave emergenza socio-sanitaria, tuttora in corso, accompagnata dalle restrizioni introdotte dai decreti governativi per contrastare la diffusione del virus Covid-19, ha determinato negli ultimi mesi un'intensa attività sia di controinformazione, sia di incitamento ad azione di protesta.

La rilevante attività di monitoraggio del web svolta dal personale del Polizia Postale ha permesso di riscontrare il considerevole aumento di canali e gruppi all'interno delle varie piattaforme di comunicazione online nei quali sono stati pubblicati numerosissimi commenti in cui emergeva la volontà di reagire alle decisioni governative attraverso vere e proprie azioni di piazza, anche violente.

Ed invero, negli ultimi mesi questa Specialità ha riscontrato un considerevole incremento dei seguenti fenomeni illeciti:
- diffusione di 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) con le quali vengono prospettate vere e proprie "teorie del complotto" volte a destabilizzare l'ordine democratico ed indirizzare i sentimenti di rabbia nei confronti di determinate "categorie sociali";
- creazione di discussioni all'interno di piattaforme di comunicazione online nell'ambito delle quali si cercano strategie di protesta e contrasto, anche violento, alle disposizioni in materia di contenimento dell'emergenza Covid.

Appare evidente, inoltre, come i problemi economici e sanitari causati dall'emergenza coronavirus siano stati strumentalizzati da numerosi esponenti di vari movimenti non precisamente collocabili politicamente, per alimentare la disinformazione ed organizzare l'imminente "chiamata alle armi per reagire al caos globale" attraverso azioni di violenza eversiva.
In tale contesto, dunque, la Polizia Postale effettua una costante attività di monitoraggio, finalizzata alla più efficace forma di prevenzione e contrasto.

Centro nazionale di contrasto alla pedopornografia online

Nel corso del 2020, il Centro Nazionale per il Contrasto alla Pedopornografia Online (C.N.C.P.O.) ha confermato il ruolo centrale della Polizia Postale e delle Comunicazioni nella lotta alla pedofilia e pornografia minorile online.

Inoltre, l'evoluzione dei fenomeni che nel web coinvolgono i minori ha determinato un ampliamento delle competenze del Centro per quanto il contrasto a tutte le forme di aggressione in rete nei confronti dei minorenni.

Fin dall'inizio della diffusione pandemica da COVID-19, la Polizia Postale e delle Comunicazioni, con l'impiego di tutte le sue articolazioni territoriali coordinate attraverso l'azione strategica assicurata dal C.N.C.P.O., ha intensificato il monitoraggio della rete, con lo scopo di scongiurare l'aumento di reati relativi allo sfruttamento sessuale dei minori online, determinato dalle misure restrittive assunte e, in particolare, la chiusura degli istituti scolastici e l'implementazione dello smartworking per diverse categorie di lavoratori.
È stato inoltre rafforzato il raccordo delle investigazioni nei canali di cooperazione internazionale di polizia e giudiziaria, presupposto determinante per disarticolare le illecite comu-

nità virtuali pedofile caratterizzate da una struttura organizzata.

Laddove possibile, è stato innalzato il livello di collaborazione con i social network più diffusi in Italia, in un'ottica di sinergia nella lotta all'utilizzo improprio del web da parte dei minori, definendo canali preferenziali di comunicazione e gestione dei casi penalmente rilevanti.

È stato implementato l'impegno funzionale all'individuazione di un numero sempre maggiore di siti che contengono materiale pedopornografico, da inserire nella black list gestita dal C.N.C.P.O., il cui accesso viene inibito, con modalità diverse a seconda dell'ubicazione dei server utilizzati, agli internauti attivi sul territorio italiano.
E' stato svolto un lavoro di valutazione settimanale dei dati relativi alla vittimizzazione dei bambini e dei ragazzi in rete al fine di monitorare la minaccia cibernetica in un momento di fragilità emotiva nazionale.
Tutto ciò, nel tentativo di adeguare la risposta, anche sotto il profilo della prevenzione, alle mutate esigenze connesse all'emergenza sanitaria in atto.

In particolare, nell'ambito dell'attività di contrasto svolta dal Centro Nazionale per il Contrasto alla Pedopornografia Online - C.N.C.P.O.- sono stati trattati **3.243** casi, che hanno consentito di indagare **1.261** soggetti (con un incremento del **132%** in relazione ai casi trattati e del **90%** in relazione alle persone indagate rispetto all'anno precedente).

L'adescamento on line

Particolarmente significativi sono i dati relativi **all'adescamento on line**, con **401** casi trattati, evidenziando un considerevole incremento di vittime d'età compresa **tra 0-9 anni**. Tale dato sorprende perché indica una crescita nel numero delle denunce che riguardano i bambini che frequentano la scuola primaria: si tratta di bambini che non dovrebbero avere accesso libero a socialnetwork o ai servizi di messaggistica che, dichiaratamente, **non ammettono alla navigazione utenti sotto i 13/14 anni**.

Si tratta di un dato che denuncia uno stato di cose a cui, evidentemente, le regole di accesso che si sono dati i servizi della rete e le campagne di informazione non riescono a dare un contenimento adeguato e per il quale occorre un supporto ulteriore da parte dei genitori perché si facciano veicolo di informazione e di una supervisione quanto più possibile puntuale sull'uso delle piattaforme social.
Emergono inoltre alcuni elementi di preoccupazione in merito alle nuove frontiere dello sfruttamento sessuale dei minori online: un fenomeno come quello della **sextortion "l'estorsione sessuale conseguente ad uno scambio di immagini sessualmente esplicite"**, sino a pochi anni fà riguardava principalmente adulti o minori che frequentassero le scuole superiori (quindi oltre i quattordici anni), nell'ultimo anno ha fatto registrare un deciso abbassamento dell'età delle vittime: **14 casi infatti hanno interessato bambini nella fascia d'età 0-13 anni** (a fronte dei 2 del 2019); ulteriore elemento di riflessione

deve essere il fatto che di questi 14 casi **4 riguardano minori nella fascia d'età 0-9 anni**, categoria il cui numero di vittime fino allo scorso anno era pari a zero.

Il cyber bullismo

Per quanto riguarda il fenomeno del cyber bullismo, la Polizia Postale e delle Comunicazioni ha trattato **412** casi e indagato **118** minori.

Dati per reati riconducibili al Cyberbullismo - Casi trattati con vittime minorenni						
	Stalking	**Diffamazione online**	**Ingiurie, minacce / molestie**	**Furto di identità su social network**	**Divulgazione e diffusione di materiale pedopornografico su social network**	**TOTALE**
Casi trattati 2020	21	116	127	71	77	412
Minorenni denunciati all'Ag 2020	2	20	23	7	66	118

Si tratta di un fenomeno che ha subito indirettamente l'influenza della pandemia laddove ha aumentato esponenzialmente il tempo di permanenza dei minori in rete, con l'evidente rischio di essere vittima di prepotenze, insulti, minacce e altre forme di prevaricazione digitale.

Sin dal marzo 2020 le attività scolastiche si sono fortemente ridotte e se, da una parte, tale stato di cose ha drasticamente ridotto il contatto diretto tra ragazzi, offrendo meno spunti per contrapporsi, dall'altra, ha aumentato la loro presenza in rete, grazie all'attivazione della Didattica a Distanza.

La maggiore presenza dei genitori in casa per il lockdown e lo smartworking, la necessità di condividere i supporti per consentire l'attività scolastica e lavorativa, hanno probabilmente potenziato almeno nelle prime fasi dell'emergenza i meccanismi di prevenzione delle condotte di prepotenza tra minori, intercettandole e bloccandole prima che diventassero diffamazioni, persecuzioni o altre gravi condotte che meritano la denuncia penale.

Le stesse restrizioni ai movimenti dei cittadini hanno favorito gli accessi al Commissariato di ps online quale portale "sicuro" da un punto di vista sanitario, per ricevere aiuto e orientamento (+213% delle visite), e hanno ritardato in molti casi la proposizione delle denunce che sono infatti ricominciate a crescere proprio subito dopo la riduzione delle restrizioni al movimento dei cittadini sul territorio nazionale (dal giugno 2020).
Interessante osservare come, nell'ultimo anno, sembri evidenziarsi sempre di più per gli adolescenti l'inconsistenza della distinzione fra i diversi fenomeni che li coinvolgono come autori e come vittime: sexting, revengeporn, cyberbullismo, grooming, sextortion e pedopornografia si mescolano sempre più frequentemente, determinando casi nei quali diventa molto complesso distinguere l'origine dall'effetto dei comportamenti problematici.

Le esplorazioni sessuali consensuali diventano talvolta il pretesto per vere e proprie diffamazioni di gruppo sui social, come nella tipica modalità del cyberbullismo, e dietro la produzione delle stesse immagini a volte c'è una sorta di gara a chi si misura meglio con espressioni sessuali performanti simili a quelle pornografiche, finendo per arrivare magari a pretendere altre immagini sessuali da coetanei, con la minaccia di viralizzare i contenuti privati scambiati per "amore".
A questo si aggiunge la superficialità tipica dell'età che porta a guardare distrattamente quanto gira sui gruppi di messaggistica in cui qualcuno fantastica di diventare il re del "gore", diffondendo spontaneamente materiale cruento, violento, mischiato con la pedopornografia.
Nel corso del 2020 sono state diverse le attività investigative che, sulla scia di quanto già osservato con gli stickers di whatsapp, immagini diffuse tra i ragazzini come ritagli di foto violente, antisemite, discriminatorie ed infine pedopornografiche, hanno consentito di individuare decine di minorenni che, con livelli assai labili di consapevolezza, partecipavano al turpiloquio tra coetanei, scambiandosi immagini illegali di pedopornografia, di violenza, rubate a compagne di classe e diffuse senza controllo.
Delle **412** denunce sporte nel 2020 per reati riconducibili al cyberbullismo, **116** hanno riguardato diffamazioni e **127** forme di molestie e minacce diffuse in rete in danno di vittime minorenni da altri minorenni.

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

Tra le attività di polizia giudiziaria, sono state effettuate **14** operazioni di rilievo condotte dagli Uffici territoriali della Specialità e coordinate dal Centro, alcune delle quali svolte in modalità sotto copertura online anche nelle Dark Net e scaturite da segnalazioni pervenute nell'ambito dell'attività di cooperazione internazionale svolta dal C.N.C.P.O.

Operazione Amnesia

Tra le indagini più significative avviate direttamente dal Centro nell'ambito dei reati di sfruttamento sessuale dei minori, si segnala una delicata attività, denominata Operazione Amnesia, svolta nell'ambito delle Dark Net, che ha consentito di trarre in arresto un 30enne

per detenzione di materiale di pornografia minorile, aggravato dall'ingente quantità, dall'utilizzo di mezzi di anonimizzazione e criptazione, nonché dalla particolare violenza di alcune immagini rinvenute.
In particolare, l'uomo produceva filmati di abusi sessuali ai danni di una bambina di pochi anni, visibilmente narcotizzata. I video sono stati poi diffusi e commercializzati nel dark web.
L'indagine ha preso il via dall'analisi dei filmati che gli investigatori del C.N.C.P.O. hanno rilevato durante un'attività sotto copertura.

Operazione "Luna Park"

A dicembre 2020, è stata inoltre portata a termine un'altra importante operazione, di contrasto alla pedopornografia, denominata "Luna Park", condotta dal Compartimento Polizia Postale e delle Comunicazioni di Milano con il coordinamento del C.N.C.P.O., presso il Servizio Polizia Postale e delle Comunicazioni. L'indagine, durata due anni, è stata condotta in modalità sotto copertura e ha consentito di individuare 159 gruppi su chat peer to peer che garantiscono l'anonimato, di cui 16 organizzati secondo i crismi di vere e proprie associazioni. Gli abusi ritratti riguardavano prevalentemente bambine e bambini in tenera età e, in alcuni casi, anche neonati.

L'accurata attività investigativa, che ha consentito raccogliere elementi probatori in relazione a 432 utenti, di cui 81 italiani, ha avuto ampio respiro internazionale, coinvolgendo, attraverso gli strumenti di cooperazione di Polizia, più di 70 Stati stranieri. Nell'apice della fase esecutiva sono stati eseguiti in tutta Italia 60 decreti di perquisizione, che hanno portato a 43 denunciati e 17 arresti per ingente quantità di materiale realizzato mediante sfruttamento sessuale dei minori.

C.N.C.P.O. – Attività di prevenzione

Per quanto concerne l'attività di prevenzione svolta dal C.N.C.P.O. attraverso una continua e costante attività di monitoraggio della rete, sono stati visionati **34.120**, di cui **2.446** inseriti in black list e oscurati in quanto presentavano contenuti pedopornografici.
Con il D.P.C.M. dell'8 marzo u.s, è stata disposta la sospensione delle attività scolastiche e la conseguente attivazione della didattica a distanza per tutti gli Istituti. A tal proposito, sono pervenute diverse segnalazioni relative a episodi di intrusione nelle piattaforme dedicate alla formazione degli studenti, verosimilmente commessi da soggetti estranei alle classi, con la finalità di disturbare le lezioni.
Gli uffici territoriali della Specialità hanno avviato numerose verifiche volte ad individuare i responsabili degli accessi non autorizzati, svolgendo un assiduo monitoraggio anche sulle app di messaggistica istantanea, all'interno delle quali è stata accertata la presenza di gruppi dedicati.

Particolare attenzione è stata indirizzata all'attività di prevenzione e contrasto al revenge porn, alla diffamazione on line e allo "stalking", reati afferenti al cosiddetto "Codice Rosso", le cui indagini sono profuse non soltanto per giungere all'identificazione del responsabile del reato, ma anche per la rimuovere i contenuti dal web o, quantomeno, per limitarne la divulgazione massiva.

Reati commessi attraverso i social network

Particolare attenzione è stata indirizzata all'attività di prevenzione e contrasto al **revenge porn**, alla **diffamazione on line** e allo "**stalking",** reati afferenti al cosiddetto "Codice Rosso", le cui indagini sono profuse non soltanto per giungere all'identificazione del responsabile del reato, ma anche per la rimuovere i contenuti dal web o, quantomeno, per limitarne la divulgazione massiva.
In relazione ai reati contro la persona perpetrati sul web sono state indagate **1362** persone, resisi responsabili di aver commesso **estorsioni a sfondo sessuale, stalking, molestie, minacce e ingiurie,** in riferimento al reato di **diffamazione online**, sono stati trattati **2227** casi, indagate **901** e visionati **2870** spazi virtuali.
Particolare rilevanza ha assunto l'attività di contrasto al **revenge porn**, con **126** casi trattati e **59** persone indagate.

Si segnala, inoltre, l'attività investigativa volta ad arginare il fenomeno dell'***hate speech***, con l'individuazione nell'ambito del monitoraggio della rete o su segnalazione di altri Uffici o di cittadini, in riferimento a commenti diffamatori e di *hate speech* nei confronti di minoranze o di determinate categorie di persone. e l'approfondimento a livello investigativo delle segnalazioni dell'UNAR (Ufficio Nazionale Anti discriminazioni Razziali), organismo della Presidenza del Consiglio dei Ministri e dell'OSCAD (Osservatorio per la Sicurezza contro gli Atti Discriminatori).

Sono state approfondite a livello investigativo **111 s**egnalazioni ricevute sul portale del Commissariato di P.S. online e di particolare rilievo è stata l'attività di **pubblico soccorso** per i manifesti intenti suicidari, segnalati attraverso il citato portale, dai vari social network e dal Servizio di Cooperazione Internazionale, che ha portato ad individuare e attivare i servizi sanitari preposti per **28** persone.

Campagne preventive di sensibilizzazione

In considerazione della specificità dei fenomeni delittuosi di interesse della Polizia Postale e delle Comunicazioni, che incidono in maniera diretta e profonda sulla vita delle persone, soprattutto in ambiti estremamente delicati come la tutela dei minori e delle fasce più esposte della cittadinanza, la Specialità, anche in collaborazione con altre articolazioni dipartimentali e altri Ministeri, svolge un'intensa attività di comunicazione, nell'ottica della massima vicinanza al cittadino e di una "educazione al digitale", che consenta a giovani e adulti un corretto approccio all'uso di internet.

In tale direzione, ormai da diversi anni, si sussegue l'impegno in campagne di sensibilizzazione e prevenzione dei rischi e pericoli connessi all'utilizzo della rete, rivolte soprattutto alle giovani generazioni; campagne che, nell'anno in esame, in relazione alle misure di contenimento intervenute a seguito dell'emergenza epidemiologica da COVID-19 e alla conseguente chiusura di numerosi istituti scolastici su tutto il territorio nazionale, sono state realizzate anche con incontri in videoconferenza: una scelta necessaria che ha, comunque, consentito di raggiungere un numero elevato di giovani e di fornire loro informazioni sulle insidie e sulle fenomenologie criminali della rete.

Tra le iniziative più tradizionali e significative realizzate in tale ottica preventiva si inserisce **"Una vita da Social"**, la campagna itinerante giunta all'8^ edizione, grazie alla quale nel corso dell'anno 2020 sono stati incontrati oltre **134.000** studenti, **7.000** genitori, **9.000** docenti, per un totale di **1.240** istituti scolastici (per i quali è stata messa a disposizione anche un'email dedicata: progettoscuola.poliziapostale@interno.it).
Nel medesimo solco di azione si segnala l'impegno della Polizia Postale e delle Comunicazioni in occasione della **Giornata mondiale per la sicurezza in rete: "Safer Internet Day"**, svoltasi in data 11 febbraio 2020: in collaborazione con gli Uffici Scolastici Regionali ed il Ministero dell'Istruzione, la Specialità ha organizzato, in **100** capoluoghi di provincia, incontri educativi sulla sicurezza *online* dal tema "*uniti per un internet migliore*", che hanno coinvolto simultaneamente oltre **60.000** studenti delle scuole di ogni ordine e grado.
Al fine di innalzare i livelli di prevenzione e per soddisfare l'avvertita esigenza di assicurare anche un supporto a tutte quelle figure di riferimento per i "nativi digitali" (che possono concorrere nel guidarli verso un rapporto equilibrato con la rete), è stato pensato e realizzato, con il contributo scientifico della Società Italiana di Pediatria, il progetto **"In rete con i ragazzi: guida all'educazione digitale"**, attraverso cui sviluppare uno strumento rapido e agevole per chi ogni giorno si confronta con i più giovani. L'iniziativa, proposta per il biennio 2020-2021 in tutti i capoluoghi di regione, prevede corsi di formazione per **30.000** medici pediatri, dirigenti scolastici e animatori digitali.

Anche nel corso dell'anno 2020, grande attenzione è stata rivolta alla prevenzione di ogni forma di prevaricazione in danno delle fasce più deboli, nella consapevolezza che il panorama del rischio *online* per i minori sia notevolmente cresciuto negli ultimi 10 anni, inducendo l'emersione non solo di casi emergenziali e sporadici, ma anche di veri e propri fenomeni di grande allarme sociale, tra cui, primo fra tutti, il *cyberbullismo* (agevolato dall'uso distorto delle nuove forme di comunicazione, connesso allo sviluppo esponenziale della tecnologia e alla formidabile attrazione subita dai bambini e dai ragazzi verso il mondo virtuale).
Per tale motivo, è stato riproposto il *format* teatrale **#cuoriconnessi,** con l'intento di prevenire qualsiasi forma di prevaricazione e di violenza di genere, attraverso un'opera di responsabilizzazione in merito all'uso della parola. Durante lo spettacolo, dedicato agli studenti delle scuole, viene richiamata l'importanza delle parole in tutte le sue sfumature, attraverso filmati, letture, musiche e testimonianze dirette, fornendo in tal modo alla platea informa-

zioni utili anche per comprendere le conseguenze che questi fenomeni possono generare nella vita di ogni adolescente.
Nella medesima direzione si segnala l'iniziativa **"Giovani Ambasciatori contro il Cyberbullismo",** frutto della sinergia tra la Polizia Postale e delle Comunicazioni, il Ministero dell'Istruzione, dell'Università e della Ricerca e il MOIGE (Movimento Italiano Genitori uniti), attraverso cui si sono resi protagonisti attivi gli studenti di varie scuole, i quali, in veste di "ambasciatori" della lotta al *cyberbullismo*, divengono punti di riferimento di altri ragazzi che abbiano necessità di chiedere aiuto o di segnalare casi concreti di tale fenomeno.

Commissariato di P.S. Online

L'esigenza di assicurare un'efficace e tempestiva azione di contenimento e di contrasto alle molteplici fenomenologie criminose, di specifico interesse per la Polizia Postale e delle Comunicazioni, trova un valido e collaudato strumento nel portale del Commissariato di P.S. online. Attraverso tale canale di riferimento, infatti, gli operatori della Specialità, non solo raccolgono le più svariate segnalazioni su eventi e situazioni che, in quanto riconducibili a potenziali condotte delittuose, appaiono suscettibili di sviluppi investigativi, ma offrono, altresì, una quotidiana assistenza agli utenti del *web*, veicolando informazioni per un uso sicuro della *rete*.

In tale direzione, il potenziamento del *Commissariato di PS online* imposto dall'emergenza epidemiologica in atto (che nella fase più acuta del primo semestre 2020 è stata caratterizzata anche da un lungo periodo di *lockdown*), ha permesso di innalzare i livelli di interazione con i cittadini, i quali, in una situazione di emergenza sanitaria, hanno mostrato un accresciuto bisogno di strumenti idonei a garantire rapidi ed efficaci riferimenti istituzionali a cui poter indirizzare le proprie segnalazioni e le proprie preoccupazioni e da cui poter apprendere le informazioni utili a prevenire il consumarsi di condotte delittuose.
La bontà dell'azione strategica prescelta è dimostrata dai dati statistici: il Commissariato ha evaso **25.952** richieste di informazioni, a fronte delle **22.853** dell'anno precedente e ricevuto **56.532** segnalazioni dai cittadini, in numero sensibilmente superiore a quelle dell'anno 2019, attestate a **23.311**.

Nell'ambito del diversificato contesto di azione preventiva, operata dalla Polizia Postale e delle Comunicazioni, particolare attenzione viene costantemente rivolta anche al fenomeno della "disinformazione", con un impegno ancor maggiore nel contesto emergenziale vissuto a causa della diffusione del virus Sars-Cov2: la crescente proliferazione delle cd. *fake news*, sovente caratterizzata da un potenziale impatto negativo sulla salute pubblica e sulla corretta ed efficace comunicazione istituzionale, ha imposto di innalzare i livelli di attenzione nell'ottica di un efficace contenimento del particolare fenomeno.
Il contrasto attuato, rispetto alle varie fenomenologie delittuose che hanno caratterizzato la fase dell'emergenza Covid-19 (talora agevolate dalla diffusione di false notizie e/o informazioni), è stato, quindi, realizzato non soltanto sotto il profilo della repressione dei reati

tentati o consumati, ma anche nell'ottica di interventi di tipo preventivo, tesi a veicolare alla cittadinanza le informazioni utili per contenere ed impedire le condotte delittuose sopra richiamate.

Anche in questo particolare ambito di azione, il raffronto tra i dati statistici del 2020, rispetto al 2019, ha consentito di registrare un notevole incremento, pari al **436 %,** delle segnalazioni effettuate dai cittadini. A tal proposito, dall'inizio dell'emergenza COVID-19, sono stati individuati **134** eventi, riconducibili al fenomeno della disinformazione, rispetto ai quali è stato predisposto uno specifico *alert* funzionale alla veicolazione delle corrette informazioni.

Periodo gennaio/dicembre	**Segnalazioni Fake News**	**Alert diramati**
Totale 2019	25	30
Totale 2020	**134**	**137**
Incremento percentuale tra 2019 e 2020	+436%	+357%

Elementi sul cybercrime nel settore finanziario in Europa

[A cura di Pier Luigi Rotondo, IBM]

Il cybercrime finanziario ha subito un'ulteriore evoluzione nel corso degli ultimi 12 mesi, sia nel modus operandi dei gruppi di criminali cyber che nei malware usati. Il cybercrime è indubbiamente dominato da gruppi internazionali, ben strutturati e organizzati.
Nell'analisi che segue, presento e commento i risultati delle rilevazioni sul cybercrime nel settore finanziario in Europa nel corso del 2020 ed evidenzio alcune tendenze che potremmo osservare nel corso del 2021. Questo lavoro è stato possibile anche grazie ai contributi del gruppo di ricerca IBM Security, IBM X-Force, i dati estratti dalla rete mondiale di IBM Security Trusteer e al lavoro quotidiano dei colleghi IBM Security che desidero ringraziare. Tutte le fonti consultate sono elencate nella bibliografia al termine del capitolo.

Un anno di cybercrime finanziario

Il *financial fraud*, frode bancaria o finanziaria, passa quasi sempre attraverso il furto delle credenziali d'accesso ai sistemi bancari o di pagamento e riutilizzate per transazioni fraudolente all'insaputa del titolare. Invece di attaccare direttamente la banca, si preferisce l'obiettivo più facile di attaccare i suoi clienti.

L'analisi delle principali campagne del 2020 mostra che la frode avviene prevalentemente attraverso i seguenti vettori di attacco:

- malware per il furto di credenziali o manipolazione di una transazione (financial malware);
- hacking del dispositivo mobile tramite SIM Swap o emulazione software dello smartphone;
- phishing per il furto di credenziali di accesso e autenticazione forte (credential theft).

La tecnica, o la combinazione di tecniche, varia in base alla vittima, con differenze tra il cliente finale (retail) oppure aziendale (corporate) [1]. Malware e phishing si sono ripartiti il compito in maniera abbastanza equa [1][2] sulle vittime retail. Per il mercato corporate c'è stata invece una prevalenza di schemi di attacco attorno ai malware [1].

Financial malware

ENISA, Agenzia dell'Unione Europea per la Cybersecurity, pone i malware al primo posto nel panorama delle minacce informatiche [3].
Nel contesto variegato di tutti i malware, qui ci limitiamo a prendere in considerazione solo il financial malware, o malware per frodi finanziarie. Riportiamo dati e valutazioni sul malware per frodi al settore finanziario e alle sue declinazioni (banche, finanza diversificata e assicurazioni) limitatamente a osservazioni fatte da IBM Security Trusteer nell'area geografica EMEA (Europa, Medio Oriente e Africa) sull'intero anno 2020.

QakBot, TrickBot, DanaBot e Bugat sono stati i principali malware dell'anno, seguiti da una nutrita lista di altri malware con un impatto minore. Il primo diagramma (**Figura 1**) descrive la distribuzione dei malware così come sono stati rilevati sugli endpoint (dispositivi utente) infetti. Continua la tendenza che osserviamo ormai da diversi anni di graduale frammentazione su un numero crescente di malware, ciascuno in porzione sempre minore. Relativamente all'Italia, abbiamo osservato numerose campagne basate su Ursnif/Gozi, sLoad downloader, Dridex, AgentTesla e soprattutto Emotet.

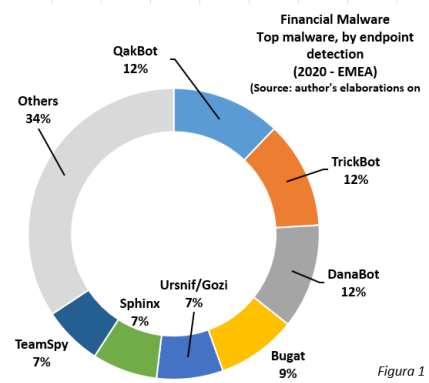


Figura 1

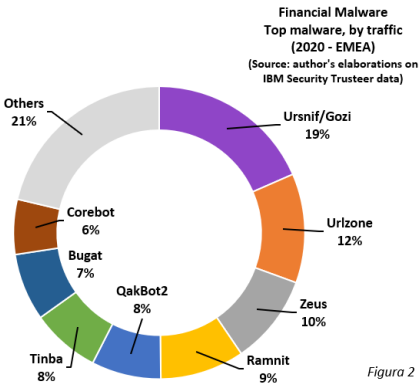


Figura 2

Nei diagrammi di **Figura 1** e **Figura 2** abbiamo scelto di *non* riportare l'incidenza di Emotet, indubbiamente diffuso in Italia e in Europa, in quanto il suo ruolo è stato prevalentemente di loader per altri malware, in particolare QakBot e TrickBot, con un probabile sodalizio tra i gruppi criminali. In questo connubio, Emotet è il veicolo che infetta la macchina della vittima, avendo spiccate caratteristiche di evasione dai prodotti antimalware, per poi scaricare il payload, spesso l'eseguibile di QakBot o TrickBot a cui poi lascia il controllo.

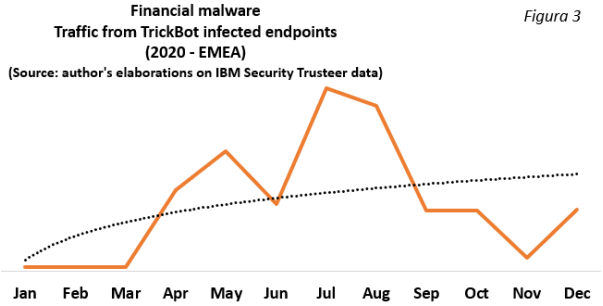
Oltre alle infezioni sugli endpoint, abbiamo catturato e analizzato il traffico generato da endpoint infetti da malware che tentano di accedere al sito web dell'organizzazione target, ad esempio una banca, per perpetrare una transazione fraudolenta (**Figura 2**).
Il questo caso i malware che hanno generato maggiore attività sono Ursnif/Gozi, Urlzone, Zeus, Ramnit, e a seguire una lunga lista di altri malware.
Questa seconda tipologia di rilevazione (**Figura 2**) è speculare a quanto già osservato relativamente agli endpoint infetti (**Figura 1**). Le due rilevazioni si integrano l'un l'altra. Mentre il diagramma di **Figura 1** misura la capacità del malware di evadere le protezioni di rete e di sistema, e infettare il computer o smartphone della vittima, la **Figura 2** misura invece la quantità di traffico che i dispositivi infetti riescono a generare verso il sito web della banca, e che potenzialmente mettono a rischio l'account utente. Nel raffrontare i due diagrammi occorre tenere in giusta considerazione il diverso comportamento di ciascun malware, e soprattutto come vengono rilevati i dati.

Una soluzione di sicurezza deve essere in grado di individuare e bloccare entrambi i fenomeni, combinandoli per proteggere l'endpoint e ciascuna fase della transazione bancaria.

Attività dei principali financial malware nel corso dell'anno

Secondo le nostre rilevazioni, i principali financial malware hanno mostrato un picco di attività nel periodo estivo, e una tendenza di leggera crescita nel corso dell'anno.

Figura 3

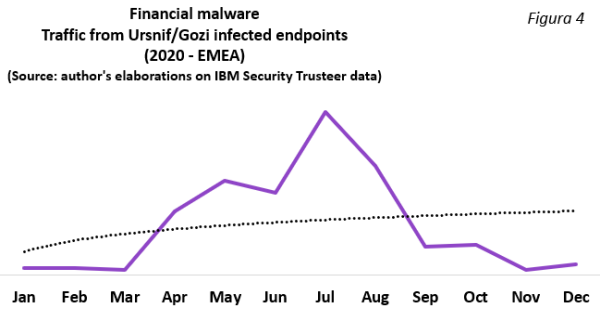


TrickBot prosegue l'evoluzione verso una vera e propria piattaforma di attacco, con una struttura modulare che consente di noleggiare il malware a terzi, secondo un modello MaaS (Malware-as-a-Service).
Ciascuna campagna TrickBot è caratterizzata da un identificatore di gruppo (tag) assegnato al cliente di turno. Ciascuno gruppo può così sfruttare le caratteristiche di propagazione di TrickBot, importando all'interno del malware le tattiche, tecniche e procedure e costruire attacchi altamente mirati [4].
Una coalizione di aziende Tech (Microsoft, FS-ISAC, ESET, Black Lotus Labs, NTT, e Broadcom/Symantec) ha smantellato a ottobre l'infrastruttura di backend della botnet per la distribuzione di TrickBot [5]. Non è da escludere che il picco negativo novembre 2021 (**Figura 3**) sia proprio conseguenza di questa operazione.
Si stima che fino a quella data TrickBot ha infettato circa 1 milione di computer, inclusi molti dispositivi IoT. Questa operazione, assieme a quella di gennaio 2021 contro la botnet di Emotet, segnano due importanti battute di arresto di TrickBot del quale speriamo di vedere ricadute positive nei prossimi mesi.

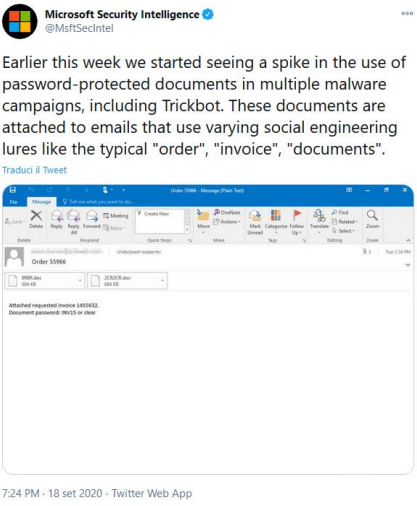
La cattura delle credenziali di accesso alla posta elettronica, sia webmail che client installati sul computer o smartphone, è un'attività apparentemente anomala per un financial malware, ma è un andamento che osserviamo in crescita già da qualche anno. I gruppi cyber criminali fanno questo per avere una base dalla quale lanciare attacchi di tipo BEC, diffondendo malware da caselle elettroniche reali e spesso note alla vittima, con un'efficacia nettamente maggiore rispetto a quanto non si riesca a fare con il tradizionale phishing. I numerosi esempi di campagne veicolate tramite PEC ne sono un esempio.

Ciascun elemento, apparentemente insignificante, può essere utile per costruire e dare maggiore credito ad attacchi futuri. Questo non può che farci pensare che mentre noi analizziamo quanto accaduto, i gruppi cyber criminali stanno già pensando a schemi di attacchi futuri.

Figura 4



L'obiettivo principale dei malware per frodi finanziarie, era e rimane, l'impossessarsi delle credenziali di accesso ai sistemi di pagamento, oppure dei dati delle carte di pagamento, oppure ancora di cambiare ad insaputa della vittima le coordinate di pagamento.
A seconda della tattica, l'attacco può spaziare dal semplice furto di credenziali di accesso, al furto del fattore di autenticazione forte del cliente (SCA – Strong Customer Authentication) introdotto della normativa PSD2 [6], al furto dei dati delle carte di pagamento, e infine alla sostituzione delle coordinate di pagamento (IBAN o del wallet elettronico) questo ultimo caso soprattutto per i malware per dispositivi mobili.



Il malware è veicolato nella maggioranza dei casi attraverso documenti Office allegati ad e-mail [3] o file .zip protetti da password, all'interno di campagne di spamming che emulano grafica e marchi conosciuti, come ad esempio le comunicazioni di banche, della pubblica amministrazione, oppure di società di recapiti.
Nel caso del documento Office, una volta aperto, l'utente viene invitato ad abilitare l'esecuzione di macro, o altri contenuti attivi. Questa operazione apparentemente innocua fornisce al documento i privilegi necessari per scaricare il resto del malware da una *drop URL* sfruttando quasi esclusivamente strumenti nativi del sistema operativo, come la Powershell di Windows.

Nel caso del file zip, il documento malevolo è all'interno del pacchetto compresso e protetto da password, ma con una password molto semplice e sempre inclusa in chiaro nel testo della mail, In questo modo la vittima è in grado di aprire il file compresso e poi il documento malevolo contenuto all'interno. La catena degli incapsulamenti, con un file compresso e protetto da password, serve esclusivamente ad eludere alcuni sistemi di scansione e analisi automatica della e-mail che non riescono ad espandere archivi protetti da password.

Il malware è ospitato su provider russi nel 31% dei casi, statunitensi del 25% dei casi, ed in percentuali via via decresciti anche in altri paesi.
La collocazione geografica del provider indica solo dove è stato inizialmente caricato il malware, e non ci fornisce indicazioni precise sui threat actors.

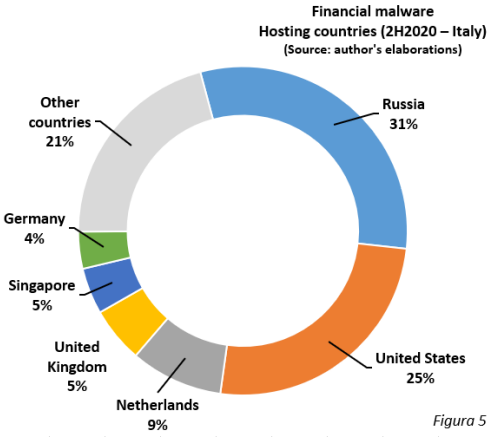
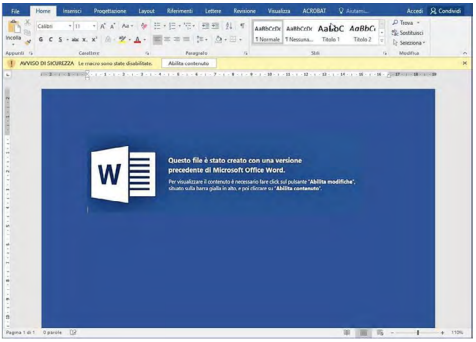


Figura 5

Analizzando nel dettaglio le singole URL, e i provider usati, si nota che i cyber criminali noleggiano spazio presso provider, oppure compromettono siti internet già esistenti, non aggiornati o con cattive configurazioni, oppure ancora depongono il malware in folder di upload pubblici e visibili, dai quali è poi universalmente disponibile. Spesso all'insaputa dei legittimi proprietari dello spazio che diventano vittime loro stesse.
Emblematico il caso della sezione Musei della Basilicata sul sito del Ministero per i Beni e le Attività Culturali che lo scorso luglio, per almeno cinque giorni, ha distribuito il malware Emotet caricato in una cartella non protetta senza che questo venisse prontamente individuato e rimosso. Da allora la URL della Direzione Regionale Musei Basilicata è segnalata come potenziale sorgente di malware, e di conseguenza la navigazione sull'intera sezione del portale è bloccata da molti browser e provider.
Questa condizione presenta un importante rischio in Italia, in quanto il recente *Monitoraggio dei portali istituzionali della PA* [7], condotto da Cert-AgID nel dicembre 2020 su oltre 21.000 portali istituzionali della Pubblica Amministrazione, evidenzia che solo il 9% di questi sono sufficientemente sicuri, mentre il restante 91% è caratterizzata da mancanza del protocollo HTTPS, gravi problemi di sicurezza, oppure ancora è mal configurato.

Nel corso del 2019 avevamo osservato molti documenti malevoli sfruttare la CVE-2017-0199 e la CVE-2017-11882, due Remote Execution Vulnerability per Windows molto insidiose, in quanto era sufficiente aprire il documento, e in talune circostanze fare la sola preview, per eseguire la componente malevola che scaricava il codice malware. Il mec-

canismo, su macchine non aggiornate, era particolarmente potente in quanto richiedeva un'interazione minima da parte della vittima.
Nel corso del 2020 gli attaccanti si sono mossi invece su un terreno decisamente più facile, sfruttando prevalentemente la debolezza umana, con documenti Office contenenti funzioni macro malevole.

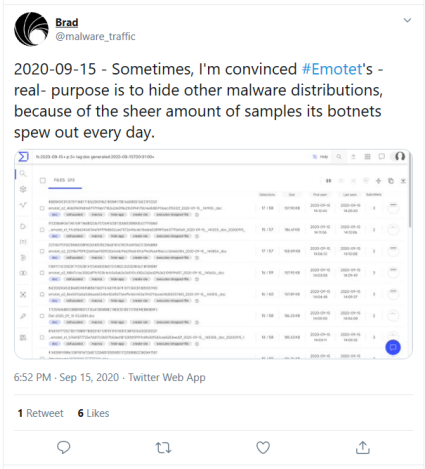


La differenziazione tra una campagna e l'altra sta principalmente nel messaggio usato per invitare la vittima ad aprire il documento e abilitare l'esecuzione delle macro, anche se l'obiettivo rimane lo stesso. Gli inviti più frequenti sono di abilitare le macro in quanto necessario per un aggiornamento di Word, oppure perché il documento è protetto, oppure molto più frequentemente in quanto il documento è creato con una versione più recente di Word. Tutte motivazioni false, il cui unico obiettivo è di eseguire la macro nascosta e non visibile all'interno del documento, che scarica e infine attiva il malware. Dopo l'attivazione, il malware comunica con la sua infrastruttura di controllo e con il gruppo cyber criminale attraverso una rete di nodi di Command-and-Control (C&C), dai quali riceve ulteriori elementi di configurazione, watch list, comandi remoti da eseguire sul sistema infetto, o attraverso i quali esfiltra i dati della macchina infetta, come username, password o URL visitate.

Durante la pandemia COVID-19 sono state osservate numerose ondate di spamming basate attorno a finte comunicazioni apparentemente provenienti dell'Agenzia dell'Entrate, INPS o altri enti che erogavano contributi economici. Tutte contenevano al loro interno allegati che sfruttavano macro di Office malevole.
Questo veicolo, molto più semplice dal punto di vista implementativo, ha reso possibile la realizzazione di una quantità molto elevata di campagne di attacco.

L'epopea di Emotet

Emotet è noto sin dal 2014, inizialmente come malware bancario specializzato nel furto di credenziali. A partire dal 2016 si ritaglia gradualmente una posizione di rilevo come *loader* per altri malware, principalmente QakBot, TrickBot e il ransomware Ryuk [8] in un probabile sodalizio criminale con altre cyber gang, offrendo la sua infrastruttura botnet per veicolare altri malware. Il modello operativo di Emotet è presumibilmente Access-as-a-Service, in quanto veicola fin dentro la macchina della vittima malware scritto da altri gruppi cyber criminali.



Anche in questo caso i documenti Office (prevalentemente Word) allegati ad e-mail invitate in automatico dalle tre botnet Epoch1, Epoch2 e Epoch3 sono stati il principale vettore.
Le campagne di spamming associate ad Emotet hanno spaziato dai pagamenti, alle notifiche di spedizioni giacenti, fino alle informazioni sul COVID-19, queste ultime soprattutto nei primi mesi della pandemia, per poi diminuire gradualmente nel corso dell'anno.
L'elusione dei sistemi antimalware passa anche tramite la generazione di codice polimorfico che cambia continuamente l'eseguibile del malware generando una quantità enorme di signatures (hash). Poiché molte soluzioni antimalware si basano proprio sul concetto di signature, una continua modifica dell'eseguibile malevolo induce difficoltà di rilevamento e analisi, rendendo possibile l'infezione anche su sistemi protetti. Negli esempi osservati da IBM X-Force ciascun hash è stato usato in media in 1.3 e-mail [9]. Con buona approssimazione possiamo immaginare che ciascuna e-mail malevola porta al suo interno una versione di Emotet pressoché unica. Alcune organizzazioni hanno individuato più di 200.000 varianti di Emotet [4].
Le vittime di Emotet sono localizzate, in ordine decrescente, negli Stati Uniti, Giappone, Germania, Italia, Regno Unito, Spagna e numerose altre nazioni. Si stima che nel periodo tra il 1° aprile 2020 e il 17 gennaio 2021 Emotet abbia infettato 1,6 milioni di computer in tutto il mondo [10].

Il 27 gennaio 2021 un'importante operazione delle forze di polizia di Olanda, Germania, Stati Uniti, Regno Unito, Francia, Lituania, Canada e Ucraina, coordinata da Europol ed Eurojust [11], ha portato all'arresto in Ucraina di due persone, e all'identificazione di molti altri fiancheggiatori in altre nazioni, ma soprattutto al controllo dei server delle tre botnet di Emotet da parte dei tecnici delle forze di polizia coinvolte. Senza dubbio una delle più imponenti operazioni di polizia contro il cybercrime dell'ultimo decennio.
Una prima analisi dei conti bancari usati dal gruppo cyber criminale ha mostrato transazioni per circa 10.5 milioni di dollari negli ultimi due anni. Gli investigatori hanno anche accertato che il gruppo ha speso oltre mezzo milione di dollari per mantenere l'infrastruttura di circa 700 server, affittati (ma a volte semplicemente compromessi) presso provider di oltre 50 nazioni [10].
Al termine dell'operazione, le forze dell'ordine sono riuscite a prendere il controllo dell'infrastruttura, reindirizzando tutti i computer infetti verso alcuni server appositamente pre-

parati, sui quali è stata caricata una configurazione per disabilitare tutti i nodi infetti. Un approccio nuovo e di sicuro risultato per interrompere efficacemente le attività del crimine organizzato informatico.
Emotet potrebbe quindi aver subito una vera e propria battuta d'arresto, anche se i malware veicolati sono ancora in circolazione e ben lungi dall'essere bloccati. È quindi necessario che le organizzazioni eseguano quanto prima la pulizia da malware come TrickBot e QakBot che potrebbero essere stati veicolati da Emotet.
La ricaduta di questa operazione, assieme al take down della botnet di TrickBot [5], potrebbe essere di notevoli proporzioni e imporrà ai creatori di malware la messa a punto di nuovi canali per la distribuzione in futuro del loro malware.

Phishing verso il settore finanziario italiano

Il settore finanziario è tra le maggiori vittime del phishing [12].
Lo studio che segue si basa sull'analisi di 594 pagine di furto di credenziali per l'accesso a banche e altre istituzioni finanziarie italiane, attive e monitorate nel periodo 1° luglio – 31 dicembre 2020 (2H2020). Questa analisi non prende in considerazione i domini registrati con nomi verosimili di banche o prodotti finanziari (domain squatting) ma mai attivati, presumibilmente bloccati durante l'attivazione oppure abbandonati dagli stessi creatori.

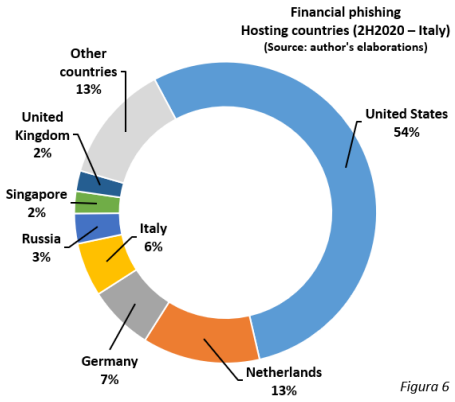


Figura 6

Limitandosi al settore finanziario italiano, nel secondo semestre del 2020 è stata osservata una media di 3,2 nuove pagine di phishing al giorno attivate e perfettamente funzionanti, con una crescita graduale nel corso dell'anno. Il picco si è raggiunto nel mese di dicembre 2020, con una media di 5,6 nuove pagine al giorno.
Una pagina di phishing ha generalmente una vita breve. Nel 72% dei casi studiati dura meno di 48 ore, ma il ricambio è tale da mantenere il numero di pagine attive sempre sostenuto. Ci sono comunque notevoli eccezioni, con alcune pagine rimaste attive anche oltre due mesi.
Il 54% dei siti di phishing verso il settore finanziario italiano è ospitato negli Stati Uniti, il 13% in Olanda, il 7% in Germania e un cospicuo 6% su due provider Italiani (**Figura 6**).
C'è da notare che quasi un terzo (32%) di tutti i siti analizzati, è ospitato su un unico provider, la statunitense Namecheap, tra le principali aziende di web hosting al mondo con oltre 10 milioni di domini gestiti.
Proprio come per le drop URL del malware, la collocazione geografica del provider che ospita la pagina di phishing non fornisce alcuna indicazione su dove siano realmente i

threat actors. È ipotizzabile che la collocazione e la scelta del provider siano da attribuirsi alla combinazione della facilità di creare domini, anche in maniera automatica via API e pagando in criptovaluta, assieme agli scarsi controlli da parte dei provider.

Il dato che più di ogni altro deve farci rilfettere è che il 91.2% delle URL di phishing usa il protocollo HTTPs, il cosidetto HTTP "sicuro".

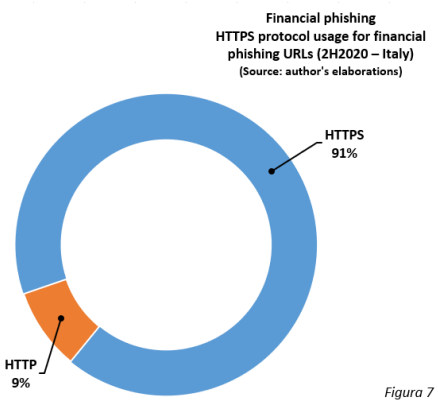


Figura 7

Tecnologie come HTTPS e l'SSL/TLS sono progettate per proteggere le comunicazioni tra client e server, tuttavia l'icona del lucchetto nella barra indirizzi del browser può creare la falsa l'illusione che un sito web possa essere considerato attendibile. Questo interferisce molto con il giudizio che i visitatori danno del internet.

Tutto questo deve indubbiamente guidare le indicazioni che le organizzazioni forniscono ai propri clienti, relativamente alla presenza di un lucchetto chiuso e dalla dicitura "https://" nella barra degli indirizzi come elementi per distinguere una pagina sicura da una non sicura. Se l'uso di una connessione HTTP di tipo semplice (http://) sicuramente non fornisce nessuna garanzia sulla controparte, l'uso del protocollo HTTPS, senza successive verifiche sul *tipo di certificato, chi lo ha emesso e per quali scopi*, ancora una volta non può darci nessuna indicazione di sicurezza.

La decisione sulla veridicità di una connessione HTTPS dovrebbe essere legata alla *validazione* del dominio. Nella totalità dei casi i phisher usano domini con certificati di tipo Domain Validation (DV), la forma più semplice di validazione e quella proposta dai siti di web hosting per qualche euro o addirittura gratuitamente. I certificati di tipo Domain Validation, malgrado siano in grado di garantire comunicazioni criptate e sicure attraverso connessioni HTTPS, poco o nulla dicono sulla autenticità di chi possiede il sito web al quale siamo collegati. Questa ambiguità viene sfruttata dai phisher quando usano comunicazioni HTTPS. Non esiste nessuna forma di controllo sull'entità o sulla persona che richiede un certificato SSL/TLS per abilitare un sito al protocollo HTTPS, ma si controlla in automatico solo che chi richiede il certificato abbia il controllo del dominio in questione, cosa ovvia.

I siti reali di banking italiani, purtroppo ancora con qualche grave eccezione, usano quasi sempre certificati di tipo Organization Validated (OV), o meglio ancora, Extended Validation (EV). Quest' ultimo tipo di validazione del certificato, il cui rilascio è articolato e subordinato a numerosi controlli anche di natura legale sull'entità che lo richiede, fornisce le maggiori garanzie sulla controparte. Per evitare il phishing, il controllo non dovrebbe essere sull'utilizzo del protocollo HTTPS, ma bensì sul tipo di validazione del certificato usato, e

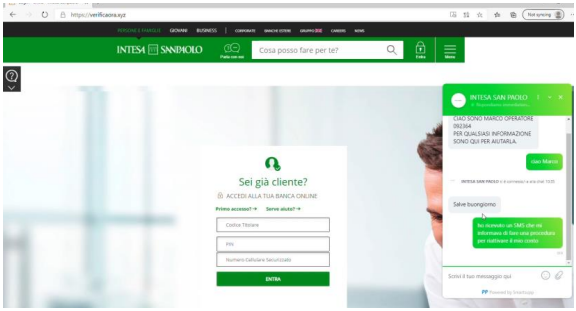
limitarsi a connessione solo verso siti che usino certificati di tipo Organization Validated (OV) o Extended Validation (EV).
Alcuni, ma non tutti, i browser forniscono un'indicazione visiva sul tipo di validazione del certificato, ed è su questo che gli utenti dei servizi di banking andrebbero informati ed istruiti.

2020-12-31	www.it-nexi.login-titolari.com
2020-12-31	it-nexi.login-titolari.com
2020-12-29	www.cartabcc.bcc-titolari.com
2020-12-29	www.sms-titolari.com
2020-12-29	cartabcc.sms-titolari.com
2020-12-29	cartabcc.bcc-titolari.com
2020-12-29	sms-titolari.com
2020-12-29	www.cartabcc.sms-titolari.com
2020-12-29	www.cartabcc.app-titolari.com
2020-12-29	cartabcc.app-titolari.com
2020-12-29	nexi-it.login-titolari.com
2020-12-29	www.nexi-it.login-titolari.com
2020-12-29	nexi-it.login-titolari-sms.com
2020-12-29	www.nexi-it.login-titolari-sms.com
2020-12-29	www.nexi-it.login-titolari-v1.com
2020-12-29	login-titolari-v1.com
2020-12-29	www.login-titolari-v1.com
2020-12-29	nexi-it.login-titolari-v1.com
2020-12-29	www.app-titolari.com
2020-12-29	app-titolari.com
2020-12-29	login-titolari.com
2020-12-29	www.login-titolari.com
2020-12-29	bcc-titolari.com

Frequente durante l'anno il fenomeno delle *phishing factory*, vere e proprie fabbriche di phishing che riescono a registrare e spesso attivare una grande quantità di domini di phishing anche verso target diversi, nel giro di poche ore.
Il phishing verso il settore finanziario italiano è veicolato principalmente tramite e-mail e SMS, e quest'ultima variante è comunemente denominata smishing, parola ottenuta dalla contrazione di SMS e phishing. In generale il phishing finanziario mira al furto delle credenziali di accesso, come il codice cliente in tutte le sue denominazioni, la password o PIN, e la OTP di accesso e tutti i suoi equivalenti, ma anche altre informazioni utili a rendere più agevole un accesso fraudolento, come numero di telefono dell'utente, il codice fiscale e l'indirizzo e-mail.
La frode è normalmente realizzata attraverso una sequenza di passi successivi, in ciascuno dei quali vengono rubate solo alcune credenziali, o pezzi di credenziali, per poi ricomporre tutto assieme durante l'attacco.

Nel corso del 2020, abbiamo notato un incremento dell'uso di falsi operatori bancari, e chat live di assistenza. I falsi operatori bancari richiamano il numero di telefono che spesso viene chiesto nella pagina di phishing, presentandosi come addetti della banca che hanno notato movimenti sospetti. Questa tecnica viene chiamata *vishing* (da Voice Phishing). Dipendentemente da quanto la vittima ha già eventualmente inserito nella prima fase del phishing, i finti operatori chiedono tutti gli elementi di autenticazione, oppure solo quelli mancanti. In particolare, questa tecnica è molto usata per convincere la vittima a dare i codici one-time di autenticazione forte del cliente (Strong Customer Authentication) che sotto diverse denominazioni ciascuna banca invia in virtù delle specifiche tecniche contenute nella direttiva PSD2. Si può ipotizzare che, mentre è al telefono con noi, il finto addetto faccia login sul sito vero della banca e per questo ha bisogno dei codici one-time che proprio in quel momento la banca invia al nostro cellulare o alla App installata sul nostro smartphone, e che lui non può avere senza il nostro aiuto.

C'è da notare che molti sistemi VOIP consentono la configurazione del numero chiamante in uscita, quindi non c'è da sorprendersi se alcune delle chiamate dai finti operatori arrivano da un numero di telefono che è proprio quello della banca [13].



Approccio simile si ha nelle finestre di chat live che cominciano ad essere presenti sul alcune pagine di furto di credenziali. In questo caso l'operatore via chat ha lo stesso ruolo dell'operatore telefonico nel caso descritto precedentemente, e mira a carpire gli elementi di autenticazione ancora mancanti, e l'elemento di autenticazione forte necessario per alcune operazioni a più alto rischio, inclusa l'immissione bonifici.
Vista la semplicità realizzativa e del basso livello di rischio di chi la perpetra, si prevede una crescita di questo approccio combinato al phishing nel corso dell'anno 2021.

Per riassumere, le caratteristiche distintive delle campagne di phishing e malware sono:

- Perfetta localizzazione in lingua italiana. Sono pressoché scomparse le e-mail contenenti i grossolani errori grammaticali che vedevamo in passato, o tradotte in automatico;
- Utilizzo frequente di chat live in lingua italiana o addetti bancari telefonici. Questo, assieme al punto precedente, ci porta a pensare che il fenomeno degli attacchi bancari in Italia è operato da attori cyber criminali italiani, anche se con utilizzo di infrastruttura estera.
- Necessità di furto del secondo fattore di autenticazione, che spinge necessariamente la frode ad un livello molto più avanzato di quanto non era fino a pochi mesi fa.

Molti phishing kit espongono in chiaro, tramite URL accessibili a chi ne conosce il path esatto, i dati delle vittime della campagna di phishing. Questa che ad una prima analisi potrebbe apparire un errore di chi ha scritto il phishing kit (Sensitive Data Exposure) per la sua frequenza potrebbe invece essere spiegata come una scelta dei *threat actor* per attingere ai dati "pescati" senza la necessità di alcuna forma di login al sito di phishing, rendendo più difficile il tracciamento e un'eventuale l'analisi forense.
Questa situazione è di particolare gravità e pericolo per la vittima, in quanto i suoi dati rimangono visibili e potrebbero cadere in mano, non solo degli attaccanti (cosa di per sé già estremamente pericolosa), ma anche di altri threat actors "parassiti" che seguono gli attacchi, e catturano le credenziali di accesso per poi costruirci nuove campagne di attacco.

SIM swap ed emulazione dello smartphone

Il *SIM swap* (scambio di SIM) è uno dei fenomeni che ha registrato maggiore crescita durante l'anno. L'attacco SIM swap parte da una nuova SIM con stesso numero telefonico della vittima, ma emessa a sua insaputa usando un suo documento rubato o contraffatto, e in taluni casi anche in assenza del documento sfruttando la compiacenza del rivenditore, e consente di ricevere gli SMS o gli altri codici autorizzativi inviati dalla banca alla vittima. Questo, associato a phishing tradizionale, permette di impossessarsi completamente dell'account della vittima (account takeover) attraverso gli SMS usati come one time password (OTP) nel processo di autenticazione o autorizzazione.

Il SIM swap è una delle tecniche più utilizzate dagli attaccanti nei confronti di vittime che si avvalgono della possibilità di ricevere i codici via telefono. [1]
Il fenomeno è cresciuto in tutta Europa, sfruttando di volta in volta le carenze procedurali o tecniche della emissione del duplicato di una SIM oppure nella portabilità del numero di telefono da un operatore all'altro, cosa che genera l'emissione di una nuova SIM.
Le app bancarie, a seconda dell'implementazione, hanno meccanismi alternativi di autorizzazione delle operazioni, che vanno dalle *push notifications*, codici di conferma mostrati a schermo attraverso l'app stessa, all'autorizzazione con l'impronta digitale, e che contribuiscono in maniera robusta all'autenticazione del reale intestatario del conto, essendo più difficili da catturare rispetto agli SMS. È quindi buona pratica installare e usare le app bancarie, allontanandosi velocemente dagli SMS, tuttavia questo non ci mette al riparo dagli attacchi SIM swap in quanto gli attaccanti possono usare la nuova SIM per installare su un loro smartphone l'app della banca usando tutte le nostre credenziali.

È da capire il ruolo che hanno avuto in questo contesto le campagne di phishing verso l'applicazione dealerfree di Telecom Italia della prima parte dell'anno. Altresì da stimare l'impatto che avrà nei prossimi mesi il databreach ad ho Mobile di dicembre 2020 [14].
Gli operatori di telefonia mobile e i loro rivenditori sono diventati, in alcuni casi, una vulnerabilità per i sistemi di autenticazione che si basano sul numero telefonico. Promettenti sono gli esperimenti portati avanti da alcuni operatori che segnalano all'intestatario l'emissione di una nuova SIM e gli danno un tempo sufficiente per bloccare l'operazione.
Completamente nuovi sono invece gli attacchi basati sull'emulazione degli smartphone [15]. Gli emulatori imitano le caratteristiche dei dispositivi mobili e vengono solitamente usati dagli sviluppatori per testare le applicazioni e le funzionalità su un'ampia gamma di tipi di dispositivi con caratteristiche diverse, senza la necessità di acquistarli.
Questi attacchi, non teorici ma già realmente osservati sul campo, emulano i dispositivi dell'utente (device spoofing) a cui ci si vuole sostituire, caricando dati esfiltrati da campagne di malware o phishing, come le caratteristiche del dispositivo, marca, modello, versione del sistema operativo, caratteristiche dello schermo, lingua, IMEI, posizione GPS e altro ancora. Cioè tutti elementi usati per il device fingerprinting. Infine, al dispositivo viene associato al nome utente e alla password della vittima per poi tentare un attacco al suo

account, che oltre le credenziali dell'utente simuli anche il suo dispositivo. Trattandosi di un'emulazione software, è possibile replicare questa operazione a volontà e in un gran numero di istanze, lanciando attacchi automatizzati in contemporanea.

Conclusioni

L'anno appena trascorso ha dimostrato ancora una volta che gli attacchi informatici sono dominati da gruppi criminali tecnicamente competenti, ben organizzati, pronti a reagire rapidamente alle contromisure di volta in volta adottate. La protezione e la risposta agli attacchi deve necessariamente adottare lo stesso approccio di competenza tecnica, strumenti, organizzazione e rapidità.
Nel caso specifico delle frodi finanziarie, punto di partenza imprescindibile è una corretta informazione al cliente e formazione del personale dipendente. Bisogna comunque mettere in conto che prima o poi un evento avverso accada realmente, a causa della crescente complessità degli schemi di attacco
Il cliente che opera attraverso il canale Internet deve essere indirizzato verso soluzioni di protezione endpoint avanzate, capaci di individuare e bloccare il malware finanziario, proteggere il browser, e impedirgli di accedere ai siti di phishing.
Visto dal lato della organizzazione che eroga il servizio, ad esempio la banca, questa deve stabilire in modo rapido e trasparente la veridicità dell'identità digitale dell'utente che si presenta al sito web, e continuare a verificarla durante tutta la transazione, classificando il livello di rischio di ciascun utente, connessione, operazione, e applicando quando necessario controlli di autenticazione più rigidi.

La tecnologia disponibile consente già di analizzare molti fattori. Analisi comportamentale dell'utente, identificazione del dispositivo, associazione, autenticità, igiene, configurazione, aggiornamento del sistema operativo e delle applicazioni, posizione, SIM, numero di telefono e informazioni sulla posta elettronica, identità utente sia per quanto riguarda le identità conosciute che quelle nuove, attributi di sessione e di rete. Questi dati possono essere combinati con l'ausilio dell'intelligenza artificiale, la threat intelligence e lo scambio di informazione con altri servizi di prevenzione dai cyber attacchi.
Gli elementi da controllare sono indubbiamente tanti, ma questo contribuisce a costruire una valutazione del rischio altamente affidabile della singola operazione, e individuare prontamente le operazioni a più alto rischio.

Più in generale, le organizzazioni sono nel mezzo di un cammino di modernizzazione degli ambienti e dei processi attraverso il cloud computing. In questo percorso, ciascuna azienda o amministrazione è in una fase diversa e intraprende scelte individuali sulla base della propria organizzazione interna, della strategia aziendale e delle normative di settore. Tutte però hanno l'esigenza di abbracciare il cloud computing in maniera sicura.
In questo momento il cloud è necessariamente ibrido, e collega sistemi, processi, dati e applicazioni dei propri datacenter, con le offerte di cloud pubblico dei numerosi provider

presenti sul mercato. Il cloud ibrido è il paradigma che più di ogni altro lascia all'organizzazione libertà di scelta.
Unico è anche l'approccio alla sicurezza di ciascuna organizzazione. Questo passa attraverso l'allineamento della strategia di sicurezza al proprio business, la definizione e l'applicazione di controlli di sicurezza volti a garantire l'accesso sicuro alle informazioni e alle risorse aziendali, e infine la protezione dalle minacce e la gestione di eventuali attacchi che dovessero manifestarsi.
Nell'analisi dei dati dell'anno trascorso osserviamo come le minacce abbiano una declinazione in base alla particolare *industry* e all'area geografica in cui si opera, in quanto i gruppi cyber criminali prendono quasi sempre di mira obiettivi omogenei. La valutazione del rischio non può ignorare questo aspetto.
Relativamente al contesto del financial cybercrime italiano, l'89% delle campagne di distribuzione malware bancario analizzata è rimasta attiva meno di 48h (**Figura 8**). Più in generale, lo sviluppo delle campagne di attacco recenti è molto rapido e per bloccare minacce e attacchi occorre agire con simile rapidità.

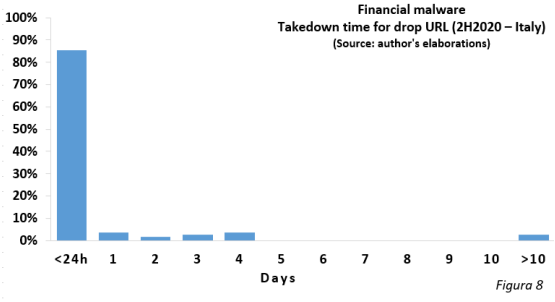


Figura 8

Una soluzione di sicurezza deve essere in grado di ricevere ed elaborare tempestivamente gli indicatori di compromissione (IOC - Indicator of Compromise) rilevanti per la specifica industry e area geografica in cui opera l'organizzazione, confrontarli con l'ambiente realmente installato per capire se, come e dove l'organizzazione è a rischio oppure è stata già colpita. Questa deve essere in grado di reagire entro le poche ore in cui tutto il fenomeno si realizza. Agire in ritardo significherà il successo dell'attacco.
Data la quantità di minacce a cui tutte le organizzazioni sono continuamente esposte nell'arco delle 24 ore, 7 giorni alla settimana, l'investigazione e la gestione di un eventuale incidente non può che avvenire combinando attività automatiche e manuali, e orchestrando azioni correttive automatizzate.
In ultimo, durante la gestione dell'incidente deve essere possibile coinvolgere tutte le figure necessarie, dando loro gli strumenti per interagire velocemente secondo le best practice di mercato e nel rispetto delle normative di settore, ma demandando il controllo e la gestione di minacce e attacchi ad una soluzione tecnologicamente avanzata, lasciando l'organizzazione in grado di operare sul suo core business, senza alcuna interruzione.

Bibliografia

[1] *Sicurezza e frodi informatiche in banca – Come prevenire e contrastare attacchi informatici e frodi su Internet e Mobile Banking* CERTFin ABI Lab, luglio 2020
[2] *Riepilogo delle campagne malevole che hanno interessato l'Italia nell'ultimo quadrimestre 2020* Cert-AgID, dicembre 2020
[3] *ENISA Threat Landscape - List of top 15 threats* ENISA European Union Agency for Cybersecurity, April 2020
[4] *Internet Organised Crime Threat Assessment 2020* Europol, October 2020
[5] C. Cimpanu *Microsoft and others orchestrate takedown of TrickBot botnet* ZDNet, October 2020
[6] *Directive (EU) 2015/2366 of the European Parliament and of the Council* Official Journal of the European Union, November 2015
[7] *Monitoraggio sul corretto utilizzo del protocollo HTTPS e dei livelli di aggiornamento delle versioni dei CMS nei portali Istituzionali della PA* Cert-AgID, dicembre 2020
[8] Pier Luigi Rotondo *Elementi sul cybercrime nel settore finanziario in Europa* Rapporto CLUSIT 2020 sulla sicurezza ICT in Italia, ottobre 2020
[9] *Emotet Botnet Activity Monitoring – public collection* IBM X-Force Exchange, 2020
[10] *Emotet Botnet Disrupted in International Cyber Operation* The United States Department of Justice, 28 January 2021
[11] *World's most dangerous malware EMOTET disrupted through global action* Eurojust – Europol, 27 January 2021
[12] A. Pilkey *Phishing is here to stay* F-Secure, December 2020
[13] *Contrasto alla criminalità finanziaria - Attività della Polizia Postale contro le frodi "Alias"* Commissariato di P.S. online, novembre 2020
[14] *ho. Mobile denuncia attività illecita di ignoti su dati di una parte della propria base clienti* https://www.ho-mobile.it/comunicazione0401/ ho. Mobile, dicembre 2020
[15] S. Gritzman, L. Kessem *IBM Trusteer Exposes Massive Fraud Operation Facilitated by Evil Mobile Emulator Farms* SecurityIntelligence, December 2020
[16] V. Drury, U. Meyer *Certified Phishing: Taking a Look at Public Key Certificates of Phishing Websites* USENIX, Proceedings of the Fifteenth Symposium on Usable Privacy and Security, august 2019
[17] *NCA in international takedown of notorious malware Emotet* United Kingdom National Crime Agency, January 2021
[18] *ENISA Threat Landscape – Phishing* ENISA European Union Agency for Cybersecurity, April 2020
[19] Pier Luigi Rotondo *Shopping e saldi invernali più sicuri con i pagamenti elettronici* IBM thinkMagazine, dicembre 2019
[20] Pier Luigi Rotondo *IBM X-Force: un passo avanti nella difesa dagli attacchi finanziari più evoluti* IBM thinkMagazine, febbraio 2018
[21] Pier Luigi Rotondo *Multifactor Authentication Delivers the Convenience and Security Online Shoppers Demand* SecurityIntelligence, January 2019
[22] Pier Luigi Rotondo *How Will Strong Customer Authentication Impact the Security of Electronic Payments?* SecurityIntelligence, September 2019
[23] Pier Luigi Rotondo *Come proteggersi dagli attacchi Business Email Compromise* INTESA, maggio 2019
[24] *Trickbot's Updated Password-Grabbing Module Targets More Apps and Services* TrendMicro, December 2019

[25] L. Abrams *TrickBot Now Steals Windows Active Directory Credentials* BleepingComputer, January 2020
[26] O. Harpaz *TrickBot's Cryptocurrency Hunger: Tricking the Bitcoin Out of Wallets* SecurityIntelligence, February 2018
[27] O. Ozer *The Curious Case of a Fileless TrickBot Infection* SecurityIntelligence, August 2019
[28] Pier Luigi Rotondo *Sai cosa sono gli attacchi BEC?* IBM thinkMagazine, giugno 2019
[29] Pier Luigi Rotondo *Multifactor Authentication Delivers the Convenience and Security Online Shoppers Demand* SecurityIntelligence, January 2019
[30] Pier Luigi Rotondo *How Will Strong Customer Authentication Impact the Security of Electronic Payments?* SecurityIntelligence, September 2019
[31] Pier Luigi Rotondo *Come proteggersi dagli attacchi Business Email Compromise* INTESA, maggio 2019
[32] Pier Luigi Rotondo *Acquisti online? Ecco come farli in modo sempre più sicuro* IBM thinkMagazine, dicembre 2018
[33] Pier Luigi Rotondo *Proteggere le risorse informative con la sicurezza cognitiva e con soluzioni in grado di adattarsi alle minacce future* ICT Security Magazine n.140/2016, October 2016
[34] M. Schieppati *I 5 tech-trend del 2020 in banca* Bancaforte, gennaio 2020

La gestione strutturata della raccolta dei dati nelle attività di Cyber Threat Intelligence

[A cura di Marco Pericò, Stefano Russo e Pasquale Digregorio - CERT Banca d'Italia][1]

Introduzione

L'organizzazione di attività di Cyber Threat Intelligence (CTI) efficaci non dovrebbe prescindere dall'individuazione preventiva delle principali esigenze informative dei propri stakeholder (Priority Intelligence Requirements - PIR) e dalla chiara conoscenza delle proprie capacità di acquisizione informativa. In base all'analisi sinottica di questi due elementi è possibile sviluppare un piano di raccolta (Collection Plan) che consenta di identificare le modalità con cui orientare le attività di Cyber Threat Intelligence per rispondere in maniera efficace ai PIR. Data la rapidità evolutiva della minaccia cyber e della trasformazione tecnologica del perimetro digitale interno all'organizzazione da proteggere è utile adottare un framework che consenta la gestione strutturata delle attività di raccolta dei dati (Collection Management Framework - CMF). Anche se i CMF possono coprire tutte le tipologie di dati e informazioni previste dal piano di raccolta, la trattazione seguente si concentra prioritariamente sulla CTI di livello tattico-operativo.

Collection Management Frameworks

Un CMF consente di efficientare l'attività di raccolta dei dati, migliorando al contempo la conoscenza dell'ambiente in cui si opera. Ogni organizzazione può sviluppare il proprio CMF cercando di rispondere alle tre domande seguenti:

- quali dati posso raccogliere e da dove?
- per quanto tempo i dati raccolti vengono archiviati?
- quali gap informativi posso colmare sfruttando i dati a disposizione?

La realizzazione di un CMF non avviene attraverso un processo statico, bensì mediante un processo iterativo, volto al miglioramento continuo. Dopo aver definito chiaramente i PIR, in modo che soddisfino i criteri SMART (Specific, Measurable, Achievable, Relevant e Time-related)[2], è possibile procedere seguendo le fasi del ciclo di Deming, detto anche ciclo PDSA dal nome dei suoi quattro stadi "Plan - Do - Study - Act".
La **Figura 1** rappresenta le fasi fondamentali di un CMF che scandiscono l'evoluzione del Collection Plan.

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

[2] Ogni requisito dovrebbe rispondere a una sola domanda, avere un focus puntuale su fatti, eventi, attività e supportare una singola decisione dello stakeholder.

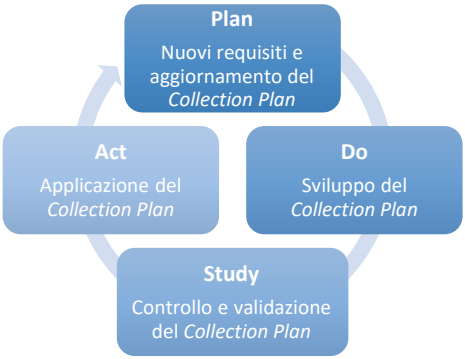


Figura 1 - *Ciclo di Deming applicato allo sviluppo del CMF*

Plan - Nuovi requisiti e aggiornamento del Collection Plan

In questa prima fase si procede alla trasformazione dei PIR in requisiti informativi da far convergere nel Collection Plan e all'identificazione di nuove capacità necessarie per l'acquisizione informativa, in base ad una gap analysis delle sorgenti informative disponibili.
A tal fine è utile profilare in via preliminare le minacce cyber in relazione agli asset dell'organizzazione da proteggere, al settore industriale di appartenenza e agli altri settori interdipendenti. Focalizzarsi sui tradecraft[3] e sulle TTP (tattiche, tecniche e procedure) utilizzate dall'avversario nelle varie fasi della Cyber Kill Chain, permette di acquisire consapevolezza su cosa possa essere utile alle attività di threat intelligence in modo continuativo e a prescindere dalle attivazioni contingenti. A questo scopo, sia la partecipazione a Table Top Exercise (TTX) sia le attività di active defense, quali ad esempio malware analysis, threat hunting, incident response e network security monitoring, contribuiscono all'individuazione del livello di maturità delle proprie capacità di collection e a chiarire quindi i potenziali margini di miglioramento.

Do - Sviluppo del Collection Plan

Chiarite le esigenze informative, coerenti con i PIR in formato SMART, è possibile definire il Collection Plan identificando le sorgenti di dati che possano rispondere operativamente alle esigenze informative di livello tecnico. Durante la fase di implementazione si procede alla creazione di nuove procedure di raccolta e all'identificazione di nuove fonti di dati potenzialmente sfruttabili per le attività di CTI. Per fare ciò è opportuno prendere in considerazione sia le sorgenti interne (SIEM, Log server, etc.) che quelle esterne (archivi di malware, database dei registrar e registrant di domini, threat intel feed, etc).

[3] Combinazione di metodi, capacità e risorse che l'avversario sfrutta nel compimento delle proprie azioni (modus operandi).

Di seguito si riporta una semplice rappresentazione di quanto illustrato, con riferimento a sorgenti informative interne ed esterne. La **Tabella 1** raffigura una possibile struttura da utilizzare per qualificare i dati acquisibili da diversi sistemi interni in base alla tipologia dei dati, alle fasi della kill chain a cui potrebbero riferirsi, alla loro collocazione fisica e al loro periodo di retention; nell'ultima riga vengono invece elencate le ulteriori opportunità di acquisizione di dati aggiuntivi già individuabili in questa fase.

	Endpoint Protection System	**Windows System**	**Linux System**	**Network**	**Firewall**	**Mail Server**
Tipo del Dato	System Alert	Windows Event Logs	Syslog	NetFlow	System Alert	Metadata
Fasi della Kill Chain	Exploitation Installation	Exploitation Installation Actions on Objectives	Exploitation Installation Actions on Objectives	Reconnaissance Delivery C2	Reconnaissance Delivery C2	Delivery Action on Objectives
Posizione del Dato	Local SIEM	Local Registry Keys SIEM	Local SIEM	SIEM	SIEM	Local SIEM
Tempo di retention	60 days	30 days	30 days	60 days	60 days	60 days
Altre opportunità di acquisizione	Malware Sample	Files and timelines	Files and timelines	Packet Capture	NetFlow	Files Event log

Tabella 1 - *CMF: un esempio di Internal Collection*

La **Tabella 2** illustra un modello utilizzabile per validare in modo strutturato le tipologie di dati acquisibili da diversi strumenti o servizi impiegati per l'analisi dei domini malevoli, connessi ad esempio a campagne di phishing o malspam.

Sorgente	Creation date	Expiration date	IPs	ASN	Domains	Historical WHOIS	Currrent WHOIS	Historic Screenshot	Current Screenshot	PDNS	TLS
ALPHA	X	X	X		X		X			X	
BRAVO	X	X	X	X	X	X	X	X	X	X	X
CHARLIE	X	X	X				X			X	
DELTA			X	X	X						

Tabella 2 - *CMF: un esempio di External Collection*

Una ulteriore tipologia di sorgente informativa esterna può essere rappresentata da quanto acquisito attraverso attività di Information Sharing, ovvero dallo scambio informativo volontario con controparti qualificate. La **Tabella 3** mostra un possibile modello per la raccolta di informazioni che schematizza i flussi autorizzati per l'Information Sharing o per lo scambio di Request for Information (RFI) con le proprie controparti fidate e le relative modalità di trasmissione delle informazioni.

Controparti	Tipologia	PoC	Email	Cifratura	A2A	TLP
ALPHA	COMMER-CIALI	NameA SurnameA	nameA.surnameA@domain.aa	N/A	TAXII/STIX FEED	GREEN AMBER
BRAVO	COMMUNITY	NameB SurnameB	nameB.surnameB@domain.aa	SMIME/ PGP	MISP	GREEN AMBER
CHARLIE	GOVERNA-TIVE	NameC SurnameC	nameC.surnameC@domain.aa	PGP	TAXII/STIX FEED	AMBER RED
DELTA	PEER	NameZ SurnameZ	nameD.surnameD@domain.aa	PGP	TAXII/STIX FEED	AMBER

Tabella 3 - *CMF: un esempio di Infosharing & RFI Collection*

Study - Controllo e validazione del Collection Plan

Definire un nuovo processo o aggiungere nuovi data source non implica necessariamente un miglioramento rispetto alla condizione di partenza. Occorre dunque controllare e valutare i vantaggi tratti dall'introduzione di nuove modalità operative, confrontando i risultati ottenuti con le previsioni attese e valutando attentamente il ritorno d'investimento. L'attività di

controllo può avvenire attraverso l'uso di apposite metriche utili non solo a qualificare l'efficienza del Collection Plan implementato, ma anche a comprendere al meglio l'evoluzione delle minacce. Il Computer Incident Response Team della Lockheed Martin Corporation (LM CIRT) suggerisce per questi scopi l'uso di metriche quali l'Analytical Completeness o la Mitigation Scorecard. L'utilizzo dell'Analytical Completeness può aiutare l'analista ad identificare la completezza del proprio Collection Plan in termini di copertura informativa applicata alle fasi della Cyber Kill Chain (CKC) e del Diamond Model (DM).
In **Figura 2** se ne propone un esempio: i valori numerici posizionati su ogni vertice del diamante (a partire dall'alto, in senso orario: Adversary, Capability/TTP, Victim, Infrastructure) si riferiscono alla quantità di intrusioni per le quali sono state raccolte informazioni. Attraverso l'utilizzo di una heatmap è possibile evidenziare per ciascuna fase della kill chain, quali delle quattro caratteristiche della minaccia mappate sul Diamond Model risentano di difficoltà nell'acquisizione o nella rappresentazione dei relativi dati. Il maggior livello di criticità è rappresentato dal rosso, mentre il verde rappresenta una condizione ottimale.

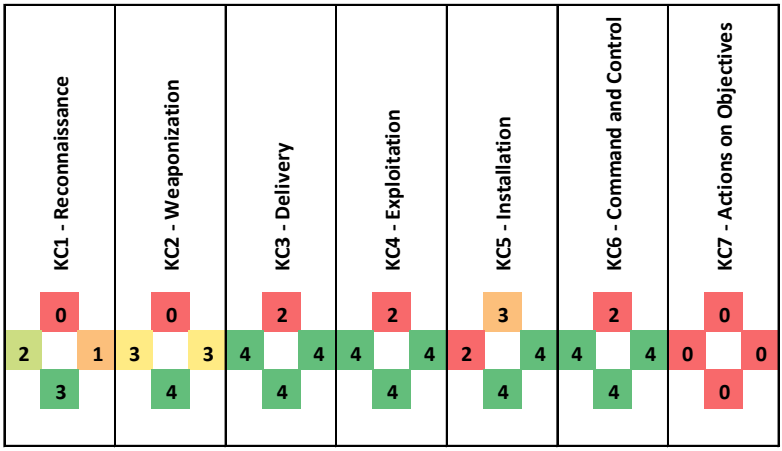


Figura 2 - *Analytical Completeness*

La Mitigation Scorecard permette invece la rappresentazione grafica, per ciascuna fase della kill chain, dell'efficacia dei Courses of Action[4] (CoA) utilizzabili per contrastare un threat actor, una generica intrusione o una campagna. La **Figura 3** rappresenta un esempio pratico dell'applicazione di questa tecnica nei confronti di diverse campagne cyber concorrenti. Le righe rosso chiaro sono relative alle capacità associabili alle CoA passive (Discover,

[4] La locuzione Course of Action (COA) identifica, nella dottrina militare, 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.

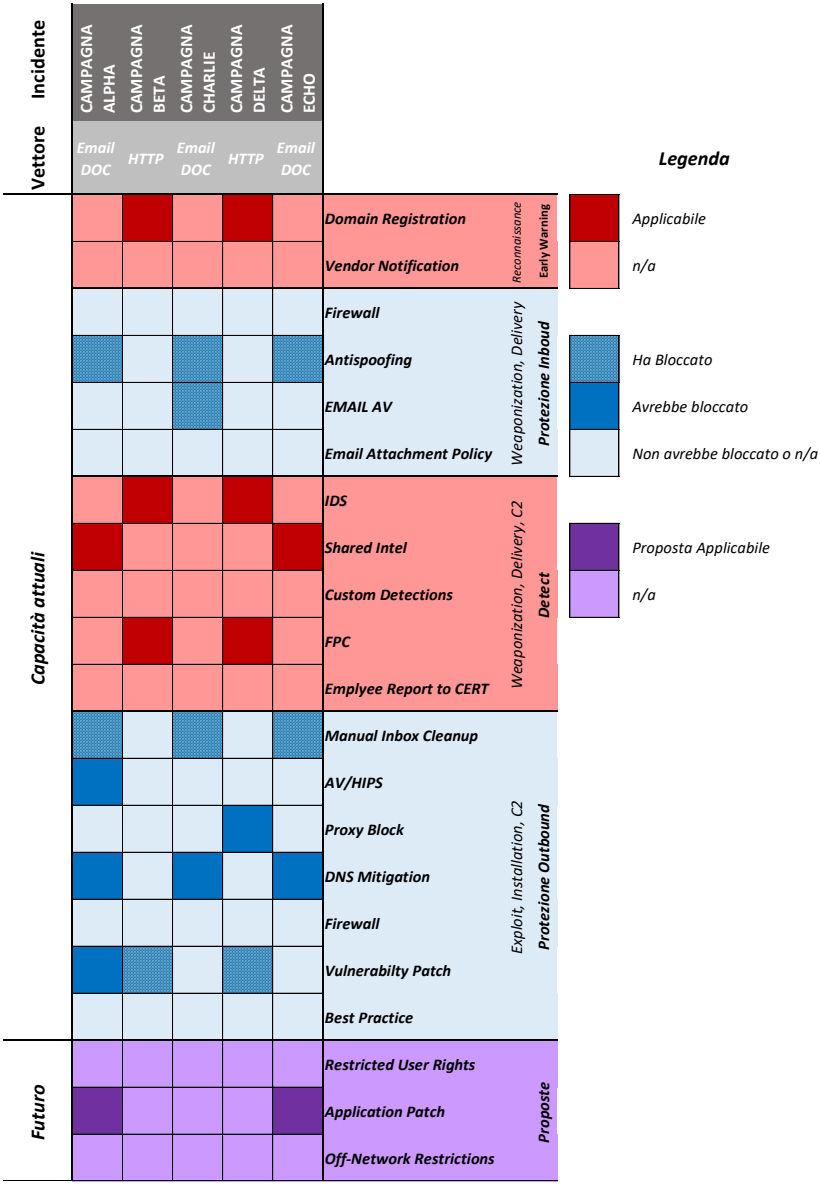


Figura 3 - *Mitigation scorecard*

Detect), il rosso scuro indica le tecnologie applicate all'incidente indicato nella colonna. Il primo gruppo di righe rosso chiaro rappresenta l'Early Warning e la fase Reconnaissance della kill chain, mentre il secondo gruppo di righe rosso chiaro rappresenta la Detection e le fasi Weaponization e Delivery della kill chain. Le righe celesti contengono le capacità mitiganti o strettamente connesse a decisioni di tipo architetturali, sono organizzate in Protezione Inbound e Outbound e si applicano rispettivamente a Weaponization e Delivery nel primo caso e ad Exploit, Installation e C2 nel secondo. Le celle blu rappresentano le capacità che avrebbero mitigato l'attività malevola se non fosse stata mitigata da altro. Le celle blu a strisce rappresentano la capacità che ha realmente mitigato l'intrusione. Le righe viola rappresentano proposte in termini di acquisizione di nuove tecnologie, di iniziative aziendali e di variazioni procedurali. Le celle in viola scuro ne indicano l'applicabilità all'intrusione.

Act - Applicazione del Collection Plan

In questa fase è necessario decidere se adottare, adattare o abbandonare quanto realizzato. Se l'obiettivo conseguito è soddisfacente si procedere alla validazione del Collection Plan e al suo utilizzo per la raccolta informativa funzionale alle attività di CTI. Il passo successivo prevede di ritornare alla fase del Plan per valutare iterativamente se il Collection Plan utilizzato ha permesso una raccolta di dati efficace rispetto ai PIR indentificati in origine; in questa fase si possono anche determinare possibili ulteriori miglioramenti, alla luce di potenziali cambiamenti avvenuti sia sul fronte interno, per variazione dei requisiti o per l'attuazione di aggiornamenti tecnologici, sia sul fronte esterno, in base all'evoluzione dello scenario della minaccia.

Integrazione del CMF con altri framework

L'utilizzo combinato di un CMF con altri framework impiegati nelle attività di Cyber Threat Intelligence permette di rendere più efficace la rilevazione di carenze nelle proprie capacità di acquisizione informativa rispetto alle esigenze discendenti dai PIR, soprattutto per quanto riguarda gli indicatori di attacco[5] più difficili da qualificare e acquisire. Infatti, gli indicatori non sono tutti uguali, in **Figura 4** è riportata una rappresentazione grafica sulla scorta della nota Pyramid of Pain di David Blanco: quelli più in basso (IP o hash) sono facilmente modificabili dagli attaccanti, ma anche di facile individuazione da parte dei difensori; quelli più in alto (TTP, tattiche tecniche e procedure) sono difficilmente mutevoli, ma anche molto più complessi da rilevare. In altre parole, il grado di persistenza di un indicatore determina la sua utilità per qualificare la minaccia che lo ha generato, di contro però gli indicatori più rilevanti per le attività di difesa sono anche i più difficili da individuare.

[5] Nella sua accezione generica, con il termine "indicatore" si intende un dato contestualizzato che descrive un aspetto di un'intrusione. Gli indicatori di compromissione (IoC) si riferiscono solitamente alle "tracce digitali" raccolte dopo una intrusione cyber ai danni una organizzazione e sono funzionali alla rilevazione delle stesse azioni condotte con le medesime modalità contro un nuovo obiettivo. Gli indicatori di attacco (IoA) sono invece funzionali all'individuazione di un potenziale attacco anche prima che ci sia contatto diretto tra attaccante e attaccato.

Per questo motivo sono stati ideati dei framework che si concentrano proprio su questi indicatori più complessi e difficilmente gestibili: ATT&CK e DeTT&CT. Il primo rappresenta una knowledge base delle varie TTP osservate in numerosi attacchi cyber, mentre il secondo permette di associare i propri data source alle TTP dei threat actor di interesse. L'integrazione di questi due modelli con il CMF permette di migliorare l'efficienza delle attività svolte in ciascuna delle sue fasi. Ad esempio, se il CMF precedentemente illustrato può rispondere alla domanda "Quali dati ho a disposizione e dove posso trovarli?", l'integrazione dei suddetti framework permette di rispondere alla più complessa domanda "Quali TTP riesco ad individuare con i data source a disposizione?".

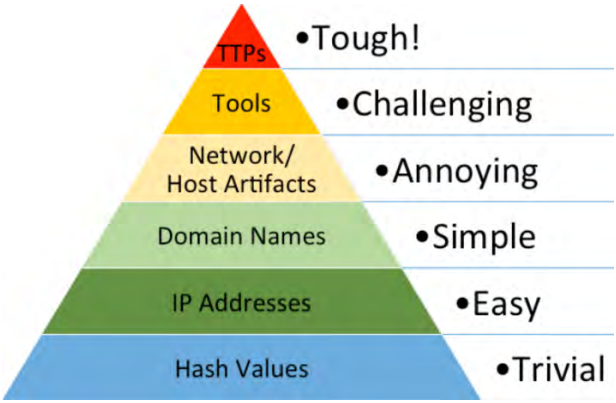


Figura 4 - *Pyramid of Pain (David J. Blanco, 2013)*

ATT&CK

Il framework ATT&CK (Adversarial Tactics, Techniques, And Common Knowledge), sviluppato da MITRE, è uno strumento che raccoglie in modo schematico ciò che un avversario solitamente sfrutta per raggiungere il proprio obiettivo (tactic), i modi in cui può farlo (technique) e i passi utilizzati per mettere in pratica l'attacco congeniato (procedure).
Il framework contiene molti dettagli per ciascuna delle 178 tecniche e delle 352 sottotecniche, fornendo descrizioni, esempi, riferimenti e consigli per la loro mitigazione e per il loro rilevamento. L'utilizzo di ATT&CK Enterprise e PRE-ATT&CK consente all'analista di coprire tutte le fasi della kill chain: PRE-ATT&CK si concentra prevalentemente su tattiche e tecniche utilizzate in fase di Reconnaissance e Weaponization, mentre ATT&CK Enterprise si concentra sulle rimanenti fasi di attacco.
ATT&CK non è un compendio teorico, bensì una knowledge base costruita utilizzando report di attacchi realmente avvenuti; tuttavia non è privo di bias, come lo stesso John Wunder, Principal Cybersecurity Engineer e Group Lead al MITRE, ha dichiarato nel suo articolo "Building an ATT&CK Sightings Ecosystem". Le tecniche possono essere infatti

realizzate in modi differenti e pertanto il blocco o il rilevamento di un'unica modalità di realizzazione non ne indica necessariamente una totale neutralizzazione.
ATT&CK fornisce anche informazioni sui possibili data source utilizzabili per rilevare la specifica minaccia, sui threat actor (gruppi), sui software da questi utilizzati per implementare una tecnica, sulla tattica attuata e sulle relative mitigazioni. Le relazioni tra questi tipi di informazioni sono mostrate nella **Figura 5**. Il framework definisce circa 60 tipi di data source, individuabili fra le proprietà di una tecnica o sottotecnica; l'attuale struttura contiene solo i nomi delle fonti di dati e al momento non vi è un allineamento con le tecnologie di rilevamento e tracciamento.

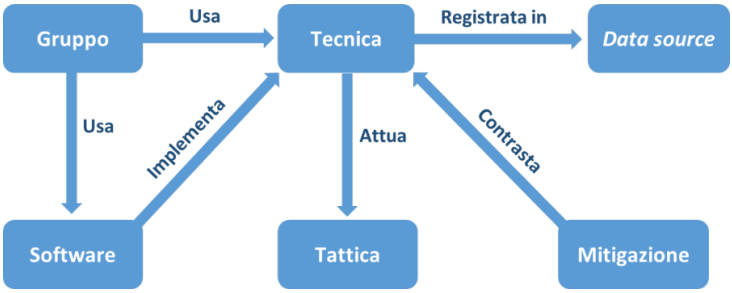


Figura 5 - *Relazioni informazioni in ATT&CK*

DeTT&CT

Il framework DeTT&CT (Detect Tactics, Techniques & Combat Threats), sviluppato da Marcus Bakker e Ruben Bouman, può essere utilizzato per classificare e valutare la qualità delle sorgenti dati (data source quality), il livello di visibilità (visibility coverage) e la capacità di rilevamento (detection coverage) rispetto alle TTP degli attaccanti, oltre a consentire la visualizzazione e il confronto di tali TTP mediante una rappresentazione grafica (threat actor behaviours). In aggiunta ai 60 data source già definiti in ATT&CK, mappati sulle TTP e inclusi nel framework, è possibile definirne di nuovi consentendo una modellazione dettagliata delle sorgenti dati individuate nel CMF. La mappatura dei dati rispetto ad ATT&CK viene realizzata per mezzo di specifici livelli (layer) che possono essere importati nello strumento di visualizzazione ATT&CK Navigator[6].
Il primo passo per la configurazione di DeTT&CT consiste nel definire i data source a disposizione. Per l'adempimento di questa fase sono fondamentali le informazioni riportate nel CMF, le quali vanno poi integrate con dei punteggi su cinque diverse metriche sulla qualità dei dati: device completeness, data field completeness, timeliness, consisten-

[6] https://mitre-attack.github.io/attack-navigator/

cy, retention[7]. Individuate queste informazioni, lo strumento è già utilizzabile per creare un'associazione tra i propri data source e le TTP individuate da ATT&CK, creando un layer che evidenzi quanto ogni determinata tecnica sia individuabile sfruttando le sorgenti dati inserite. In **Figura 6** se ne riporta un estratto.

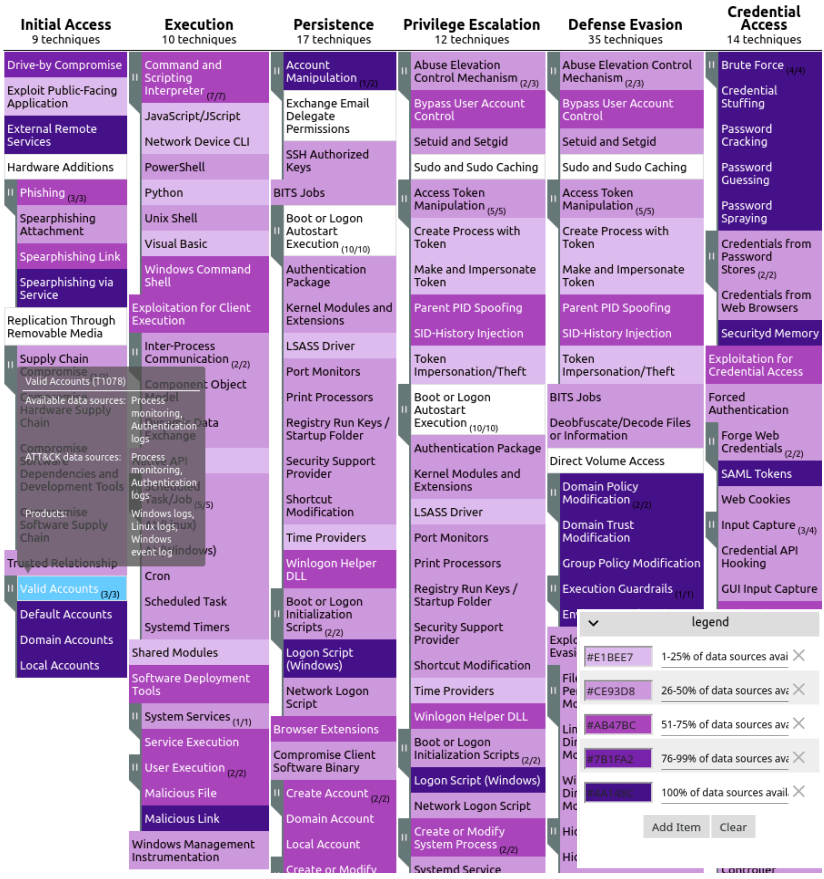


Figura 6 - *DeTT&CT layer "data sources"*

[7] Device completeness: quanti degli asset a disposizione sono coperti dai dati; data field completeness: il livello di completezza dei campi dati; timeliness: l'accuratezza temporale dei dati e la loro disponibilità; consistency: quanto i dati e i relativi campi sono standardizzati; retention: per quanto tempo i dati sono disponibili.

DeTT&CT può essere ulteriormente affinato per calcolare nel dettaglio il livello di visibilità per ogni tecnica. Per questa seconda fase si può creare una configurazione grezza a partire dai dati forniti nella precedente, che andrà successivamente dettagliata manualmente indicando un visibility score in base alla conoscenza specifica delle sorgenti informative. Potrebbe infatti accadere che un data source, seppur presente, possa non essere ritenuto sufficientemente completo per l'identificazione di tutti gli aspetti di una determinata tecnica; oppure, al contrario, che si abbia a disposizione un data source non contemplato in ATT&CK per l'identificazione di specifiche tecniche. Con queste nuove informazioni si può creare un ulteriore layer che mostri, per le varie TTP, l'esatto livello di visibilità, ossia quanti dettagli relativi ad esse è possibile identificare con le sorgenti a disposizione.
Il terzo passo per la configurazione del framework consiste nell'identificare la capacità di rilevamento per ogni tecnica, in maniera duale rispetto alla fase precedente. Il calcolo di questa metrica, il detection score, non può essere svolto automaticamente, poiché è il team di analisti che deve definire le proprie capacità di rilevamento rispetto alle varie tecniche, considerando quanto osservato in campagne precedenti o valutando le funzionalità degli strumenti a propria disposizione. La differenza tra visibility e detection può risultare sottile, ma è un aspetto fondamentale: può ad esempio capitare che si abbia un'elevata visibility (es. molti dati, dettagliati e completi) e una bassa detection (es. gli attacchi vengono riconosciuti solo in base a delle firme statiche, ci possono essere elevati casi di falsi positivi, etc.); al contrario, si potrebbe avere un'elevata detection (es. identificazione automatica basata sulla correlazione di più sorgenti informative, con basso numero di falsi positivi) con una bassa visibility (es. pochi dati, incompleti e che coprono pochi aspetti relativi alla tecnica).
Il layer prodotto dallo strumento con le informazioni riportate in questa fase è simile al precedente, ma esprime stavolta il sopraindicato concetto di capacità di detection per ognuna delle TTP. In aggiunta, è possibile creare un layer per comparare le due metriche visibility e detection, in modo da verificare quali TTP sono coperte da entrambe.
Una volta completata la configurazione per ciò che riguarda sorgenti dati, livello di visibilità e capacità di rilevamento, DeTT&CT mette a disposizione delle funzioni per comparare le informazioni riportate rispetto alle tecniche comunemente usate dai threat actor, secondo quanto definito in ATT&CK. Questi dati vengono ottenuti automaticamente dallo strumento, tuttavia è anche possibile definire dei nuovi gruppi non censiti su ATT&CK oppure indicarne un sottoinsieme di specifico interesse. I layer che il framework consente di creare in questa fase finale sono tre:

1. Comparazione tra gruppi – un layer che mostra una heatmap delle TTP più utilizzate dai threat actor scelti, dove il colore rosso è tanto più scuro quanto la tecnica viene usata da più gruppi;
2. Comparazione tra gruppi e livello di visibilità – un layer che evidenzia quali sono le TTP utilizzate dai threat actor scelti sulle quali si ha un certo livello di visibilità, dove il colore giallo è tanto più scuro quanto il visibility score è elevato, mentre in blu sono invece segnalate le TTP senza corrispondenze con i gruppi scelti (in **Fig.** 7 se ne riporta un estratto);

3. Comparazione tra gruppi e capacità di rilevamento – un layer che evidenzia quali sono le TTP utilizzate dai threat actor scelti per le quali si ha una certa capacità di rilevamento, dove il colore giallo è tanto più scuro quanto il detection score è elevato, mentre in verde sono invece segnalate le TTP senza corrispondenze con i gruppi scelti.

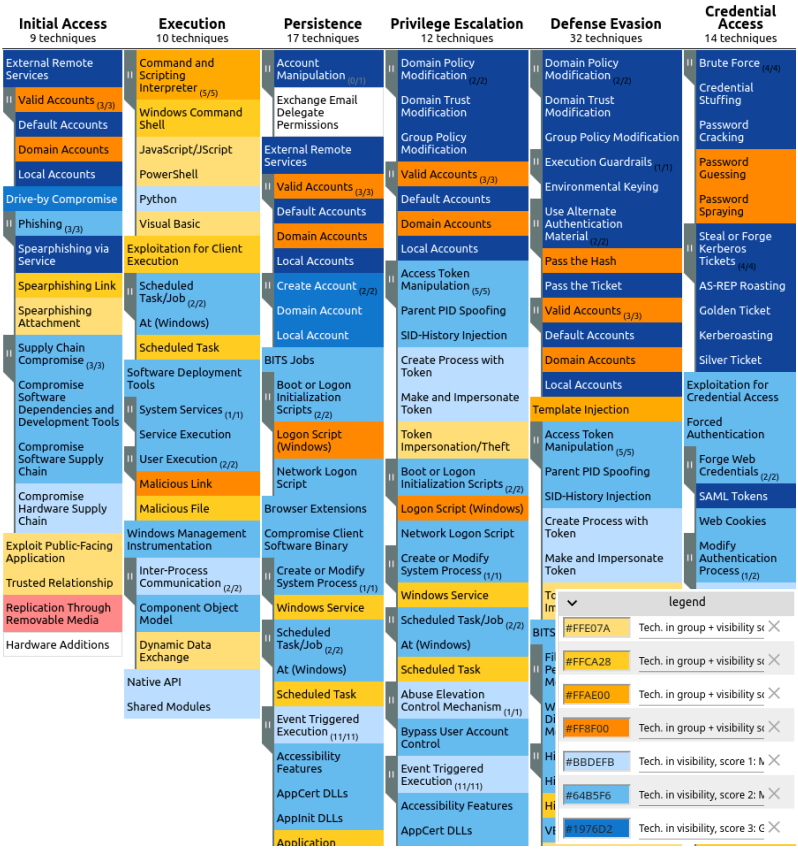


Figura 7 - *DeTT&CT layer "visibility vs APT"*

Gli ultimi tre layer descritti sono particolarmente utili per individuare eventuali lacune informative; tali dati potranno quindi essere sfruttati per verificare l'adeguatezza del CMF, aggiornarlo o, nel caso venissero individuate mancanze strutturali, anche per prioritizzare le attività da sviluppare per il miglioramento delle proprie capacità di difesa a seconda delle modalità di attacco dei threat actor di maggiore interesse.

Conclusioni

Il profilo evolutivo della minaccia cyber vede la costante diffusione di tecniche d'attacco complesse sempre più difficili da rilevare e contrastare. In questo scenario, l'impiego della dottrina intelligence al servizio della cybersecurity rappresenta un fattore abilitante per lo sviluppo delle capacità di threat intelligence, funzionali a incrementare e aggiornare un'adeguata cyber situational awareness. Un approccio strutturato alla gestione della raccolta informativa è un prerequisito importante per il raggiungimento di questo obiettivo. In quest'ottica lo sviluppo e l'applicazione di un CMF integrato con i principali framework di CTI permette di: sviluppare una visione chiara della tipologia di dati ottenibili all'interno o all'esterno della propria organizzazione; contestualizzare adeguatamente i dati raccolti; mettere questi ultimi in relazione con le principali tattiche, tecniche e procedure d'attacco; essere consapevoli delle proprie capacità di rilevare queste ultime e individuare la priorità da dare agli investimenti e alle attività necessarie a colmare le carenze capacitive rilevate.

Riferimenti

- Doran, G. T. (1981), There's a S.M.A.R.T. way to write management's goals and objectives, Management Review, Vol. 70, Issue 11, p35-36, 2p.
- Steffens T. (2020), Attribution of Advanced Persistent Threats – How to Identify the Actors Behind Cyber-Espionage
- Shostack A. (2014), Threat Modeling: Designing for Security
- Joint Publication 2-0, Joint Intelligence Defense Technical Information Center (DTIC)
- https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_0.pdf
- Martin T. Bimford, A Definition of Intelligence – Central Intelligence Agency. Declassified 18 Sept 1995. Retrieved 4 Oct 2014.
- https://www.cia.gov/static/554d7d05a62d7d6de84b5b84ae6702ae/A-Definition-Of-Intelligence.pdf
- Army Doctrine Field Manual 34-2, Collection Management and Synchronization Planning
- https://fas.org/irp/doddir/army/fm34-2/toc.htm
- Lee Robert. M., Miller B. e Stacey M. (2018), Collection Management Frameworks - Looking Beyond Asset Inventories in Preparation for and Response to Cyber Threats
- https://www.dragos.com/wp-content/uploads/CMF_For_ICS.pdf
- Lee Robert M. (2015), Data, Information, and Intelligence: Why Your Threat Feed Is Likely Not Threat Intelligence
- https://www.sans.org/blog/data-information-and-intelligence-why-your-threat-feed-is-likely-not-threat-intelligence/
- Hutchins Eric. M., Cloppert M.J., Amin R.M. (2011), Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains
- https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

- Lockheed-Martin Corporation (2015), Seven Ways to Apply the Cyber Kill Chain with a Threat Intelligence Platform
- https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Seven_Ways_to_Apply_the_Cyber_Kill_Chain_with_a_Threat_Intelligence_Platform.pdf
- Caltagirone S., Pendergast A., Betz C.(2013), The Diamond Model of Intrusion Analysis
- https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf
- Blanco David J. (2013), The Pyramid of Pain
- https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html
- Strom Blake E., Applebaum A., Miller Doug P., Nickels K.C., Pennington A.G., Thomas C.B. (2018), MITRE ATT&CK™: Design and Philosophy
- https://www.mitre.org/sites/default/files/publications/pr-18-0944-11-mitre-attack-design-and-philosophy.pdf
- Bouman R. (2019), MTRE ATT&CK Mapping
- https://github.com/siriussecurity/mitre-attack-mapping
- Bakker M., Bouman R. (2019), Detect Tactics, Techniques & Combat Threats
- https://github.com/rabobank-cdc/DeTTECT
- Bakker M., Bouman R. (2019), DeTT&CT: Mapping your Blue Team to MITRE ATT&CK™
- https://www.mbsecure.nl/blog/2019/5/dettact-mapping-your-blue-team-to-mitre-attack
- Wunder J. (2019), Building an ATT&CK Sightings Ecosystem
- https://medium.com/mitre-attack/building-an-attack-sightings-ecosystem-b43d52cac151
- Rodriguez Jose L. (2020), Defining ATT&CK Data Sources, Part I: Enhancing the Current State
- https://medium.com/mitre-attack/defining-attack-data-sources-part-i-4c39e581454f
- Rodriguez Jose L. (2020), Defining ATT&CK Data Sources, Part II: Enhancing the Current State
- https://medium.com/mitre-attack/defining-attack-data-sources-part-ii-1fc98738ba5b
- Rodriguez R. (2017), How Hot Is Your Hunt Team?
- https://cyberwardog.blogspot.com/2017/07/how-hot-is-your-hunt-team.html
- Rodriguez R. (2017), Ready to hunt? First, Show me your data!
- https://cyberwardog.blogspot.com/2017/12/ready-to-hunt-first-show-me-your-data.html
- Roberts Scott J. (2016), CTI SquadGoals - Setting Requirements
- https://sroberts.medium.com/cti-squadgoals-setting-requirements-41bcb63db918
- Fox David B., Arnoth E.I., Skorupka C.W., McCollum C.D., Bodeau D.J. (2018), Cyber Threat Model for Financial Services Sector Institutions
- https://www.mitre.org/sites/default/files/publications/pr_18-1725-ngci-enhanced-cyber-threat-model-for-financial-services-sector-institutions.pdf

Miglioramento del controllo degli aspetti di sicurezza nella Supply Chain ICT: è una via praticabile?

[A cura di Roberto Obialero]

L'articolo è focalizzato sull'esigenza di definire, e poi verificare, l'adozione di requisiti di sicurezza adeguati attraverso l'intero ciclo di vita dell'acquisizione ed utilizzo di servizi e applicazioni ICT, instaurando allo stesso tempo con il fornitore un rapporto di partnership volto a condividere obiettivi e successi nell'implementazione.

Il contesto, i trend di esternalizzazione e i modelli di outsourcing applicabili

Nel corso degli ultimi venti anni si è assistito al graduale spostamento della responsabilità di esecuzione delle attività concernenti la gestione operativa ICT dalle organizzazioni verso servizi esternalizzati; questo fenomeno è sostanzialmente riconducibile ai seguenti fattori:

- difficoltà nel reperimento sul mercato del lavoro di competenze adeguate, da mantenere sempre aggiornate possibilmente a costi ragionevoli;
- specializzazione e globalizzazione dell'offerta, con player in grado di offrire livelli di servizio adeguati a tutte le esigenze;
- disponibilità di servizi offerti in modalità cloud in grado di offrire una migrazione delle risorse elaborative in tempi rapidi con buone capacità associate ad offerte competitive;
- aspettative degli utenti legate alla fruizione di applicazioni da qualunque luogo ed in qualunque orario;
- scelta delle organizzazioni di concentrarsi sul core business delegando servizi specialistici a partner esterni dedicandosi prevalentemente ad un ruolo di governance.

Il panorama dei servizi ICT erogati per l'organizzazione da una o più terze parti può essere così articolato:

- outsourcing di servizi sistemistici e manutenzione applicativa erogato sia in modalità on premise che da remoto;
- esternalizzazione della fornitura di servizi applicativi generalmente tramite modello di servizio cloud, che può arrivare sino alla delega nella gestione di alcune attività strategiche ed operative quali il servizio Security Operations Center – SOC od il Customer Relationship Management - CRM;
- adozione di software modulare, in cui alcune componenti specifiche tra cui le librerie, possono essere realizzate da terze parti, ad esempio nel caso dei prodotti software open source.

La penetrazione nel mercato ICT delle attività in outsourcing è in costante aumento trainata in particolar modo dalla crescita dei numeri relativi all'offerta di servizi erogati nelle varie accezioni del paradigma cloud.

Riferimenti normativi e best practices di settore

Il riferimento normativo è senza dubbio rappresentato dal Regolamento GDPR in materia di protezione dei dati personali, che definisce tramite l'articolo 28 gli oneri in capo al ruolo del responsabile del trattamento; sono inoltre presenti degli spunti interessanti nella regolamentazione di settore bancaria e assicurativa relativa alla sicurezza e riduzione del rischio informatico.

Estendendo l'ambito alla tutela del patrimonio digitale dell'organizzazione, occorre dare il giusto rilievo alle sezioni relative alla gestione della catena di fornitura definite puntualmente negli standard internazionali della serie ISO/IEC 27001, nel Cyber Security Framework pubblicato dal NIST (National Institute of Standards and Technologies) americano e nella categoria Application Security della collezione Critical Security Controls - CSC dal Center for Internet Security.

Incidenti di sicurezza di pubblico dominio

Nel corso dell'anno 2020 sono stati registrati parecchi incidenti di sicurezza che hanno copinvolto la catena di fornitura; nella tabella seguente sono sintetizzati i casi principali che hanno ottenuto la rilevanza dei media:

Ambito	*Categoria*	*Data*	*Incidente*	*Descrizione*	*URI di approfondimento*
Processo di sviluppo e distribuzione del software	Attacco con compromissione dell'integrità	17/4/20	Caricate librerie dannose nel repository RubyGems	Un gruppo di hacker ha caricato file dannosi nel sistema di gestore pacchetti software RubyGems. Tali file hanno nomi con uno o due caratteri diversi dai file legittimi. Nel caso di download di librerie dannose, il software che verrà compilato includerà del malware funzionale a rubare bitcoin.	https://arstechnica.com/information-technology/2020/04/725-bitcoin-stealing-apps-snuck-into-ruby-repository/ https://threatpost.com/bitcoin-stealers-700-ruby-developer-libraries/154937/
	Attacco con compromissione dell'integrità	28/5/20	Attacco alla catena di fornitura software open source: infettati 26 progetti ospitati da GitHub tramite Il Malware Scanner Octopus	All'inizio di marzo 2020, l'Incident Response Team di GitHub ha appreso che alcuni repository allocati in progetti open source erano stati infettati da malware noto come Octopus Scanner. Il malware è una backdoor creata per infettare i progetti NetBeans. Un rapporto GitHub descrive l'attacco dalle fasi di rilevamento sino alla neutralizzazione.	https://www.cyberscoop.com/github-octopus-malware-supply-chain/ https://cyware.com/news/how-github-untangled-itself-from-an-octopus-malware-that-infected-26-projects-b81edbd3
	Vulnerabilità dei componenti software CMS	28/7/20	Reso disponibile un aggiornamento per risolvere un difetto critico nel plugin WordPress wpDiscuz	Un difetto critico nell'esecuzione di codice in modalità remota nel plug-in di commento wpDiscuz per WordPress potrebbe essere sfruttato da utenti non autenticati per assumere il controllo di siti Web vulnerabili. Gli utenti sono invitati ad aggiornare wpDiscuz alla versione 7.0.5i.	https://www.wordfence.com/blog/2020/07/critical-arbitrary-file-upload-vulnerability-patched-in-wpdiscuz-plugin/ https://portswigger.net/daily-swig/wordpress-plugin-vulnerability-exposes-80-000-sites-to-remote-takeover
	Vulnerabilità dei componenti software CMS	3/8/20	Aggiornamento disponibile per risolvere i difetti del plugin newsletter di WordPress	Sono stati rilevati difetti nel plug-in Newsletter per WordPress che possono essere sfruttati per stabilire backdoor, creare account amministrativi e probabilmente assumere il controllo di siti vulnerabili. Gli sviluppatori del plugin hanno rilasciato una versione aggiornata, Newsletter 6.8.3, che risolve la vulnerabilità.	https://www.wordfence.com/blog/2020/08/newsletter-plugin-vulnerabilities-affect-over-300000-sites/ https://www.bleepingcomputer.com/news/security/newsletter-plugin-bugs-let-hackers-inject-backdoors-on-300k-sites/
	Funzionalità illecite su componenti di terze parti	7/8/20	Più di 80 milioni di installazioni di estensioni dannose di Google Chrome	Sono state trovate disponibili nel Google Chrome Web Store quasi 300 estensioni dannose del browser. Le estensioni includono utility fasulle e programmi ad blocker che inseriscono annunci nei risultati di ricerca o sfruttano cookie stuffing. Google ha rimosso le estensioni dopo la pubblicazione di un post sul blog di AdGuard. Le estensioni in questione sono state scaricate 80 milioni di volte	https://www.theregister.com/2020/08/07/chrome_web_store_slammed/ https://adguard.com/it/blog/fake-ad-blockers-part-3.html
	Sfruttamento di exploit dovuti a componenti software CMS	1/9/20	Possibilità di sfruttare la vulnerabilità del plugin di WordPress File Manager	Gli sviluppatori del plug-in File Manager per WordPress hanno rilasciato una versione aggiornata per risolvere una vulnerabilità che interessa le versioni di File Manager dalla 6.0 alla 6.8. Gli utenti sono stati invitati ad aggiornare il plug-in alla versione 6.9. Il difetto potrebbe essere sfruttato per consentire agli utenti non autenti-	https://arstechnica.com/information-technology/2020/09/hackers-are-exploiting-a-critical-flaw-affecting-350000-wordpress-sites/ https://www.zdnet.com/article/wordpress-file-manager-bug-causing-full-website-takeover-

Ambito	Categoria	Data	Incidente	Descrizione	URI di approfondimento
				cati di eseguire comandi e caricare file dannosi su un sito di destinazione. Il plug-in File Manager può contare più di 700.000 installazioni.	exploited-in-the-wild/
Servizi ICT gestiti	Attacco ransomware	10/1/20	L'aeroporto di Albany, New York è stato colpito da un ransomware diffuso tramite il fornitore di servizi ICT	I server di gestione dell'aeroporto internazionale di Albany (New York) sono stati colpiti da un attacco ransomware nel dicembre 2019. Il malware è stato veicolato tramite la rete dell provider di servizi gestiti (MSP) che ha infettato i server di backup dell'aeroporto. La società di gestione dell'aeroporto ha chiuso la relazione con il fornitore, confermando di aver pagato un riscatto non precisato per riottenere l'accesso ai suoi dati.	https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-hits-new-york-airport-systems/ https://www.itsecurityguru.org/2020/01/13/new-york-airport-systems-attacked-by-sodinokibi-ransomware/
	Attacco ransomware	3/6/20	La banda che opera sul Ransomware DoppelPaymer ha confermato di aver colpito un appaltatore della NASA	Gli operatori del ransomware DoppelPaymer affermano di aver infettato la rete di DMI, un'azienda di servizi IT e di sicurezza informatica gestiti. I clienti DMI includono aziende incluse nell'elenco Fortune 100 e agenzie governative. Pare che gli attaccanti abbiano ottenuto file riservati relativi al cliente NASA attraverso la rete di DMI e ne hanno pubblicati alcuni su un portale dark web.	https://www.zdnet.com/article/ransomware-gang-says-it-breached-one-of-nasas-it-contractors/ https://siliconangle.com/2020/06/03/nasa-contractor-allegedly-hit-dopplepaymer-ransomware-group/
	Attacco ransomware	26/9/20	Tyler Technologies: un attacco ransomware colpisce enti pubblici statali e locali	Una società che fornisce servizi IT ai governi statali e locali degli Stati Uniti ha confermato un incidente informatico qualificato come attacco ransomware. Alcuni clienti di Tyler Technologies hanno segnalato di aver rilevato accessi sospetti. La società sta sollecitando i propri clienti a modificare le proprie password per gli account di accesso remoto.	https://www.reuters.com/article/us-tyler-tech-cyber/tyler-technologies-says-clients-reported-suspicious-logins-after-hack-idUSKBN26H13I https://www.tylertech.com/security-incident
	Attacco ransomware	17/11/20	Managed.com colpita da un attacco Ransomware	Il provider di servizi hosting Managed.com è stato colpito da un attacco ransomware iniziato all'inizio di questa settimana. La società ha disattivato tutti i suoi server per far fronte all'incidente. L'attacco ha colpito i sistemi di hosting pubblico; i siti di alcuni clienti sono stati crittografati.	https://www.zdnet.com/article/web-hosting-provider-managed-shuts-down-after-ransomware-attack/ https://www.bleepingcomputer.com/news/security/revil-ransomware-hits-managedcom-hosting-provider-500k-ransom/
	Data Breach	27/7/20	I dati dei clienti SEI sono stati compromessi in seguito ad un attacco ransomware verso il fornitore	Un attacco ransomware alla rete di M.J. Brunner, un fornitore di servizi applicativi, ha esposto i dati appartenenti ai clienti di uno dei suoi clienti, SEI Investments. Gli attaccanti hanno rubato file contenenti nomi utente, e-mail e altre informazioni personali associate al prodotto software sviluppato e supportato da Brunner per SEI Investments. Il fornitore si è rifiutato di pagare il riscatto richie-	https://www.scmagazine.com/home/security-news/ransomware/sei-investments-customer-data-exposed-in-ransomware-attack-on-vendor/ https://www.bloomberg.com/news/articles/2020-07-27/fund-administrator-to-pimco-and-others-saw-data-breach-at-vendor

Ambito	Categoria	Data	Incidente	Descrizione	URI di approfondimento
				sto e la banda operatrice del malware ha in seguito pubblicato i dati rubati online.	
Catena di fornitura produttiva e servizi generali	Attacco ransomware	2/1/20	Un attacco ransomware ha costretto il distretto scolastico a ritardare la data di inizio delle lezioni	Un attacco ransomware ha costretto le scuole Richmond Community nel Michigan a ritardare la riapertura dopo le vacanze. Il malware, che ha colpito i sistemi IT del distretto il 27 dicembre, sembra essersi diffuso nei sistemi scolastici attraverso una connessione di rete con il fornitore di servizi di assistenza del riscaldamento e della ventilazione (HVAC) del distretto scolastico. L'attacco ha colpito numerosi sistemi delle scuole, inclusi il sistema di riscaldamento, i telefoni e la gli impianti tecnologici nelle aule. Il personale IT ha ripristinato i sistemi dal server di backup. Il distretto avrebbe dovuto riaprire il 2 gennaio 2020, ma la data di inizio delle lezioni è stata posticipata al 6 gennaio.	https://edscoop.com/michigan-richmond-community-schools-k12-district-ransomware/ https://www.scmagazine.com/home/security-news/ransomware/ransomware-forces-richmond-community-schools-to-close/
	Attacco ransomware	3/6/20	Il Ransomware Maze colpisce il subappaltatore militare statunitense Westech	Gli operatori del ransomware Maze hanno colpito Westech, un subappaltatore della difesa statunitense coinvolto nella manutenzione del programma missilistico nucleare statunitense Minuteman III. Sembra che gli hacker abbiano rubato dati sensibili sui missili nucleari dalla rete Westech e abbiano iniziato a diffondere i file online.	https://news.sky.com/story/hackers-steal-secrets-from-us-nuclear-missile-contractor-11999442 https://threatpost.com/nuclear-contractor-maze-ransomware-data-leaked/156289/
	Attacco ransomware	9/11/20	Il produttore di laptop Compal colpito da un attacco ransomware	Compal, una società che produce laptop per Apple, Acer, Dell, HP e altre società, è stata colpita da un attacco ransomware durante il fine settimana. Compal ha rilevato l'incidente domenica 8 novembre. Secondo una dichiarazione dell'azienda, l'incidente ha interessato la rete interna degli uffici ma non la rete di produzione.	https://www.zdnet.com/article/compal-the-second-largest-laptop-manufacturer-in-the-world-hit-by-ransomware/ https://www.bleepingcomputer.com/news/security/laptop-maker-compal-hit-by-ransomware-17-million-demanded/
	Attacco ransomware	7/12/20	Foxconn conferma di aver subito un attacco ransomware	Il produttore di dispositivi elettronici Foxconn ha confermato che la rete di un suo impianto produttivo in Messico è stata colpita da ransomware alla fine di novembre. E' stato registrato anche un furto di informazioni.	https://www.reuters.com/article/us-foxconn-cyber-idUSKBN28I10S https://threatpost.com/foxconn-confirms-cyber-attack/162035/

Il caso probabilmente più eclatante degli ultimi anni: l'attacco a Solarwinds

Quale diretta conseguenza delle indagini condotte da FireEye, primaria compagnia americana fornitrice di soluzioni di sicurezza e servizi di incident response, colpita da un attacco informatico nella settimana precedente[1] è stato reso pubblico Il 13 dicembre 2020 un attacco con impatti potenzialmente devastanti nei confronti di SolarWinds, altra società americana fornitrice della piattaforma di gestione di rete Orion[2] e dei servizi associati.

La situazione che si è determinata è da ritenersi veramente preoccupante in quanto la base installata dei servizi e prodotti SolarWinds è costituita da circa 300.000 clienti di dimensioni molto rilevanti operativi su un perimetro mondiale sia in ambito governativo che privato quali :

- Dipartimenti americani del Tesoro, del Commercio, di Stato, della Sicurezza Nazionale, dell'Energia Nucleare[3];
- Ministeri della Difesa e degli Interni, ospedali gestiti dal Sistema Sanitario Nazionale inglese;
- Aziende del calibro di Microsoft, Intel, Cisco, Mimecast, VMware, Palo Alto, FireEye[4].

Dalle prime indagini sembra che l'offensiva sia stata portata a termine utilizzando tecniche molto sofisticate, quindi probabilmente riconducibili ad azioni adeguatamente finanziate da governi esteri, e si sia avvalsa di vettori di attacco diversi che sono riusciti nell'obiettivo di sostituire sul sito Internet preposto all'aggiornamento dei programmi l'immagine software da scaricare con una versione compromessa contenente una backdoor; secondo le prime analisi è stato possibile risalire al mese di marzo 2020 come data iniziale delle operazioni che hanno portato alla compromissione.
L'aggiornamento reso disponibile è stato configurato in modo da prevedere un tempo di inattività del malware onde evaderne il rilevamento; le indagini hanno poi rivelato che dei circa 30.000 clienti attivi SolarWinds pare che circa 18.000 lo abbiano scaricato.
Sono poi emersi altri particolari che potrebbero avere particolare rilevanza in quanto potenzialmente riconducibili ad un episodio di insider trading[5]: sembra che nelle settimane precedenti l'annuncio dell'attacco due grossi investitori, che detenevano circa il 70% del pacchetto azionario, abbiano venduto una quota importante della loro partecipazione evitando una perdita di valore azionario che, a fronte delle ripercussioni negative dell'incidente, ha fatto registrare una diminuzione di circa il 20%.

---

1 https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

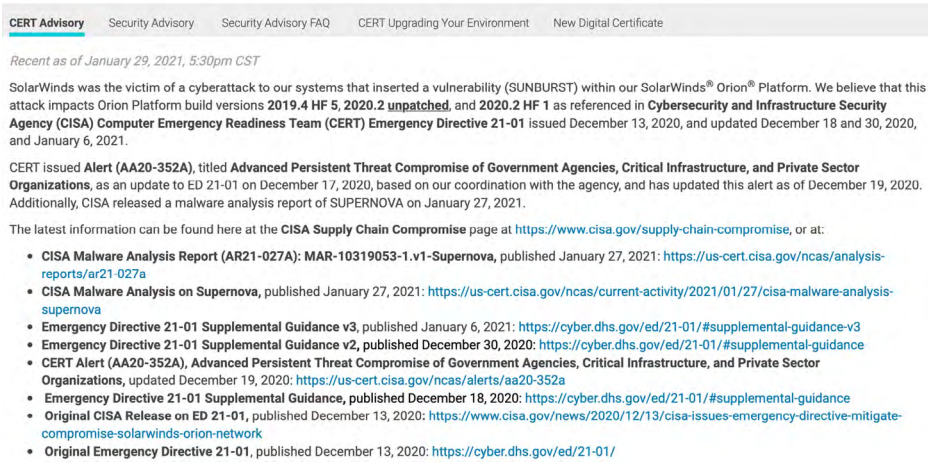
2 https://www.cyberscoop.com/solarwinds-supply-chain-treasury-commerce-espionage/

3 https://krebsonsecurity.com/tag/solarwinds-breach/

4 https://www.bankinfosecurity.com/solarwinds-orion-campaign-victims-include-cisco-intel-a-15619

5 https://www.theregister.com/2020/12/16/solarwinds_stock_sale/

Nella figura seguente, estratta dalla sezione CERT Advisory della compagnia, è riportata l'evoluzione delle notifiche elaborate dai CERT americani volti alla mitigazione dei rischi corsi dai clienti:



CERT Advisory | Security Advisory | Security Advisory FAQ | CERT Upgrading Your Environment | New Digital Certificate

Recent as of January 29, 2021, 5:30pm CST

SolarWinds was the victim of a cyberattack to our systems that inserted a vulnerability (SUNBURST) within our SolarWinds® Orion® Platform. We believe that this attack impacts Orion Platform build versions **2019.4 HF 5, 2020.2 unpatched**, and **2020.2 HF 1** as referenced in **Cybersecurity and Infrastructure Security Agency (CISA) Computer Emergency Readiness Team (CERT) Emergency Directive 21-01** issued December 13, 2020, and updated December 18 and 30, 2020, and January 6, 2021.

CERT issued **Alert (AA20-352A)**, titled **Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations**, as an update to ED 21-01 on December 17, 2020, based on our coordination with the agency, and has updated this alert as of December 19, 2020. Additionally, CISA released a malware analysis report of SUPERNOVA on January 27, 2021.

The latest information can be found here at the **CISA Supply Chain Compromise** page at https://www.cisa.gov/supply-chain-compromise, or at:

- **CISA Malware Analysis Report (AR21-027A): MAR-10319053-1.v1-Supernova,** published January 27, 2021: https://us-cert.cisa.gov/ncas/analysis-reports/ar21-027a
- **CISA Malware Analysis on Supernova,** published January 27, 2021: https://us-cert.cisa.gov/ncas/current-activity/2021/01/27/cisa-malware-analysis-supernova
- **Emergency Directive 21-01 Supplemental Guidance v3**, published January 6, 2021: https://cyber.dhs.gov/ed/21-01/#supplemental-guidance-v3
- **Emergency Directive 21-01 Supplemental Guidance v2, published December 30, 2020:** https://cyber.dhs.gov/ed/21-01/#supplemental-guidance
- **CERT Alert (AA20-352A), Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations,** updated December 19, 2020: https://us-cert.cisa.gov/ncas/alerts/aa20-352a
- **Emergency Directive 21-01 Supplemental Guidance, published December 18, 2020:** https://cyber.dhs.gov/ed/21-01/#supplemental-guidance
- **Original CISA Release on ED 21-01,** published December 13, 2020: https://www.cisa.gov/news/2020/12/13/cisa-issues-emergency-directive-mitigate-compromise-solarwinds-orion-network
- **Original Emergency Directive 21-01**, published December 13, 2020: https://cyber.dhs.gov/ed/21-01/

Analisi di cause e impatti degli incidenti

Le cause degli incidenti sin qui citati si possono pertanto ricondurre alle seguenti considerazioni:

- diversi casi, tra cui quello con gli impatti potenziali maggiori, ripropongono il tema della salvaguardia dell'integrità dei componenti software, cui vengono aggiunti dei componenti malevoli che vengono poi resi inconsapevolmente disponibili ai clienti;
- alcune situazioni sono riferibili alla presenza di componenti software e plugin prodotti da terze parti, non adeguatamente verificati dal punto di vista della sicurezza, che possono introdurre vulnerabilità applicative facilmente sfruttabili;
- diversi fornitori di servizi di gestione delle infrastrutture ICT sono stati oggetto di attacchi ransomware portati a compimento che hanno in seguito contribuito a diffondere l'infezione malevola nelle reti dei clienti fino a generare episodi riconducibili a data breach.

Per quanto concerne gli impatti degli incidenti si possono segnalare:

- necessità di rimuovere il software malevolo, operazione complicata dal fatto che è installato su milioni di istanze;
- bisogno di reinstallare i server partendo dalle copie di backup, conseguenza tipica degli attacchi di natura ransomware;
- esigenza di modificare le credenziali di autenticazione;
- divulgazione di informazioni riservate;
- perdita di reputazione, e conseguente valore azionario, per le società più note.

Approccio per la minimizzazione dei rischi e suggerimenti misure di protezione

Onde evitare le ripercussioni negative di simili episodi si rende necessario affrontare in modo coordinato, insieme agli attori coinvolti nel processo di procurement, il tema della sicurezza sin dalla condivisione delle specifiche di un prodotto o di un servizio; questa prassi aiuterà l'organizzazione a capire se il fornitore sia in grado di garantire una serie di interventi coerenti al principio security by design.
E' opportuno formalizzare i requisiti di sicurezza tramite la condivisione preventiva di checklist, possibilmente sostenibili dal fornitore e mirate in funzione del grado di sicurezza desiderato; nei contratti di fornitura dovranno essere inserite delle clausole dettate dall'organizzazione contenenti istruzioni precise; questo consentirà un'adeguata attribuzione delle responsabilità in caso di accertata negligenza, oppure di carente applicazione delle misure di protezione.

Dev'essere assicurato il diritto di audit in modo da poter verificare preventivamente la sicurezza di un programma software (in modo da assegnare la responsabilità della rimozione di eventuali vulnerabilità al fornitore) oppure la possibilità di verificare tramite test periodici le misure di sicurezza adottate durante le fasi del ciclo di erogazione di un servizio.
E' inoltre di fondamentale importanza accertarsi preventivamente che tali previsioni possano essere estese all'intera catena in caso di subfornitura.
Facendo poi riferimento agli specifici incidenti segnalati si ritiene opportuno suggerire l'introduzione di meccanismi adeguati a protezione dell'integrità del software, quali ad esempio soluzioni HIPS (Hot based Intrusion Prevention System) con associate funzionalità di file integrity monitoring unite a sistemi di monitoraggio accurato degli accessi logici e logging delle attività svolte sui sistemi ad alto grado di criticità.
E' naturalmente fondamentale l'adozione delle best practices in tema di sviluppo sicuro lungo tutto il ciclo di vita di creazione ed utilizzo del software accompagnata ad un processo adeguato di gestione delle vulnerabilità.

Per quanto concerne la mitigazione del rischio legato alle attività di gestione dell'infrastruttura aziendale occorre prima di tutto verificare una adeguata gestione delle identita e dei profili autorizzativi associati, gli accessi strettamente nominali, il logging delle attività svolte dagli operatori che vanno svolte esclusivamente tramite dispositivi "trusted" la cui configurazione di sicurezza (antimalware, aggiornamenti ecc) venga verificata in modo continuo.

Conclusioni e auspici

Il tema della sicurezza della supply chain è stato sinora abbastanza trascurato, probabilmente perché richiede un certo dispendio di energie ed un buon livello di competenza da parte dei soggetti coinvolti che, in caso di mancanza di risorse, sono costretti ad affidarsi alle conoscenze e all'esperienza dei fornitori.

L'adozione degli interventi descritti, una volta verificata una buona cooperazione tra cliente e fornitore, potrebbe trasformarsi in una partnership virtuosa in grado di assicurare reciproche soddisfazioni limitando i rischi associati e migliorando allo stesso tempo il livello di maturità del processo.

La maturità delle organizzazioni in Italia in ambito Supply Chain security

[A cura dell'Osservatorio Cybersecurity & Data Protection della School of Management del Politecnico di Milano]

Nel mondo interconnesso di oggi, le aziende fanno affidamento su una vasta gamma di fornitori di beni e servizi necessari per raggiungere i loro obiettivi aziendali. Da un punto di vista della sicurezza, non è più sufficiente pertanto mitigare i rischi cyber all'interno del proprio perimetro, ma è necessario concentrarsi anche sulla protezione dei sistemi e dei processi delle terze parti: gli attacchi Supply Chain si verificano infatti ogni volta che un malintenzionato riesce a violare i sistemi di un fornitore, di un partner o di un cliente di un'azienda per ottenere a cascata l'accesso ai dati della stessa.

Il numero di questi attacchi, che sfruttano l'anello più debole della catena per fare breccia all'interno dell'organizzazione, è in continuo aumento. In aggiunta, la situazione di emergenza sanitaria contingente impone di ripensare l'approccio alla supply chain e di rivedere le relazioni lungo tutta la filiera, riformulando le stime del rischio cyber e puntando su catene di fornitura meno globali e più locali. Per fronteggiare le sfide emergenti in questo settore occorre mettere in campo sistemi di governance che prevedano la ripartizione delle responsabilità di sicurezza tra i diversi attori, strutturare nuovi processi e prendere decisioni insieme ai propri partner che siano basate sempre di più sul concetto di fiducia digitale (Digital Trust), ovvero sulla valorizzazione di un insieme di elementi reputazionali e di approccio alla security ritenuti mutualmente importanti.

L'Osservatorio Cybersecurity & Data Protection, al suo sesto anno di Ricerca, si è posto l'obiettivo di rispondere al bisogno di conoscere, comprendere e affrontare le principali problematiche della cybersecurity e della data protection e di monitorare l'utilizzo di nuove tecniche e tecnologie a supporto di tale area da parte delle aziende end user, creando una community permanente di confronto.

La Ricerca 2020 dell'Osservatorio ha proposto una Survey di rilevazione che ha coinvolto 651 CISO, CSO, CIO, Compliance Manager, Risk Manager, Chief Risk Officer e DPO di imprese italiane. In particolare, sono state coinvolte 151 grandi organizzazioni (>249 addetti) e 500 PMI (tra 10 e 249 addetti).
La Survey sulle grandi imprese, oltre a monitorare il mercato della cybersecurity e l'impatto di alcuni dei principali trend dell'innovazione digitale sul modello della gestione della sicurezza informatica all'interno delle organizzazioni, ha dedicato un approfondimento specifico al mondo della Supply Chain security[1].

[1] Con Supply Chain security si fa riferimento a processi, tecnologie e competenze attraverso cui un'organizzazione gestisce e regola il

Le soluzioni tecnologiche adottate per la gestione della Supply Chain security

I rischi cyber inerenti la Supply Chain possono riguardare diversi aspetti quali l'approvvigionamento, la gestione dei fornitori, la continuità del servizio e la sicurezza delle informazioni: in merito a quest'ultimo punto, il ricorso massivo ad ambienti Cloud, la crescente automazione e il cambiamento delle modalità di lavoro impongono di rivedere le priorità di sicurezza, superando il concetto tradizionale di difesa del perimetro. I soggetti malintenzionati utilizzano per lo più vettori di attacco tradizionali (es. business email compromise, phishing, botnet, DDoS) per fare breccia all'interno dell'organizzazione, oppure sfruttano i punti di accesso da remoto riservati alle terze parti con privilegi elevati.

Tutti questi fattori contribuiscono a dipingere un quadro poco rassicurante, che si traduce in un pericolo concreto per le organizzazioni: secondo quanto emerge dall'indagine dell'Osservatorio, quasi un'azienda su quattro (24%) ha dichiarato di aver subito negli ultimi 12 mesi un incidente di sicurezza legato a una violazione delle proprie terze parti. Per mitigare i rischi è necessario adottare soluzioni tecnologiche specifiche per la gestione della sicurezza informatica nell'ambito Supply Chain, che sono però ancora poco diffuse e conosciute: solo il 20% delle organizzazioni, infatti, afferma di aver adottato questa tipologia di strumenti.
Le soluzioni di Supply Chain security introdotte hanno l'obiettivo di garantire il monitoraggio della postura cyber delle terze parti attraverso uno scoring basato su dati di cyber threat intelligence e permettere la mappatura delle relazioni con i fornitori lungo tutta la catena di approvvigionamento. Si ricorre inoltre a strumenti di virtualizzazione di rete e desktop, per permettere l'assistenza remota, soluzioni di autenticazione multi-fattore e utilizzo di connessioni sicure che permettono di prevenire i rischi di attacco lungo tutta la catena (**Figura 1**).

Il presidio della Supply Chain security all'interno delle organizzazioni

Le sfide che le aziende si trovano a dover affrontare quando si parla di Supply Chain security non sono però soltanto legate al campo tecnologico, ma anche alla sfera della governance.

È necessario, innanzitutto, individuare il presidio organizzativo della materia e i profili di responsabilità. In secondo luogo, assume un ruolo fondamentale l'info-sharing e, quindi, la comunicazione efficace tra gli attori della filiera mediante la condivisione di informazioni utili, linee guida e best practices da mettere a fattor comune. Infine, occorre determinare le regole di accesso ai sistemi dell'organizzazione, gestire le credenziali e avere il controllo dei dati scambiati con le terze parti in tutte le fasi della relazione, dal momento di stipula dell'accordo fino alla fase di off-boarding. Le responsabilità di sicurezza tra i diversi soggetti

rapporto con le terze parti (fornitori, partner, clienti), al fine di mitigare i rischi e le minacce cyber derivanti dalla propria catena del valore.

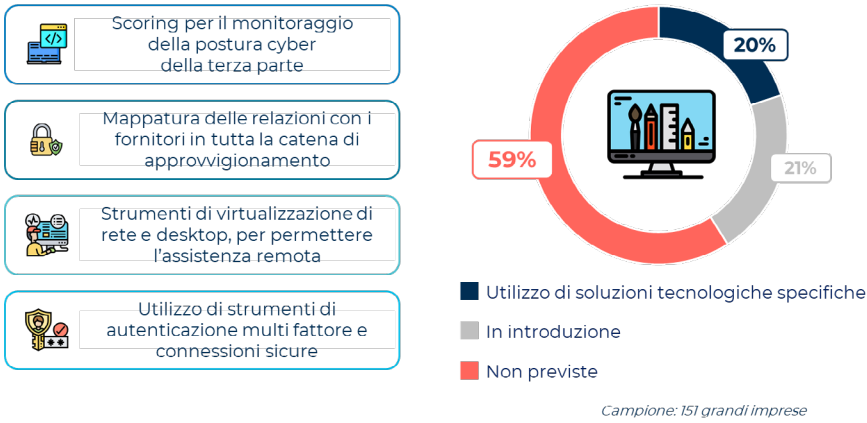


Figura 1- *Le tecnologie adottate in ambito Supply Chain security – Fonte: Osservatorio Cybersecurity & Data Protection, School of Management Politecnico di Milano*

coinvolti devono essere definite in maniera chiara e esplicita, mediante la formalizzazione di apposite clausole contrattuali.

Secondo quanto emerge dalla Survey, la responsabilità in materia di Supply Chain security all'interno delle grandi aziende italiane è gestita in maniera piuttosto eterogenea: molto spesso viene demandata alla funzione IT (54%) o alla funzione Security (31%), se diversa dall'IT, mentre sono poche le organizzazioni in cui la responsabilità è affidata a funzioni differenti (es. Operations, Procurement, Risk Management, Legal e Compliance). All'interno del campione si registrano alcuni casi "virtuosi", con un modello di gestione strutturato su più livelli oppure in cui è molto forte la collaborazione tra le diverse funzioni (**Figura 2**). Solo nel 33% delle aziende, però, esiste un presidio formale della materia, che non implica necessariamente la presenza di una figura dedicata.

Considerando la numerosità delle organizzazioni che hanno adottato soluzioni tecnologiche specifiche per la gestione degli aspetti di sicurezza informatica nell'ambito dei rapporti con le terze parti e, allo stesso tempo, previsto un presidio organizzativo formale della materia, il risultato è piuttosto allarmante: si denota complessivamente una situazione di scarsa maturità, con solo il 13% delle imprese del campione che prevede sia l'utilizzo di strumenti tecnici sia l'introduzione di un modello di governance adeguato.

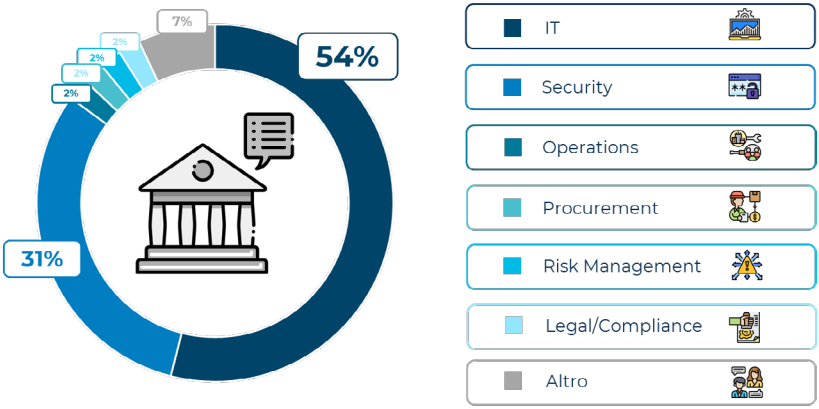


Figura 2 - *La responsabilità di gestione della Supply Chain security – Fonte: Osservatorio Cybersecurity & Data Protection, School of Management Politecnico di Milano*

Il processo di gestione della Supply Chain security e le azioni implementate

La Ricerca dell'Osservatorio ha inoltre indagato lo svolgimento da parte delle organizzazioni di alcune azioni necessarie per minimizzare i rischi per la sicurezza derivanti dal rapporto con le terze parti.

La prima azione esaminata consiste nell'identificazione della catena di fornitura, degli asset e dei dati trattati dalle terze parti in relazione ai servizi erogati. Un'azienda che si trova ad affrontare il problema della sicurezza della Supply Chain è infatti chiamata prima di tutto a verificare chi sono le terze parti con cui lavora (partner commerciali, fornitori di servizi, o altro), chi tra essi ha accesso ai sistemi e alle risorse dell'organizzazione, chi tratta i dati dell'azienda e quale è il livello di criticità dei dati scambiati. Questa azione viene attualmente svolta dal 48% delle organizzazioni.

La seconda tra le attività indagate consiste nello svolgimento di security risk assessment e audit sulle terze parti. Esistono varie soluzioni e metodi per la valutazione della postura di sicurezza delle terze parti e ciascuna organizzazione può scegliere quello che ritiene più adatto a seconda, ad esempio, del settore di appartenenza, del numero di fornitori con cui si relaziona e, in generale, della propria strategia di sicurezza. Solamente il 34% delle organizzazioni ha però svolto security risk assessment sulle terze parti e/o sui sub-contractors ("quarte parti").

Una volta effettuate le attività di analisi e assessment della terza parte, l'azienda deve continuare a monitorarla per tutto il corso della relazione, al fine di rilevare eventuali nuovi rischi

cyber che non erano emersi precedentemente e, in generale, per assicurare la conformità con quelli che sono gli obiettivi di sicurezza aziendali. Il monitoraggio continuativo dei rischi cyber associati alle terze parti viene effettuato dal 30% delle organizzazioni.

Infine, vi è il tema della compliance normativa. Sono numerosi i testi di legge che impongono infatti il rispetto di specifici requisiti di sicurezza nel rapporto con le terze parti. A titolo puramente esemplificativo si può menzionare il GDPR che, come noto, vincola i Titolari del trattamento a valutare le misure di sicurezza del Responsabile del trattamento per garantire i diritti degli interessati e richiede che il Responsabile stesso supporti il Titolare in caso di data breach e gestione degli incidenti. I requisiti di sicurezza previsti dalle normative vanno identificati e successivamente formalizzati in apposite clausole contrattuali, al fine di definire esplicitamente la ripartizione delle responsabilità di sicurezza tra gli attori della filiera. Questa attività risulta essere quella più compiuta dalle organizzazioni, nello specifico dal 63% del campione.

In conclusione, dall'analisi effettuata dall'Osservatorio emerge una maggiore attenzione sul tema della formalizzazione dei requisiti di sicurezza e della definizione delle responsabilità tra i vari attori della filiera. Si riscontra invece minore maturità sulle attività di assessment e audit sulle terze parti, e soprattutto, sulle attività di monitoraggio continuativo dei rischi cyber: dato quest'ultimo poco confortante, in quanto un'efficace strategia di Supply Chain security deve passare necessariamente dalla previsione di un processo strutturato che non si esaurisca nel compimento di alcune specifiche attività, essendo richiesta un'attenzione costante e continua per tutta la fase di relazione con la terza parte (**Figura 3**).

Figura 3 - *Il processo di gestione della Supply Chain security – Fonte: Osservatorio Cybersecurity & Data Protection, School of Management Politecnico di Milano*

Ahi Ahi Ahi IoT!

Vulnerabilità nei progetti basati sull'implementazione delle tecnologie IoT: considerazioni da valutare opportunamente nelle fasi di progettazione, realizzazione e gestione.

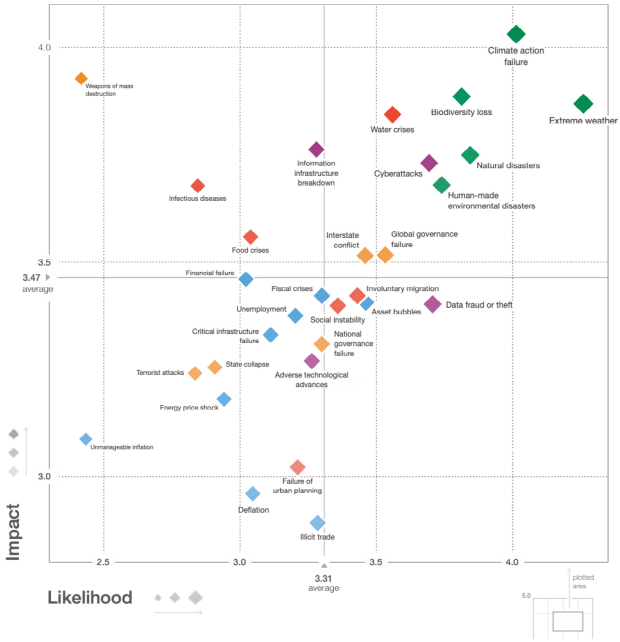
[A cura di Alessandro Vallega e Roberto Obialero]

Le soluzioni basate sull'IoT non hanno ancora raggiunto quella maturità necessaria a farci stare tranquilli. L'utilizzo in grande scala dell'IoT è relativamente recente e presenta diverse vulnerabilità dovute alle inevitabili pressioni derivanti dalla necessità di arrivare sul mercato prima della concorrenza.
Con l'IoT la società nel suo complesso sta intraprendendo una strada pericolosa e ci aspettiamo dei parallelismi con quella dell'introduzione di Internet (il Rapporto Clusit e i giornali ne testimoniano regolarmente gli incidenti) ma con una importante differenza: **l'IoT è ormai dappertutto!**[1]

Trascurare il tema della cybersecurity in questa fase evolutiva significa esporre la società, l'economia, la competizione internazionale, la sicurezza nazionale ed Europea, e la salute e il benessere dei cittadini a rischi molto grandi.
Nel rapporto Global Risk Report 2020 del World Economic Forum il rischio "CyberAttack", figura, per probabilità e impatto, tra i primissimi rischi globali ed è il primo rischio di tipo tecnologico.

L'interconnessione tra rischi di natura diversa aumenta i danni potenziali causati dalla vulnerabilità delle infrastrutture basate sul software e sulle reti sempre di più distribuite con sensori e attuatori nel mondo fisico e degli oggetti IoT.

[1] Il focus della nostra analisi prescinde dalle applicazioni specifiche al mondo dei sistemi di controllo industriale noto come OT (Operational Technology).



Fonte "Global Risk Report 2020 – Insight Report 15th edition"

Sicuramente non si può attribuire solo ai fornitori (produttori ed integratori delle soluzioni) la responsabilità della messa in sicurezza di tali infrastrutture; il mercato, infatti, raggiunge un equilibrio tra domanda e offerta ed è il mercato che dovrebbe considerare, oltre al prezzo, anche la Sicurezza e, in senso lato la Qualità delle soluzioni.
Di conseguenza è importante per la domanda aumentare la propria consapevolezza di questi requisiti non funzionali e, da una parte, pretendere e dall'altra, adottare le regole ispiratrici del principio "Security by Design". Ciò si configura attraverso un opportuno investimento iniziale di analisi della sicurezza che dovrebbe guidare la progettazione di tutti i nuovi sistemi e servizi, così salvaguardando le aziende dalle maggiori spese relative all'applicazione dei rimedi su sistemi di produzione e dal rischio potenziale di gravi incidenti.

Vulnerabilità

Le realizzazioni di progetti innovativi basati sull'introduzione di nuove tecnologie si trovano inevitabilmente a fare i conti con la presenza di vulnerabilità tecnologiche ed organizzative che vengono sfruttate da agenti ostili per architettare delle azioni offensive.
Di seguito sono riportate alcune notizie recenti e rapporti internazionali in merito alle potenziali vulnerabilità:

26 aprile 2019 – Milioni di dispositivi Internet of Things (IoT) sono vulnerabili ad attacchi di session hijacking a causa di due vulnerabilità nel componente software peer-to-peer (P2P) iLnkP2P. La prima vulnerabilità è un difetto di enumerazione che consente agli attaccanti di scoprire facilmente i dispositivi collegati; il secondo può essere sfruttato per intercettare le comunicazioni tra gli utenti ed i loro dispositivi. Il protocollo iLnkP2P, sviluppato da un produttore OEM cinese che rivende a diversi brand la sua soluzione, è utilizzato per la gestione di milioni di telecamere di sicurezza, webcam, baby monitor, campanelli intelligenti e sistemi di registrazione immagini DVR. Il software è stato progettato per consentire ai proprietari di accedere facilmente ai loro dispositivi tramite Internet; i dispositivi non richiedono autenticazione per l'accesso e non utilizzano la crittografia. Al momento non risulta disponibile alcuna soluzione.[2]

29 luglio 2019 - Alcuni ricercatori di sicurezza hanno identificato delle vulnerabilità che interessano il sistema operativo real time VxWorks, attualmente utilizzato da almeno due miliardi di dispositivi connessi a Internet in tutto il mondo, tra cui apparecchiature SCADA, dispositivi medicali e controller per ascensori. Le 11 falle di sicurezza identificate, applicabili ad una base installata costituita da 200 milioni di dispositivi vulnerabili, sono state soprannominate Urgent11; sei delle vulnerabilità consentono l'esecuzione di codice in modalità remota; i problemi non riguardano la versione più recente di VxWorks.[3]

10 marzo 2020 - Un rapporto di Palo Alto Networks ha rilevato che l'83% dei dispositivi di medical imaging negli Stati Uniti utilizza sistemi operativi obsoleti. Ciò rappresenta un aumento del 56% in due anni, che può essere in parte attribuito alla mancanza del supporto di Microsoft per Windows 7 giunto a fine vita nel gennaio 2020. Il rapporto ha analizzato un perimetro composto da 1,2 milioni di dispositivi IoT in migliaia di infrastrutture IT e sanitarie ubicate negli Stati Uniti. I ricercatori hanno anche rilevato come nel 98% dei casi il traffico inviato dai dispositivi IoT non venga crittografato.[4] Il report punta anche l'attenzione sul fatto che le apparecchiature vulnerabili non siano correttamente installate nell'ambito di sezioni di rete segregate tramite VLAN, essendo quindi facilmente raggiungibili da dispositivi PC e server adibiti a scopi ben diversi.

---

2 www.zdnet.com: Over two million IoT devices vulnerable because of P2P component flaws;
krebsonsecurity.com: P2P Weakness Exposes Millions of IoT Devices;
threatpost.com: 2 Million IoT Devices Vulnerable to Complete Takeover

3 arstechnica.com: 200 million devices–some mission-critical–vulnerable to remote takeover;
www.scmagazine.com: Over 200M devices affected by critical flaws found in real-time operating system;
threatpost.com: 'URGENT/11' Critical Infrastructure Bugs Threaten EternalBlue-Style Attacks

4 unit42.paloaltonetworks.com: 2020 Unit 42 IoT Threat Report;
www.wired.com: Most Medical Imaging Devices Run Outdated Operating Systems;
www.theregister.co.uk: The Internet of Things is a security nightmare reveals latest real-world analysis: unencrypted traffic, network crossover, vulnerable OSes

16 giugno 2020 - I ricercatori di JSOF, una società di sicurezza israeliana, hanno scoperto un gruppo di vulnerabilità che interessano milioni di dispositivi Internet of Things (IoT). Ripple20 rappresenta una serie di vulnerabilità di tipo zero-day insite in una libreria software TCP / IP di basso livello ampiamente utilizzata e sviluppata da Treck, Inc. Almeno quattro vulnerabilità sono riferibili ad una valutazione di gravità CVSS superiore a 9. A marzo, il produttore ha pubblicato una versione aggiornata della libreria che dovrebbe risolvere i difetti. Tuttavia, sarà molto difficoltoso rintracciare tutti i dispositivi vulnerabili (in quanto si parla di milioni di oggetti) oltre ad esserci delle situazioni in cui è certo che non sia possibile applicare gli aggiornamenti di sicurezza ai dispositivi. Secondo le informazioni di Forescout, il settore sanitario sembra avere un numero di dispositivi potenzialmente vulnerabili di gran lunga maggiore rispetto ad altri settori. L'articolo della testata Bleeping Computer include un elenco di fornitori con prodotti che si conferma essere interessati da Ripple20.[5]

26 ottobre 2020 - Una società di sicurezza israeliana ha scoperto più di 100 sistemi di irrigazione intelligenti esposti su Internet non protetti. I sistemi vulnerabili sono stati installati con le impostazioni predefinite dell'account di amministrazione che non richiede una password. Gli attaccanti potrebbero quindi facilmente accedere al pannello di controllo del sistema, modificare le impostazioni ed eliminare altri utenti. La società ha notificato la situazione al CERT Israeliano, che ha in seguito contattato le aziende interessate ed il produttore del sistema (Motorola) per la soluzione della vulnerabilità.[6]

Incidenti di dominio pubblico

Come abbiamo visto vengono spesso scoperte e sfruttate vulnerabilità di ogni tipo per realizzare malware, attacchi e data breach.
Nel seguente elenco riportiamo alcuni incidenti di pubblico dominio corredati da una pri ma analisi delle vulnerabilità presenti, occorsi nel corso degli ultimi 2 anni, che hanno coinvolto aziende fornitrici di progetti e soluzioni basate su tecnologie IoT.

18 marzo 2019 - Una nuova variante del malware botnet Mirai ha aggiunto nuovi exploit per diversi nuovi dispositivi Internet of Things (IoT), inclusi i sistemi di presentazione wireless WePresent WiPG-1000 e le TV LG Supersign. La nuova variante Mirai ha anche nuove credenziali da utilizzare negli attacchi brute force. Questa variante Mirai include 27

[5] www.jsof-tech.com: Ripple20 | 19 Zero-Day Vulnerabilities Amplified by the Supply Chain;
www.wired.com: A Legion of Bugs Puts Hundreds of Millions of IoT Devices at Risk;
www.darkreading.com: 'Ripple20' Bugs Plague Enterprise, Industrial & Medical IoT Devices; www.bleepingcomputer.com: List of Ripple20 vulnerability advisories, patches, and updates;
www.forescout.com: Identifying and Protecting Devices Vulnerable to Ripple20

[6] ww.zdnet.com: Over 100 irrigation systems left exposed online without a password

exploit, 11 dei quali sono completamente nuovi per il malware.[7]
In questo caso si fa riferimento allo sviluppo di codice malevolo creato appositamente per infettare dispositivi basati su IoT vulnerabili in quanto utilizzano credenziali di gestione di default oppure non aggiornati periodicamente con l'obiettivo di renderli parte di una botnet, Mirai, che già nel corso del 2016 ha provocato un attacco D-DoS devastante.[8]

26 giugno 2019 - Un malware chiamato Silex ricerca ed identifica dispositivi Internet of Things (IoT) scarsamente protetti basati su Unix o Linux e li rende inutilizzabili. Secondo il presunto creatore di Silex l'obiettivo del malware, è unicamente quello di impedire che i dispositivi non protetti siano oggetto di attacchi di tipo hijacking da parte di persone meno scrupolose allo scopo di essere utilizzati in una botnet. Prima che il server adibito ad attività di comando e controllo venisse chiuso Silex ha bloccato almeno 4.000 dispositivi IoT.[9]
Sono stati attaccati dispositivi facilmente raggiungibili via rete pubblica tramite il protocollo insicuro telnet e gestiti con credenziali deboli; da notare come il malware sia stato espressamente creato con l'obiettivo primario di identificare dispositivi vulnerabili onde evitare che potessero essere facilmente reclutati nelle file di qualche bot-net.

29 dicembre 2019 - È stato erroneamente esposto su Internet per oltre 3 settimane un database non sufficientemente protetto appartenente al fornitore di prodotti Internet of Things (IoT) Wyze contenente le informazioni sui dispositivi e sugli indirizzi e-mail dei clienti. Il data breach associato riguarda circa 2,4 milioni di utenti. Wyze commercializza fotocamere intelligenti, serrature intelligenti e altri prodotti IoT per la casa; alcuni dei dati compromessi includono informazioni personali sulla salute dei clienti.[10]
Questo incidente, anche se non riferibile ad una vulnerabilità specifica dei sistemi IoT, ha per protagonista la società Wyze, produttore che commercializza fotocamere e serrature intelligenti oltre ad altri prodotti IoT per la casa; a causa di un errore umano è avvenuta una esposizione su rete pubblica del database dei clienti, anche se per un tempo limitato, che ha provocato un data breach relativo ai nominativi ed al dettaglio dei dispositivi acquistati da circa 2,4 milioni di clienti.

---

7 www.zdnet.com: New Mirai malware variant targets signage TVs and presentation systems
arstechnica.com: Brace yourselves: New variant of Mirai takes aim at a new crop of IoT devices
www.cyberscoop.com: Mirai offshoot offers 'greater firepower' for DDoS attacks, researchers warn

8 https://arstechnica.com/information-technology/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever/

9 duo.com: The Curious Case of Silexbot- threatpost.com: Thousands of IoT Devices Bricked By Silex Malware
www.bleepingcomputer.com: New Silex Malware Trashes IoT Devices Using Default Passwords

10 www.zdnet.com: IoT vendor Wyze confirms server leak –
www.scmagazine.com: Wyze Labs data breach exposes 2.4 million, includes PHI - arstechnica.com: Employee error to blame for massive data leak, Wyze says

2 febbraio 2020 - Alcuni criminali hanno utilizzato attacchi di tipo hijacking verso i sistemi di controllo degli accessi agli edifici intelligenti utilizzandoli per lanciare attacchi DDoS (Distributed Denial of Service). È stata rilevato un aumento delle attività di scansione verso i sistemi Nortek Security & Control (NSC) Linear eMerge E3 che denotano vulnerabilità gravi sfruttabili tramite un attacco noto di tipo command injection.[11]
In questa situazione è stata evidenziata la presenza di diverse falle di sicurezza in una soluzione software utilizzata nel controllo accessi fisici degli smart building che ha consentito di prendere il controllo dei dispositivi per attuare attacchi di tipo D-DoS.

L'inadeguatezza delle misure di protezione

Analizzando le cause degli incidenti riportati nei paragrafi precedenti si possono sintetizzare problemi comuni ed annosi derivanti dalla mancata adozione di regole di sicurezza fondamentali nella fase di progettazione, nella configurazione sicura dei dispositivi e nell'adozione delle misure di sicurezza, ovvero:

- **L'uso di credenziali di autenticazione di default**: molti produttori di sistemi di elaborazione dati integrano all'interno dei dispositivi delle credenziali standard utilizzabili sia per attività di manutenzione che per eventuale monitoraggio; le best practices di sicurezza ne prevedono la rimozione o almeno la rinomina dell'account per evitare di lasciare indizi utili nelle fasi preliminari di definizione di un attacco.
- **La possibilità di accedere in modo non autenticato ai dispositivi IoT**: alcuni sensori impiegati nelle reti di campo sono collegati ai sistemi di gestione tramite protocolli di rete di basso livello che non prevedono l'autenticazione degli accessi; una modifica non autorizzata alla loro configurazione oppure ad un comando di un attuatore potrebbe indurre conseguenze molto spiacevoli.
- **La gestione remota tramite protocolli di connessione insicuri**: la gestione remota dei dispositivi tramite utilizzo di protocolli di rete insicuri, quali ad esempio telnet, non dovrebbe essere utilizzata in nessun modo perché non prevede la cifratura delle comunicazioni e consente con facilità di intercettare le credenziali utilizzate per la gestione.
- **La mancata cifratura delle comunicazioni**: in una rete distribuita e poco presidiata è molto plausibile la minaccia dell'intercettazione delle comunicazioni che potrebbe avere come conseguenze l'impersonificazione delle utenze oppure attacchi di tipo Man In The Middle.
- **La commistione e la mancanza di segregazione delle reti**: in certi casi le reti in cui sono installati i componenti IoT non sono logicamente separate e non hanno un accesso controllato rispetto alle reti su cui sono attestati i servizi ICT convenzionali.

[11] securitynews.sonicwall.com: Linear eMerge E3 Access Controller Actively Being Exploited
www.darkreading.com: Attackers Actively Targeting Flaw in Door-Access Controllers
cyware.com: Attackers Exploit Security Flaws in Smart Building Systems

- **Il mancato aggiornamento del firmware**: come tutto il software anche quello presente nel firmare è soggetto a bug di sicurezza e quindi occorre prevedere dei meccanismi sicuri ed efficaci di aggiornamento periodico alle ultime versioni del codice rilasciato dal produttore. In questo caso l'operazione è complicata dalla numerosità e dalla dispersione geografica dei dispositivi da aggiornare.
- **L'utilizzo di sistemi operativi obsoleti**: le stesse considerazioni sopra esposte, allargate a tutta la catena di fornitura, valgono per i sistemi operativi a supporto degli strati software applicativi.
- **Il software non viene sviluppato in maniera sicura e non viene controllato adeguatamente:** il software sviluppato (programmi) e integrato (librerie di supporto) dovrebbe seguire un percorso ideale che parte dalla condivisione di requisiti di sicurezza irrinunciabili sino alla loro verifica attraverso le varie fasi del ciclo di vita che includa un penetration test eseguito prima della messa in produzione del sistema.

Come anticipato queste debolezze potrebbero essere mitigate attraverso l'adozione delle best practices, disponibili a livello internazionale, relative alla progettazione e gestione di sistemi con componenti IoT e raccolte nella pubblicazione "IoT Security e Compliance. Gestire la complessità e i rischi" edita dalla Clusit Community for Security, scaricabile gratuitamente all'indirizzo:

https://iotsecurity.clusit.it/#/

Applicabilità delle contromisure in una realtà complessa ed eterogenea

Le difficoltà e i pericoli sono riconducibili alla numerosità degli oggetti IoT (trattandosi di miliardi di oggetti distribuiti e difficilmente aggiornabili ex-post) e dei sistemi che li gestiscono, oltre che all'eterogeneità dei sistemi e delle tecnologie da utilizzare.
Statista, un fornitore di dati e ricerche basato in UK, stima che nel 2030 saranno connessi in rete 24 miliardi di device[12], mentre già nel 2019, secondo gli Osservatori del Politecnico di Milano, il mercato dell'IoT in Italia è cresciuto del 24% fino ad arrivare ad un volume di 6,2 miliardi di euro.

Rispetto all'eterogeneità dei sistemi, troviamo l'IoT dappertutto e con l'IoT l'automazione è uscita dai data center ed è arrivata ovunque nelle nostre case, nelle auto, nella logistica, sui mezzi pubblici, come risulta nell'elenco dei dispositivi coinvolti nei singoli attacchi citati:

- webcam, router, sistemi di presentazione wireless aziendali.
- Telecamere di sicurezza, baby monitor, campanelli intelligenti e sistemi di registrazione immagini DVR.
- Sistemi medicali utilizzati nelle strutture sanitarie.
- Pompe per somministrazione di insulina, stampanti, sistemi UPS (Uninterruptible Power Supply), dispositivi di rete, sistemi di videoconferenza, ecc.
- Sistemi di controllo di ascensori ed applicazioni mission critical.
- Sistemi di controllo degli accessi fisici a sedi, uffici, sale riunioni presenti negli smart building.
- Sistemi di controllo dell'irrigazione.

L'IoT ci presenta una sfida complessa che deve essere analizzata sin dal principio; solamente facendo così possiamo sperare di evitare di dover pagare successivamente un prezzo molto elevato a causa della nostra superficialità. È indubbiamente una sfida che la società non può permettersi di perdere!

[12] https://www.statista.com/statistics/1183463/iot-connected-devices-worldwide-by-technology

Attacchi e minacce alle infrastrutture critiche italiane

[A cura di Aldo Di Mattia, Fortinet]

Nel corso del 2020 la pandemia ha cambiato drasticamente la vita e le abitudini di ogni persona in tutti i settori. Nella sicurezza informatica, di conseguenza, il Covid-19 ha stravolto repentinamente le logiche di protezione ormai consolidate. Le infrastrutture critiche italiane hanno visto un numero considerevole di minacce che analizziamo in dettaglio estraendo i dati dai FortiGuard Labs.

FortiGuard Labs è l'organizzazione globale di threat intelligence e ricerca sulle minacce di Fortinet. La sua missione è fornire informazioni di threat intelligence alle soluzioni di sicurezza Fortinet con lo scopo di aumentare la prevenzione e la protezione degli attacchi informatici. Utilizzando milioni di sensori, i FortiGuard Labs monitorano la superficie di attacco mondiale e utilizzano l'intelligenza artificiale per estrarre i dati relativi alle minacce.

Per capire cosa è accaduto nelle infrastrutture critiche italiane nel corso del 2020 sono stati presi in considerazioni tre aspetti:

- Attacchi OT individuati attraverso specifiche firme
- Le dieci famiglie di minacce web più importanti nei quattro trimestri
- Le prime tre firme individuate di malware, attacchi e botnet per alcuni dei mercati di riferimento delle infrastrutture critiche nei quattro trimestri

Operation Technology Security

Il **Grafico 1** mostra i più importanti attacchi OT individuati in Italia. I principali mercati di riferimento per la funzionalità ICS/SCADA protection sono Energy & Utilities (che include Oil/Gas e Water/Wastewater), trasportation, chemicals e manufacturing. Lungo l'asse delle ascisse sono indicate le signature degli attacchi individuati, mentre l'asse delle ordinate rappresenta il numero di volte che sono state riscontrate le minacce.

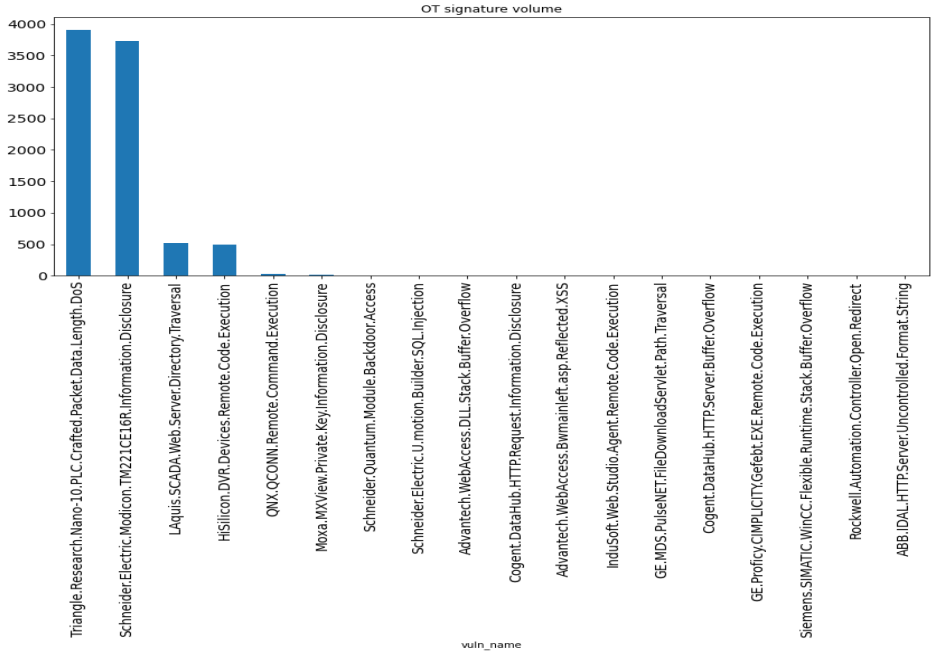


Grafico 1 - *Top attacchi OT nel corso del 2020*

Nel sito web https://www.fortiguard.com , nel campo di ricerca al centro della pagina, può essere inserito il nome delle signature mostrate nei vari grafici così da avere ogni dettaglio.

Gli attacchi più critici, considerando l'uso del sistema finale attaccato, sono stati:

- **Triangle.Research.Nano-10.PLC.Crafted.Packet.Data.Lenght.Dos** - Attacco contro una vulnerabilità Denial of Service in dispositivi PLC Triangle Research International Nano-10. La vulnerabilità è causata da un errore quando il software vulnerabile gestisce un pacchetto Modbus / TCP non valido. Consente a un utente malintenzionato remoto di bloccare i sistemi vulnerabili inviando un pacchetto specifico alla porta tcp 502. Questa componente è tipicamente utilizzata da molte aziende nei settori: agriculture and food, building automation, transportation systems, water and wastewater e energy.

- **Laquis.SCADA.Web.Server.Directory.Traversal** - Tentativo di attacco sfruttando una vulnerabilità di attraversamento di directory in LAquis SCADA. Un utente malintenzionato remoto e non autenticato può sfruttare questa vulnerabilità inviando una richiesta specifica al server di destinazione. Sfruttando questa vulnerabilità l'attaccante potrebbe accedere a qualsiasi file presente senza restrizioni. Questa componente è largamente utilizzata in ambiente agriculture and food in relazione alla gestione di pompe, caldaie e valvole.
- **QNX.QCONN.Remote.Command.Execution** - Attacco contro una vulnerabilità di esecuzione di comandi remoti in QNX QCONN. La vulnerabilità è dovuta all'incapacità del software vulnerabile di controllare adeguatamente i dati forniti dall'utente. Un utente malintenzionato remoto potrebbe essere in grado di sfruttare la vulnerabilità per eseguire comandi di shell arbitrari. QNX è un sistema operativo rivolto principalmente al mercato dei sistemi embedded. QNX è stato uno dei primi sistemi operativi commerciali microkernel di successo. A partire dal 2020, è utilizzato in una varietà di dispositivi tra cui automobili.
- **ABB.IDAL.HTTP.Server.Uncontrolled.Format.String** - Attacco che sfrutta una vulnerabilità della stringa di formato non controllata in ABB IDAL HTTP Server. Un utente malintenzionato remoto non autenticato può sfruttare questa vulnerabilità inviando una richiesta specifica al server vulnerabile. Lo sfruttamento della vulnerabilità comporta l'esecuzione di codice arbitrario da remoto o una condizione di disservizio del sistema di destinazione. ABB è uno principali produttori di sistemi di automazione industriale (robot).

Le più importanti minacce web

Nel corso dei mesi del 2020 le infrastrutture critiche hanno visto mutare la percentuale delle distinte famiglie di attacco web. Nei grafici da 2 a 5, distinta per trimestre viene mostrata la percentuale delle organizzazioni che hanno impattato una famiglia di minaccia. È interessante vedere come le percentuali siano largamente variati nel corso dei mesi soprattutto in riferimento ai cambiamenti improvvisi conseguenti alla pandemia. Le truffe on-line nel corso del 2020 meritano sicuramente il gradino più alto del podio e le paure scatenate dalla pandemia hanno contribuito a questo risultato. Il primato è schiacciante sommando HTML.phishing (siti malevoli di phishing), HTML.MicPhishing (attacchi phishing contenenti script all'interno del body) e HTML.Scam (truffa in cui gli hacker cercano di ingannare le persone per indurle a dare loro informazioni o denaro). Si può notare un cambiamento notevole a marzo, quando l'Italia è finita improvvisamente in lockdown, e nei successivi mesi che hanno visto un cambio di rotta ben distinto rispetto i primi due mesi dell'anno.

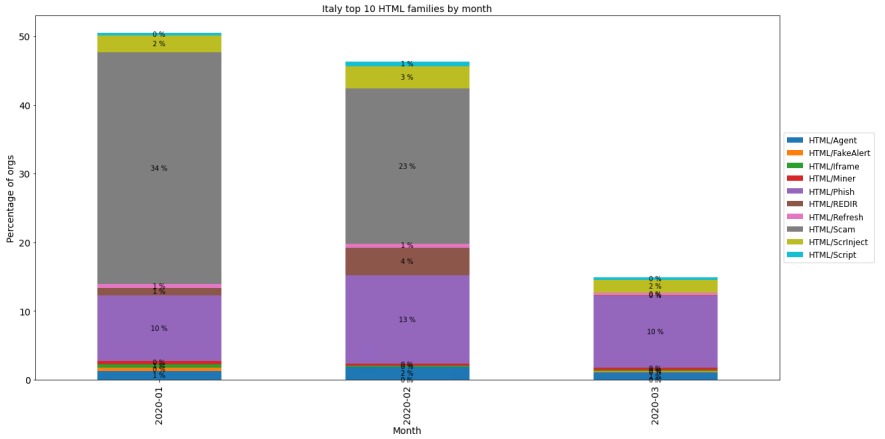


Grafico 2 - *Percentuale organizzazioni colpite da attacchi HTML nel primo trimestre*

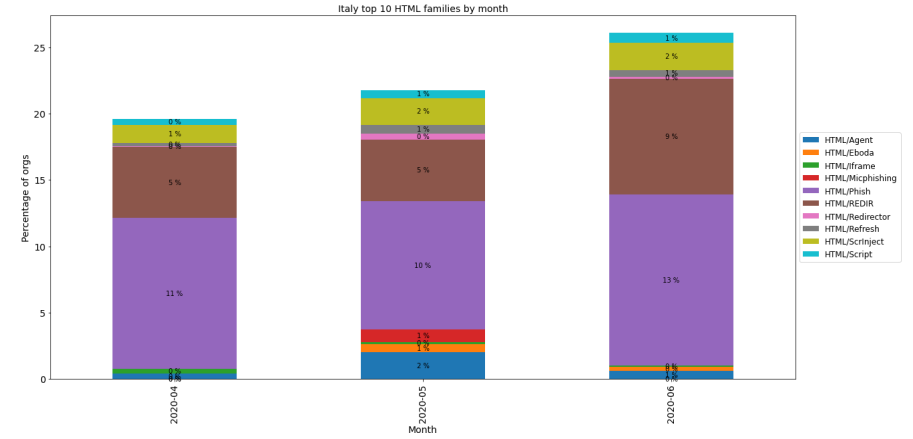


Grafico 3 - *Percentuale organizzazioni colpite da attacchi HTML nel secondo trimestre*

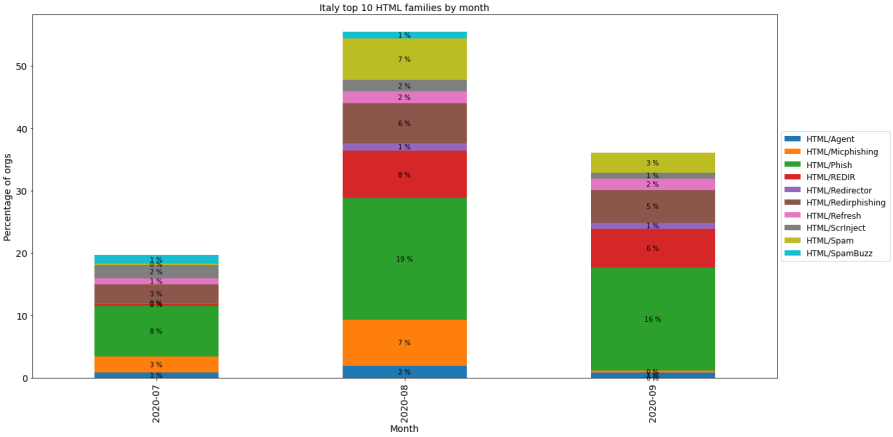


Grafico 4 - *Percentuale organizzazioni colpite da attacchi HTML nel terso trimestre*

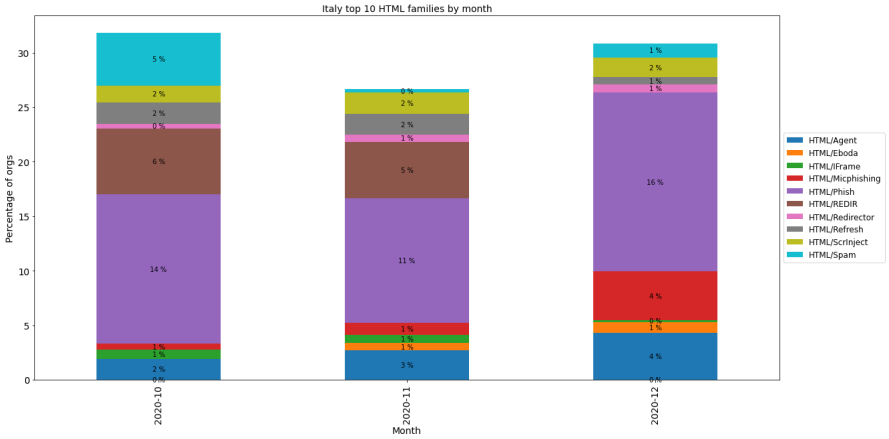


Grafico 5 - *Percentuale organizzazioni colpite da attacchi HTML nel quarto trimestre*

Di seguito una descrizione delle famiglie di minacce indicate nei grafici.

HTML/Agent	URL target di attacchi generati da spam e phishing
HTML/Eboda	pagine di phishing specifico su software Adobe
HTML/FakeAlert	finestre che danno alert di infezione virus per ottenere click
HTML/IFrame	pagine contenenti iframe malevoli
HTML/Micphishing	pagine di phishing contenenti script all'interno del body
HTML/Phish	pagine di phishing generico tipicamente generate da mail
HTML/Redirect	redirect del traffico su pagine indesiderate (anche HTML/Redirector)
HTML/Refresh	refresh della pagina con redirect su siti malicious, phishing, adversiting
HTML/ScrInject	codice di injection associato a siti malevoli
HTML/Spam	pagine generiche di spam
HTML/SpamBuzz	spam con richieste di denaro per servizi (eg: più followers su Instagram)
HTML/Redirphishing	redirect del traffic su siti di phishing
HTML/Scam	inganno per indurre le vittime a dare informazioni o denaro
HTML/Script	pagina di login fac-simile create tipicamente con JavaScript

Le minacce nei mercati verticali

Un altro dato importante riguarda le minacce più rilevate in alcuni dei mercati che costituiscono le infrastrutture critiche nel corso dei quattro trimestri del 2020.
I grafici seguenti mostrano lungo l'asse delle ascisse le tre signature antivirus, IPS e botnet con maggiore volume riscontrato nel corso dei quattro trimestri, lungo l'asse delle ordinate viene indicata la percentuale del volume, in termini di quantità di traffico riscontrata. In questo caso si possono fare interessanti considerazioni visto che le minacce cambiano in base al mercato specifico. In alcuni casi si possono vedere gli stessi attacchi con una percentuale di volume differente mentre in altri casi gli attacchi sono completamente distinti.

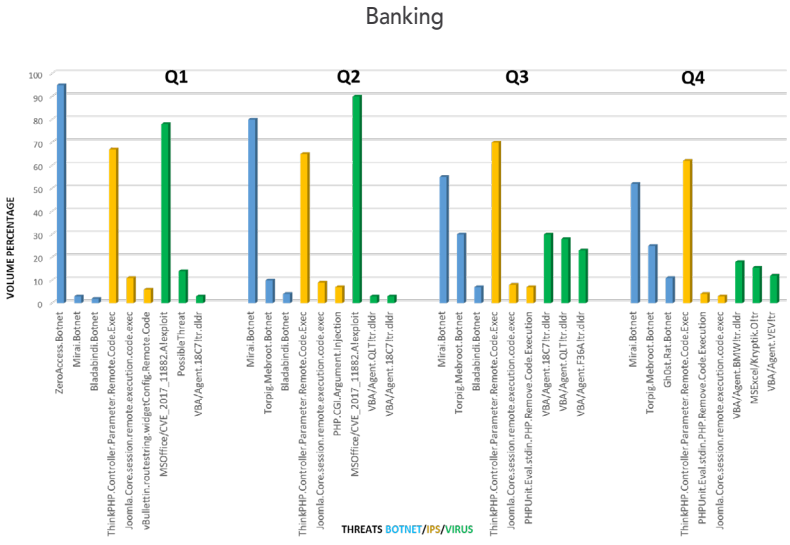


Grafico 6 - *Top 3 signature IPS, AV, Botnet nel mercato Banking durante i quattro trimestre*

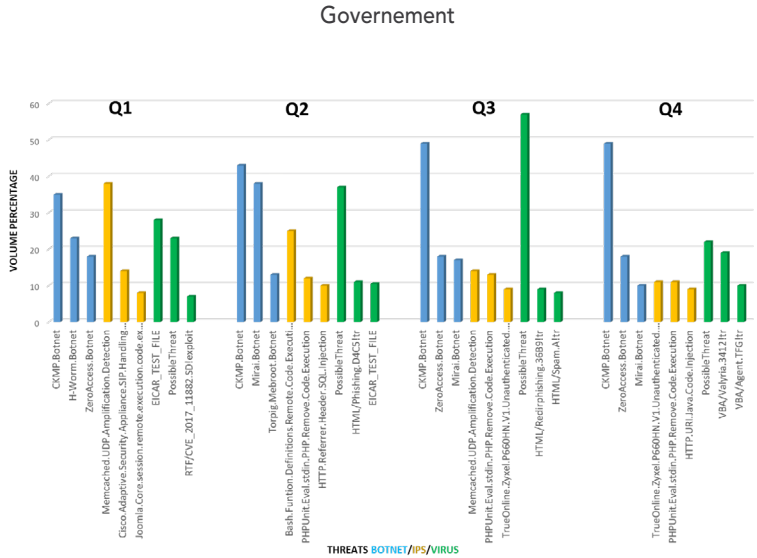


Grafico 7 - *Top 3 signature IPS, AV, Botnet nel mercato Governement durante i quattro trimestri*

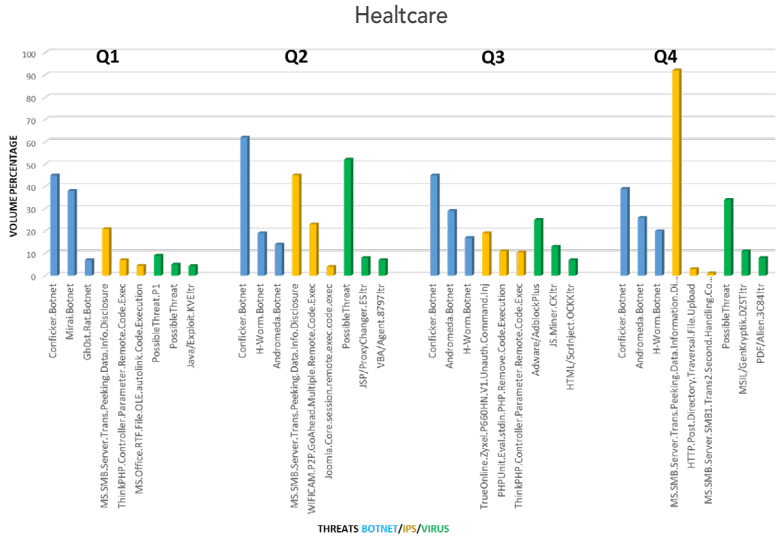


Grafico 8 - *Top 3 signature IPS, AV, Botnet nel mercato Healtcare durante i quattro trimestri*

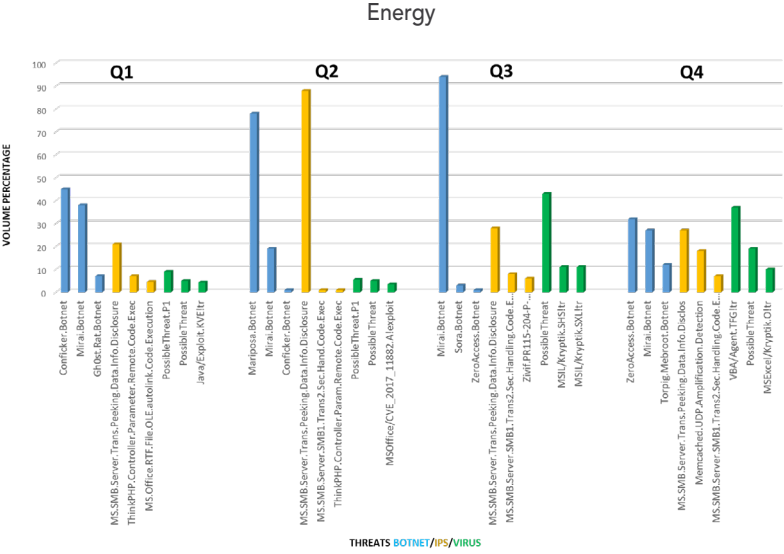


Grafico 9 - *Top 3 signature IPS, AV, Botnet nel mercato Energy durante i quattro trimestri*

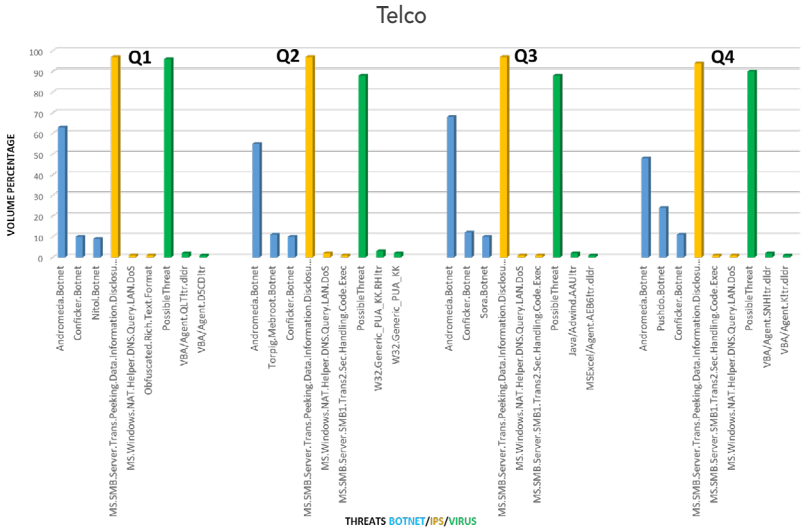


Grafico 10 - *Top 3 signature IPS, AV, Botnet nel mercato Telco durante i quattro trimestri*

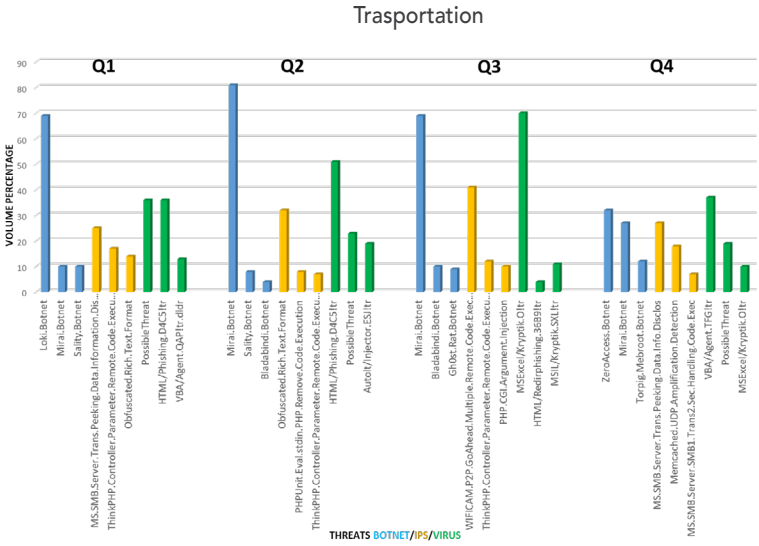


Grafico 11 - *Top 3 signature IPS, AV, Botnet nel mercato Trasportation durante i quattro trimestri*

Anche in questo caso è possibile sfruttare il sito FortiGuard per avere tutti i dettagli relativi alle firme indicate quali: applicazione o sistema operativo affetto, prima data di avvistamento della minaccia, ultima data di aggiornamento, descrizione, eventuale CVE o rimandi a siti esterni che integrano la descrizione e il funzionamento della minaccia oltre che le azioni raccomandate per bloccarla.

Infrastrutture critiche italiane - previsioni 2021

Il 2020 ha messo in luce come i cybercriminali siano in grado di sfruttare velocemente ogni fattore per perpetrare attacchi senza precedenti. Ora ci troviamo di fronte a un altro significativo cambiamento dovuto allo sviluppo di intelligent edge oltre che l'introduzione del 5G. Queste nuove architetture oltre ad essere prese di mira, saranno utilizzate a loro volta per colpire altre vittime, sfruttando le elevatissime risorse (in termini di CPU e RAM) e la velocità introdotta dal 5G. Per prevenire lo scenario che si sta delineando, tutti gli edge devono essere implementati con soluzioni di sicurezza che abbiano la capacità di individuare attacchi sconosciuti attraverso l'intelligenza artificiale e il machine learning oltre che avere la capacità di collaborare attraverso IoC (Indici di Compromissione) con l'infrastruttura di sicurezza circostante e con quella dei propri partner. I FortiGuard Labs, nel più recente rapporto "threat predictions", ipotizzano alcuni importanti scenari nel corso del 2021, tra i quali:

- Trojan evoluti con lo scopo di colpire l'edge
- Attacchi swarm edge-enabled per sfruttare le risorse messe a disposizione dall'edge
- Social Engineering molto più smart e dispositivi IoT domestici presi di mira (come antifurti e sorveglianza)
- Malware sfruttati per chiedere il riscatto di device OT.

La metà dei CISO italiani crede che la "guerra" informatica sia una minaccia imminente per le loro aziende

[A cura di Liviu Arsene, Bitdefender]

Questo studio mette in evidenza come nuove minacce ransomware, problemi di comunicazione e skill gap di competenze stiano minando il settore e impongano per il futuro interventi concreti per affrontare la criminalità informatica.
La metà dei professionisti italiani della sicurezza informatica ritiene che la guerra informatica sia una minaccia per la loro azienda, eppure un terzo degli esperti di sicurezza in Italia ammette di non avere una strategia in atto per mitigare questo rischio.
Ciò è particolarmente allarmante in un periodo di sconvolgimento globale senza precedenti, poiché la metà degli intervistati concorda sul fatto che l'inasprimento di una guerra informatica danneggerà l'economia il prossimo anno.

I CISO e i professionisti della sicurezza informatica stanno comunque rafforzando le loro difese - il 43% infatti ritiene di aver bisogno di una strategia contro la guerra informatica nei prossimi 12-18 mesi.
Questi risultati vengono rivelati da uno studio internazionale che evidenzia come, nei prossimi 10 anni, il successo della sicurezza informatica risieda nell'adattabilità dei responsabili delle decisioni in materia di sicurezza, e allo stesso tempo, guarda all'ultimo decennio per vedere se sono già state apprese preziose lezioni sulla necessità di apportare cambiamenti tangibili in settori come la diversità. In dettaglio, lo studio esplora il divario tra il modo in cui i responsabili delle decisioni in materia di sicurezza e i professionisti della sicurezza informatica vedono l'attuale panorama della cybersecurity e mette in evidenza i cambiamenti che sanno di dover apportare nei prossimi mesi e anni.

Lo studio prende in considerazione i punti di vista e le opinioni di oltre 6.700 professionisti del settore, tra cui CISO, CSO e CIO, in Italia, Regno Unito, Stati Uniti, Australia/Nuova Zelanda, Germania, Francia, Spagna, Danimarca e Svezia. Gli intervistati rappresentano un ampio spaccato di aziende che vanno dalle PMI fino a imprese quotate in borsa con 10.000 e oltre dipendenti in un'ampia varietà di settori, tra cui quello finanziario, governativo, sanitario e della tecnologia.

L'incremento delle violazioni causate dai ransomware

Oltre all'incremento delle minacce relative alla guerra informatica, una vecchia minaccia sta tornando in auge: il ransomware.

Nel corso del travagliato 2020, il ransomware ha subito un'impennata con quasi la metà (44%) dei professionisti italiani della sicurezza informatica che hanno segnalato di aver rilevato un aumento degli attacchi ti questa tipologia. La cosa più preoccupante è che circa un CISO/CIO su due in Italia si aspetta un aumento degli attacchi ransomware nel prossimo anno e mezzo.

Ciò è particolarmente interessante in quanto anche quasi la metà dei CISO/CIO (46%) teme che un attacco ransomware possa portare alla chiusura della loro attività durante questo periodo se non dovessero aumentare gli investimenti nella sicurezza.

Ma cosa sta provocando l'aumento degli attacchi ransomware? Alcuni esperti suggeriscono che sia dovuto al crescente numero di persone che lavorano da remoto nelle proprie abitazioni, in questo modo il dipendente, non più tutelato dal firewall aziendale, diventa un bersaglio più facile da attaccare. La vera causa potrebbe tuttavia essere più strettamente legata alla riscossione del riscatto. Infatti, un terzo dei CISO/CIO italiani coinvolti nell'indagine ritengono che l'azienda per cui lavorano pagherebbe il riscatto pur di impedire la pubblicazione di dati/informazioni aziendali sensibili – questo comportamento rende così gli attacchi ransomware una fonte potenzialmente molto redditizia.

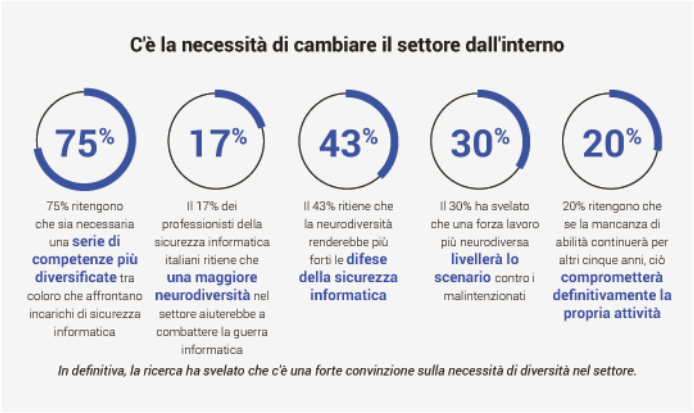
Emerge la necessità di una svolta radicale nelle modalità di comunicazione

Nell'ambito delle tematiche relative alla sicurezza informatica, cyberwarfare e ransomware sono argomenti complessi da affrontare. La difficoltà intrinseca in questi concetti e nei temi che in generale coinvolgono il settore, rende arduo il percorso per ottenere budget interni da investire a sostegno dei progetti. Per questo motivo i professionisti del settore credono che sia necessario un cambiamento. Infatti, la metà dei professionisti della sicurezza intervistati, che hanno anche un elevato potere decisionale all'interno delle loro aziende, concorda sul fatto che, per poter aumentare gli investimenti nella sicurezza informatica, il modo in cui comunicano le questioni ad essa legate debba cambiare radicalmente.

In questo contesto è quindi necessario porsi la domanda su quali siano i cambiamenti da apportare. Due quinti dei professionisti della sicurezza informatica ritengono che in futuro sarà necessario comunicare di più ad un target di referenti più ampio e con i clienti, in modo che tutti, sia all'interno che all'esterno della società, comprendano meglio i rischi. Inoltre, uno su tre sottolinea la necessità di facilitare una migliore comunicazione con la dirigenza, soprattutto quando si tratta di comprendere i rischi aziendali più ampi. E infine, ma non meno importante, l'uso di un linguaggio meno tecnico aiuterebbe tutto il settore a comunicare meglio, in modo che l'intera azienda possa comprendere quali sono i rischi e come rimanere protetta.

La diversità, e in particolare la neurodiversità[1], è la chiave del successo nel prossimo futuro. Oltre ai radicali cambiamenti necessari nel modo in cui i professionisti della sicurezza informatica comunicano, c'è anche la necessità di operare un cambiamento all'interno della composizione stessa della forza lavoro. Il settore della sicurezza informatica nel suo complesso ha sofferto a lungo di una carenza di competenze, e questo continua ad essere un problema persistente e sempre più evidente. Il 14% dei professionisti italiani della sicurezza informatica ritiene che l'aspetto legato alla sicurezza informatica che aumenterà maggiormente nei prossimi 12-18 mesi sarà l'incremento del deficit di competenze. Se lo skill gap continuerà per altri cinque anni, uno su tre degli intervistati a livello globale crede che avrà conseguenze catastrofiche per le imprese. Metà dei professionisti italiani coinvolti nella survey ritiene inoltre che il deficit di competenze comprometterà gravemente il settore se proseguirà per i prossimi 5 anni.

[1] Si veda al riguardo: https://en.wikipedia.org/wiki/Neurodiversity



Oggi, tuttavia, è necessario qualcosa di più che il semplice reclutamento di esperti qualificati per portare un effettivo cambiamento e proteggere le aziende.
Nel 2015, la metà dei lavoratori della sicurezza informatica concordavano sulla mancanza di diversificazione delle competenze nella sicurezza informatica e sul fatto che ciò fosse fonte di reale preoccupazione.
Cinque anni dopo, nel 2020, questo aspetto rimane esattamente lo stesso e questo è un problema significativo in quanto un terzo dei professionisti italiani della sicurezza informatica afferma che l'industria della sicurezza informatica dovrebbe riflettere la società che la circonda per essere efficace.

Inoltre, il 75% dei professionisti italiani interpellati ritiene che vi sia la necessità di una serie di competenze più diversificate tra coloro che si occupano di sicurezza informatica. Questo perché quasi la metà (43%) dice che la neurodiversità renderà le difese della sicurezza informatica più forti, e uno su tre ha rivelato che una maggior neurodiversità della forza lavoro porterà ad un confronto più paritario con gli hacker.

"Il 2020 è stato un anno di cambiamenti, non solo per il mondo intero, ma anche per il mondo della sicurezza informatica. Anche nel 2021 il panorama della sicurezza continuerà ad evolversi.
Assisteremo a dei cambiamenti, ma ora possiamo fare in modo che questi avvengano in chiave positiva e non negativa. Per avere successo nel nuovo panorama della sicurezza, il modo in cui noi, come settore, parliamo di sicurezza deve diventare più accessibile a un pubblico più ampio per ottenere supporto e investimenti dall'interno dell'azienda.
Inoltre, dobbiamo iniziare a pensare di colmare il gap di competenze in un modo diverso - dobbiamo concentrarci sulla diversità, e in particolare sulla neurodiversità, se vogliamo mantenere la nostra posizione e alla fine debellare la criminalità informatica".

La sicurezza dei dati nel cloud nel 2020

[A cura di Maurizio Tagliorетti, Netwrix Corporation]

Sintesi

Nel 2020, molte aziende hanno adottato rapidamente tecnologie cloud per supportare l'improvviso passaggio al lavoro remoto. Abbiamo rivisto il nostro rapporto annuale sulla sicurezza dei dati nel cloud per riflettere su questi cambiamenti senza precedenti, utilizzando un sondaggio di 937 professionisti IT in tutto il mondo condotto tramite un questionario online. Questo report aiuterà le aziende a confrontare i loro sforzi di sicurezza rispetto ai loro colleghi e a comprendere meglio le minacce ai dati archiviati nel cloud.

I risultati chiave includono quanto segue:

Dati nel cloud

Un numero inferiore di organizzazioni memorizza i dati nel cloud rispetto allo scorso anno. Nel 2019, il 57% degli intervistati ha affermato di archiviare dati non sensibili nel cloud; ora solo il 46% lo fa. Il numero di archiviazione dei dati dei clienti nella nube è sceso dal 50% al 44%.

Incidenti di sicurezza nel cloud

Le aziende hanno subito un media di 2,8 incidenti di sicurezza negli ultimi 12 mesi. I primi 3 tipi di incidenti sono stati phishing (40%), ransomware (24%) e fuga accidentale di dati (17%).

Conseguenze della violazione dei dati

Per il 49% degli intervistati, gli incidenti di sicurezza non hanno conseguenze gravi. Ma il 28% ha dovuto affrontare spese non pianificate per correggere le lacune di sicurezza, l'11% ha dovuto pagare multe per la conformità e l'8% ritiene di aver perso il proprio vantaggio competitivo.

Gli incidenti che includevano la compromissione della catena di fornitura hanno avuto il maggiore impatto sulle organizzazioni, comprese multe per conformità (53% delle organizzazioni), diminuzione delle nuove vendite (47%), cambiamento nella leadership senior (24%) e cause legali (29%).

Più di un terzo (35%) delle organizzazioni che hanno subito il furto di dati da parte di hacker ha affermato che l'incidente ha causato loro la perdita del vantaggio competitivo e / o un aumento dell'abbandono dei clienti.

Rilevamento e risposta agli incidenti

I primi tre incidenti che le organizzazioni in genere scoprono in pochi minuti o ore sono phishing e ransomware (86%) e attacchi mirati all'infrastruttura cloud (83%). Il furto di dati da parte di addetti ai lavori e la perdita accidentale di dati hanno richiesto più tempo per essere rilevate. Mentre il 50% degli intervistati ha trascorso minuti o ore per rilevare il furto

di dati privilegiati, un'altra metà non era a conoscenza dell'incidente per giorni, settimane o addirittura mesi. La perdita accidentale di dati è stata scoperta in pochi minuti o ore solo dal 39% delle organizzazioni, mentre il 61% ha avuto bisogno di giorni o settimane per individuare l'incidente.
Il furto di dati e la perdita accidentale di dati hanno anche comportato una reazione più lenta: il 43% degli intervistati ha avuto bisogno di giorni, settimane o mesi per rispondere al furto di dati da parte di un insider; e il 40% degli intervistati ha richiesto lo stesso tempo per rispondere agli attacchi hacker.
La classificazione dei dati e il controllo delle attività degli utenti hanno ridotto sia i tempi di rilevamento che di risposta. La maggior parte delle organizzazioni che utilizzano entrambe le tecnologie hanno rilevato e risolto gli incidenti in pochi minuti o ore.

Sfide per la sicurezza dei dati cloud
Il 48% dei CISO segnala che la pressione aziendale per una rapida digitalizzazione, trasformazione e crescita li distrae dalla sicurezza dei dati.
Le prime tre sfide che le organizzazioni hanno dichiarato di dover superare sono i team IT con personale ridotto (52%), la mancanza di budget (47%) e la mancanza di esperienza nella sicurezza cloud (44%).
Il 51% delle grandi aziende non ha una conoscenza sufficiente sulla sicurezza del cloud per garantire la protezione dei dati sensibili.

Misure di sicurezza dei dati cloud
I tre controlli di sicurezza cloud che le organizzazioni utilizzano sono la crittografia (62%), il controllo dell'attività degli utenti (58%) formazione dei dipendenti (58%). Nel 2019, il 59% dei dati crittografati, il 52% dell'attività degli utenti controllati e il 51% hanno applicato criteri di sicurezza più rigorosi.
Limitazione dei dati nel cloud

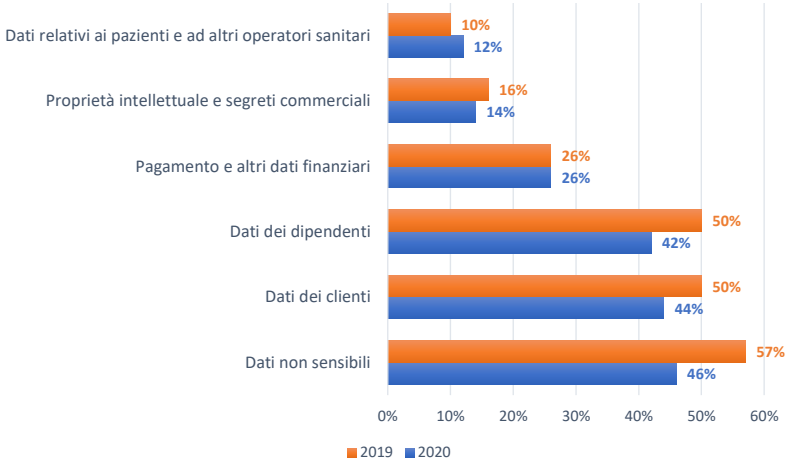
Il 62% delle organizzazioni rimuoverà i dati sensibili dal cloud o lo ha già fatto, al fine di migliorare la sicurezza dei dati. Si tratta di un aumento rispetto al 48% del 2019.
Spesa per la sicurezza informatica e budget per la sicurezza cloud

La pandemia non ha avuto alcun impatto sulla spesa per la sicurezza informatica e sulle priorità per il 21% delle organizzazioni. Il 36% degli intervistati ha dichiarato di dover modificare le proprie priorità, ma di aver comunque dovuto agire entro il bilancio esistente. Solo il 24% delle organizzazioni ha registrato un aumento della spesa.
In media, le organizzazioni assegnano il 27% del budget per la sicurezza informatica alla sicurezza cloud.

Dati nel cloud

La nostra ricerca dello scorso anno ha scoperto che molte organizzazioni (57%) memorizzavano dati "*non sensibili*" nel cloud. A causa del drammatico aumento del lavoro remoto nel 2020, ci aspettavamo che ancora più organizzazioni memorizzassero questi dati nel cloud. Tuttavia, è diminuito considerevolmente, a solo il 46%. Anche il numero di organizzazioni che archiviano i dati di clienti e dipendenti nel cloud è diminuito, anche se in modo meno drastico.

Per altri tipi di dati, la percentuale non è stata modificata molto. Sembra che alcune organizzazioni dopo aver immerso il dito nel cloud mettendo lì dati sensibili e non sensibili, hanno rivalutato i loro rischi e bisogni e siano tornati indietro.



Tipi di organizzazioni dati archiviano nel cloud

Factoidi

- Il 54% delle aziende che archiviano i dati dei clienti nel cloud ha avuto incidenti di sicurezza negli ultimi 12 mesi, rispetto al 77% dell'anno precedente.

Incidenti di sicurezza nel cloud

Anche se vorremmo confrontare i risultati dell'indagine di quest'anno con gli anni precedenti, è impossibile perché abbiamo rimodellato diverse domande e offerto ai nostri intervistati opzioni più dettagliate tra cui scegliere. Abbiamo ritenuto che le domande precedenti non riflettevano i casi d'uso nel mondo reale e i risultati non fornivano informazioni utilizzabili per aiutare le organizzazioni a costruire strategie di sicurezza informatica più adeguate per proteggere i dati archiviati nel cloud. In particolare, abbiamo apportato le seguenti modifiche:

- "Attacco esterno" è stato suddiviso in diversi tipi di incidenti, attacchi mirati all'infrastrut-

tura, compromissione dell'account, perdita di dati, furto di dati e compromissione della catena di approvvigionamento.
- "Errori accidentali" è stato limitato a "perdita accidentale di dati".
- "Attività dannosa degli addetti ai lavori" è stata definita più chiaramente come "furto di dati da parte degli addetti ai lavori".

Il phishing è stato l'incidente più comunemente sperimentato, seguito da ransomware. Una perdita di dati accidentale è in terza posizione, il che non sorprende poiché può accadere facilmente, soprattutto se i dati sono memorizzati online.

Incidenti di sicurezza più comuni

Attacchi di phishing	40%
Ransomware o altri attacchi malware	24%
Perdita accidentale di dati	17%
Attacchi mirati all'infrastruttura cloud	16%
Compromissione dell'account	16%
Perdita di dati	13%
Furto di dati da parte di addetti ai lavori	10%
Furto di dati da parte di hacker	7%
Compromissione sulla catena di approvvigionamento	6%

Le aziende più grandi avevano maggiori probabilità di subire attacchi esterni, come phishing, ransomware e attacchi mirati all'infrastruttura cloud. Altri di loro hanno anche segnalato perdite accidentali di dati e compromissione di account, che è comprensibile in quanto hanno semplicemente più utenti. Al contrario, le imprese più grandi sono meno soggette al furto di dati privilegiati. Forse questo perché hanno un monitoraggio delle attività più avanzato, contratti di lavoro più dettagliati e una migliore educazione alla sicurezza informatica per gli utenti.

Incidenti di sicurezza cloud per dimensione dell'organizzazione*

	Piccola	Media	Grande
Attacchi di phishing	30%	38%	52%
Ransomware o altri attacchi malware	15%	23%	35%
Perdita accidentale di dati	15%	14%	21%
Attacchi mirati all'infrastruttura cloud	13%	14%	21%
Compromissione dell'account	13%	15%	20%
Perdita di dati	14%	11%	15%

Furto di dati da parte di addetti ai lavori	12%	9%	9%
Furto di dati da parte di hacker	6%	4%	12%
Compromissione sulla catena di approvvigionamento	6%	2%	11%

**"Piccola" = 1-100 dipendenti, "media"=101-999 dipendenti e "grande" = oltre 1.000 dipendenti.*

Factoidi

- Le organizzazioni hanno sperimentato una media di 2.8 incidenti di sicurezza cloud negli ultimi 12 mesi.

Conseguenze della violazione dei dati

Non tutti gli incidenti di sicurezza provocano la stessa quantità di danni. Quasi la metà degli intervistati ha dichiarato che gli incidenti di sicurezza subiti non hanno avuto alcun problema. Il 28% degli intervistati ha riscontrato spese non pianificate per correggere le lacune di sicurezza e l'11% delle organizzazioni è stata soggetta a multe per la non conformità. È interessante notare che le grandi imprese avevano maggiori probabilità di includere costi per colmare le lacune in materia di sicurezza, ed erano anche più propense a perdere un dirigente di livello C: **Ogni dieci aziende enterprise,** una ha dovuto cambiare leadership senior come parte della loro risposta alla violazione **dei dati.**

Conseguenze più comuni sulla violazione dei dati

Nessun problema	49%
Spese non pianificate per colmare le lacune di sicurezza	28%
Ammende di conformità	11%
Perdita di vantaggio competitivo	8%
Abbandono dei clienti	8%
Diminuzione delle nuove vendite	8%
Diminuzione della valutazione aziendale	7%
Cambiamento nella leadership senior	6%
Cause	4%

Conseguenze della violazione dei dati per dimensione dell'organizzazione*

	Piccola	Media	Grande
Nessun problema	55%	55%	38%
Spese non pianificate per colmare le lacune di sicurezza	22%	28%	35%
Ammende di conformità	11%	7%	13%
Perdita di vantaggio competitivo	6%	8%	11%
Abbandono dei clienti	9%	8%	8%
Diminuzione delle nuove vendite	8%	6%	10%
Diminuzione della valutazione aziendale	7%	4%	10%
Cambiamento nella leadership senior	3%	5%	10%
Cause	6%	1%	5%

**"Piccola" = 1-100 dipendenti, "media"=101-999 dipendenti e "grande" = oltre 1.000 dipendenti.*

Nota importante

Non siamo in grado di identificare con precisione al 100% quali incidenti hanno portato a quali conseguenze perché una violazione dei dati spesso comportava diversi modelli di attacco (ad esempio, un attacco di phishing porta a una compromissione dell'account, che si traduce in un furto di dati). Di conseguenza, in questo rapporto, non diremo cose come "la perdita accidentale di dati ha portato a spese non pianificate nel 62% dei casi" ma piuttosto "incidenti di sicurezza cloud che hanno comportato perdite accidentali di dati hanno portato a spese non pianificate nel 62% dei casi. "

Siamo rimasti sorpresi dal fatto che gli incidenti che includevano la compromissione della catena di approvvigionamento avessero il maggiore impatto sulle organizzazioni. Hanno portato a multe di conformità (53% delle organizzazioni), diminuzione delle nuove vendite (47%), cambiamento nella leadership senior (24%) e cause legali (29%) - i risultati più alti in tutti i tipi di incidenti. Gli incidenti di sicurezza che hanno comportato il furto di dati privilegiati hanno influito negativamente sulla valutazione aziendale per il 33% delle organizzazioni, mentre il furto di dati da parte degli hacker ha portato all'abbandono dei clienti e alla perdita del vantaggio competitivo (35% ciascuno). Infine, gli errori umani o gli incidenti che hanno comportato perdite accidentali di dati hanno obbligato il 62% degli intervistati ad aumentare il budget di spesa per colmare le lacune di sicurezza associate.

Conseguenze della violazione dei dati cloud per tipo di identificazione

	Attacchi mirati all'infrastruttura cloud	Attacchi di phishing	Ransom ware	Compromissione sulla catena di approvvigionamento	Furto di dati privilegiati	Furto di dati da hacker	Perdita accidentale di dati	Compromissione dell'account	Perdita di dati
Nessun problema	23%	35%	27%	12%	11%	10%	13%	21%	17%
Spese non pianificate per colmare le lacune di sicurezza	51%	50%	58%	47%	59%	60%	62%	56%	50%
Ammende di conformità	33%	17%	24%	53%	26%	40%	29%	26%	36%
Perdita di vantaggio competitivo	26%	12%	15%	29%	26%	35%	22%	21%	25%
Abbandono dei clienti	28%	11%	15%	18%	15%	35%	22%	14%	25%
Diminuzione delle nuove vendite	26%	7%	15%	47%	19%	30%	16%	23%	17%
Diminuzione della valutazione aziendale	23%	10%	13%	24%	33%	25%	16%	14%	25%
Cambiamento nella leadership senior	16%	9%	9%	24%	15%	20%	18%	16%	19%
Cause	12%	5%	7%	29%	11%	25%	4%	9%	11%

Rilevamento e risposta agli incidenti

Abbiamo chiesto ai nostri intervistati di stimare quanto tempo le loro organizzazioni avevano bisogno per scoprire e rispondere agli incidenti di sicurezza cloud che hanno subito negli ultimi 12 mesi.

Tempo medio di rilevamento

Siamo rimasti piuttosto sorpresi dalla rapidità con cui le organizzazioni sono state in grado di individuare gli incidenti - nella maggior parte dei casi - gli intervistati avevano bisogno solo di ore per rilevare l'incidente, il che in realtà non è così male. Phishing e ransomware erano i più facili da rilevare; L'86% lo ha individuato in pochi minuti o ore. Le organizzazioni sono state anche in grado di individuare attacchi mirati all'infrastruttura cloud abbastanza rapidamente (83% in pochi minuti o ore).

Tuttavia, il furto di dati da parte di addetti ai lavori e la perdita accidentale di dati sono molto più problematici. Secondo la nostra ricerca, il 50% degli intervistati ha avuto bisogno di giorni, settimane o mesi per rilevare il furto di dati privilegiati e il 61% ha ammesso che ci sono voluti giorni o settimane per individuare perdite accidentali di dati.

Alcune organizzazioni hanno anche faticato a scoprire il furto di dati da parte degli hacker. È l'unico tipo di incidente che ha richiesto anni per essere rilevato; Lo ha riferito il 5% degli intervistati.

È importante notare che tutti gli incidenti di **cui abbiamo appena parlato sono** associati ai dati e alla loro **sovraesposizione.** Le organizzazioni devono assicurarsi di poter tenere traccia di ciò che gli utenti stanno facendo con i dati e ottenere avvisi se è accessibile o condiviso in modo improprio per poter agire immediatamente.

Time per rilevare incidenti di sicurezza nel cloud

	Minuti	Ore	Giorni	Settimane	Mesi	Anni
Attacchi mirati all'infrastruttura cloud	32%	51%	15%	2%	0%	0%
Attacchi di phishing	44%	42%	13%	1%	0%	0%
Ransomware o altri attacchi malware	35%	51%	9%	5%	0%	0%
Compromissione sulla catena di approvvigionamento	23%	53%	18%	0%	6%	0%
Furto di dati da parte di addetti ai lavori	23%	27%	27%	19%	4%	0%
Furto di dati da parte di hacker	16%	53%	21%	0%	5%	5%
Perdita accidentale di dati	16%	23%	47%	14%	0%	0%
Compromissione dell'account	20%	49%	24%	7%	0%	0%
Perdita di dati	23%	42%	29%	6%	0%	0%

Factoidi

- Il 10% delle piccole organizzazioni ha richiesto mesi per rilevare il furto di dati da parte degli addetti ai lavori.
- Il 25% delle organizzazioni di medie dimensioni ha avuto bisogno di anni per rilevare il furto di dati da parte degli hacker.
- Il 10% delle aziende enterprise ha impiegato mesi per rilevare la compromissione della catena di approvvigionamento.

Impatto della classificazione dei dati e del controllo delle attività sulla velocità di rilevamento

La classificazione dei dati consente alle organizzazioni di contrassegnare ogni file sensibile in modo che possano migliorare il controllo sulla posizione in cui vengono archiviati i dati e su chi può accedervi. Questa tecnologia ha migliorato significativamente la velocità di rilevamento per quattro tipi di incidenti: furto di dati da parte di addetti ai lavori, furto di dati da parte di hacker, perdita accidentale di dati e perdita di dati. Le organizzazioni che hanno classificato i loro dati sono state in grado di individuare questi incidenti in minuti o ore, mentre altre organizzazioni hanno avuto bisogno di giorni, settimane o persino mesi.

Impatto della classificazione dei dati sulla velocità di rilevamento degli incidenti

	Dati classificati	Dati non classificati
Furto di dati da parte di addetti ai lavori	58% scoperto in minuti o ore	Scoperto al 55% in giorni o settimane
Furto di dati da parte di hacker	75% scoperto in minuti o ore	Scoperto al 60% in giorni o mesi

Perdita accidentale di dati	Scoperto al 60% in minuti o ore	Scoperto l'85% in giorni o settimane
Perdita di dati	Scoperto il 53% in poche ore	Scoperto il 56% in pochi giorni

Il controllo dell'attività dell'utente ha migliorato i tempi di rilevamento in modo simile per cinque tipi di incidenti: compromissione della catena di approvvigionamento, furto di dati da parte di addetti ai lavori, furto di dati da parte di hacker, perdita accidentale di dati e compromissione dell'account.

Impatto del controllo dell'attività dell'utente sulla velocità di rilevamento degli incidenti

	Con controllo dell'attività dell'utente	Senza controllo dell'attività dell'utente
Compromissione sulla catena di approvvigionamento	75% scoperto in minuti o ore	69% scoperto in giorni o settimane
Furto di dati da parte di addetti ai lavori	64% scoperto in minuti o ore	Scoperto al 58% in giorni, settimane o mesi
Furto di dati da parte di hacker	78% scoperto in minuti o ore	Scoperto il 66% in settimane o mesi
Perdita accidentale di dati	58% scoperto in minuti o ore	Scoperto al 70% in giorni o settimane
Compromissione dell'account	76% scoperto in minuti o ore	Scoperto il 67% in giorni o settimane

È consigliabile implementare entrambe le tecnologie per migliorare i tempi di individuazione degli incidenti e mitigare i rischi.

Factoidi

- Le organizzazioni che classificano i dati e controllano l'attività degli **utenti hanno 1,5 volte più probabilità** di individuare incidenti in pochi minuti.

Tempo medio di risposta

La gestione delle conseguenze di un incidente di sicurezza richiede alle organizzazioni più tempo del rilevamento degli incidenti. I migliori risultati sono stati per il phishing: l'82% delle organizzazioni risolve l'incidente in pochi minuti o ore. Successivamente sono stati mirati attacchi e perdita di dati, che il69% ha risolto in minuti o ore.

All'altra estremità dello spettro c'erano incidenti legati a perdite accidentali di dati, che il 51% delle organizzazioni aveva bisogno di giorni, settimane, mesi o persino anni per risolvere. Il 43% degli intervistati aveva bisogno di giorni, settimane o mesi per rispondere al furto di dati dall'interno e il 40% aveva bisogno di atrettanto tempo per rispondere agli attacchi hacker.

Vorremmo anche sottolineare che il 15% delle organizzazioni ha avuto bisogno di mesi per

gestire il furto di dati da parte degli hacker, che è il peggior risultato in tutti i tipi di incidenti che abbiamo analizzato.
È interessante notare **che il furto di dati e la perdita accidentale di dati hanno richiesto il** tempo **più lungo sia per rilevare che per rispondere.** Le organizzazioni devono assicurarsi di poter identificare tempestivamente l'accesso non autorizzato ai dati o la condivisione dei dati e sviluppare processi di risposta agli effetti per ridurre al minimo i danni, ridurre i costi delle violazioni dei dati e trovare e correggere la causa principale per prevenire incidenti simili in futuro.

Tempi di risposta agli incidenti di sicurezza nel cloud	Minuti	Ore	Giorni	Settimane	Mesi	Anni
Attacchi mirati all'infrastruttura cloud	20%	48%	20%	10%	2%	0%
Attacchi di phishing	41%	41%	15%	2%	1%	0%
Ransomware o altri attacchi malware	26%	39%	27%	6%	2%	0%
Compromissione sulla catena di approvvigionamento	18%	46%	24%	12%	0%	0%
Furto di dati da parte di addetti ai lavori	26%	31%	27%	12%	4%	0%
Furto di dati da parte di hacker	15%	45%	20%	5%	15%	0%
Perdita accidentale di dati	9%	40%	33%	14%	2%	2%
Compromissione dell'account	29%	34%	27%	5%	5%	0%
Perdita di dati	19%	49%	20%	6%	6%	0%

Factoidi
- Il 20% delle piccole organizzazioni ha speso mesi per risolvere il furto di dati da parte degli hacker.
- Il 25% delle organizzazioni di medie dimensioni ha avuto bisogno di settimane per risolvere il furto di dati da parte di hacker o dipendenti.
- Il 18% delle grandi imprese ha perso mesi per risolvere il furto di dati da parte degli hacker e il 13% ha avuto bisogno dello stesso tempo per il furto di dati da parte degli addetti ai lavori.

Impatto della classificazione dei dati e del controllo delle attività sulla velocità di risposta

La classificazione dei dati ha permesso all'organizzazione di rispondere più rapidamente a cinque tipidi incidenti: ransomware, furto di dati da parte di addetti ai lavori, furto di dati da parte di hacker, perdita accidentale di dati e perdita di dati. La classificazione dei dati consente alle organizzazioni di determinare quali incidenti coinvolgono dati critici e necessitano di un'attenzione urgente,in modo che possano adottare iniziative di recupero dei dati. Di conseguenza, le organizzazioni con la classificazione dei dati in atto sono state in

grado di risolvere questi incidenti in minuti o ore, mentre altre organizzazioni hanno avuto bisogno di giorni, settimane o mesi.

Impatto della classificazione dei dati sulla velocità di risposta agli incidenti

	Dati classificati	Dati non classificati
Ransomware o altri attacchi malware	Risolto al 72% in minuti o ore	Risolto al 50% in giorni o settimane
Furto di dati da parte di addetti ai lavori	Risolto al 66% in minuti o ore	Risolto al 55% in giorni o settimane
Furto di dati da parte di hacker	Risolto al 67% in minuti o ore	Risolto per l'80% in giorni, settimane o mesi
Perdita accidentale di dati	Risolto al 70% in minuti o ore	Risolto al 63% in giorni o settimane
Perdita di dati	Risolto al 74% in minuti o ore	Risolto al 64% in giorni o settimane

Il controllo dell'attività degli utenti ha migliorato la velocità di risposta per sette tipi di incidenti: attacchi mirati, ransomware, furto di datida parte di addetti ailavori, furto di dati da parte di hacker,perdita accidentale di dati, compromessa dell'account e perdita di dati. Avere un audit trail ha permesso alla maggior parte delle organizzazioni di rispondere a questi incidenti in pochi minuti o ore, mentre le altre organizzazioni richiedevano giorno, settimane o mesi.

Impatto del controllo dell'attività dell'utente sulla velocità osulla risposta agli incidenti

	Con controllo dell'attività dell'utente	Senza controllo dell'attività dell'utente
Attacchi mirati all'infrastruttura cloud	Risolto al 75% in minuti o ore	Risolto al 63% in giorni o settimane
Ransomware e altri malware	Risolto al 72% in minuti o ore	Risolto al 59% in giorni o settimane
Furto di dati da parte di addetti ai lavori	Risolto al 73% in minuti o ore	Risolto al 61% in giorni o settimane
Furto di dati da parte di hacker	Risolto al 60% in minuti o ore	Risolto al 74% in giorni o settimane
Perdita accidentale di dati	Risolto al 55% in minuti o ore	Risolto al 59% in giorni o settimane

Compromissione dell'account	Risolto al 65% in minuti o ore	Risolto al 60% in giorni, settimane o mesi
Perdita di dati	Risolto al 61% in minuti o ore	Risolto al 70% in giorni o settimane

Sfide per la sicurezza dei dati cloud

Le principali sfide in materia di sicurezza dei dati nominate dagli intervistati sono state la mancanza di personale IT (52%), la mancanza di budget (47%) e mancanza di competenze in materia di sicurezza cloud (44%). La negligenza dei dipendenti è stata nominata dal 38% degli intervistati, ma solo il 17% ha scelto come problema comportamenti volutamente dannosi degli addetti ai lavori. Questa scoperta riflette la realtà, dal momento che solo il 10% delle organizzazioni ha segnalato il furto di dati da parte dei dipendenti.

Un partecipante su quattro ha affermato che i dirigenti aziendali hanno esercitato pressioni sul team IT per promuovere una rapida trasformazione o crescita digitale a scapito della sicurezza dei dati. Questo problema è particolarmente critico per i **CISO: il 48% nota che** il desiderio **di crescita dell'azienda** ostacola gli sforzi per **garantire la sicurezza dei dati nel cloud.**

Le principali sfide per garantire la sicurezza dei dati nel cloud

Il team IT/sicurezza è a corto di personale	52%
Mancanza di budget	47%
Mancanza di esperienza sulla sicurezza del cloud	44%
Negligenza dei dipendenti	38%
Mancanza di visibilità sui dati sensibili nel cloud	28%
Pressione aziendale per una rapida digitalizzazione, trasformazione o crescita	26%
Strumenti e processi incoerenti a causa di più carichi di lavoro su diverse piattaforme cloud	25%
Azioni dannose da parte dei dipendenti	17%
Incapacità di fissare i punti finali	16%

Le preoccupazioni per i CISO

- 73% - Carenza di personale IT/di sicurezza
- 48% - Pressione del top management per una rapida digitalizzazione, trasformazione o crescita
- 41% - Negligenza dei dipendenti

Le preoccupazioni per i CIO

- 68% - Carenza di budget
- 48% - Carenza di personale informatico
- 48% - Carenza di competenze

Le stesse sfide erano nei primi tre posti indipendentemente dalle dimensioni dell'organizzazione. Ciò che ci ha sorpreso è che metà delle organizzazioni aziendali ha elencato la mancanza di conoscenze sulla sicurezza cloud come una sfida per la sicurezza del cloud. Chiaramente, le loro infrastrutture complesse e l'uso più ampio delle tecnologie cloud richiedono professionisti IT con competenze avanzate; se sai come gestirlo e stai cercando un lavoro, sai cosa fare.

Principali sfide per garantire la sicurezza dei dati nel cloud in base alle dimensioni dell'organizzazione

	Piccola	Media	Grande
Il team IT/sicurezza è a corto di personale	45%	62%	47%
Mancanza di esperienza nella sicurezza del cloud	40%	41%	51%
Mancanza di budget	44%	48%	48%
Negligenza dei dipendenti	40%	33%	41%
Azioni dannose da parte dei dipendenti	18%	16%	16%
Strumenti e processi incoerenti a causa di più carichi di lavoro su diverse piattaforme cloud	27%	24%	22%
Incapacità di fissare i punti finali	14%	15%	18%
Mancanza di visibilità sui dati sensibili nel cloud	27%	31%	26%
Pressione aziendale per una rapida digitalizzazione, trasformazione o crescita	26%	22%	31%

Elenco di controlli per la sicurezza dei dati cloud

I controlli di sicurezza cloud più popolari che le organizzazioni hanno già nel loro arsenale sono la crittografia (62%), il controllo dell'attività degli utenti (58%) formazione dei dipendenti (58%). Le misure sono state anche elencate come i principali controlli per la sicurezza del cloud nel nostro sondaggio del 2019. È interessante notare che nel 2019, il 37% degli intervistati ha dichiarato di aver adottato o migliorato strategie di backup dei dati; nel 2020, il 58% delle organizzazioni afferma di fare già backup e il 24% prevede di farlo in futuro. Inoltre, la stragrande maggioranza degli intervistati classifica già i dati sensibili nel cloud (49%) o pianifica l'attuazione di questo controllo in futuro (31%). La misura più impopolare è l'utilizzo di broker di sicurezza di accesso cloud (CASB) - il 40% non prevede affatto di implementare questa tecnologia.

Dati di unclouding (de-clouding)

- Nella ricerca dell'anno scorso, abbiamo notato che non tutte le organizzazioni erano contente delle loro infrastrutture cloud. Circa il 48% degli intervistati si era spostato o aveva pianificato di spostare i dati sensibili in locale per migliorare la sicurezza dei dati. Nel 2020, nonostante l'impulso nell'adozione del cloud a causa della necessità di supportare il lavoro remoto, la quota di organizzazioni che hanno già rimosso i dati sensibili dal cloud o che stanno pianificando di farlo è aumentata al 62%.
- Le aziende di grandi dimensioni sono più propense a rimuovere i dati dal cloud; Il 40% ha già rimosso alcuni dei dati sensibili e il 30% prevede di farlo. Al contrario, quasi la metà delle organizzazioni di medie dimensioni non ha in programma di rimuovere dati sensibili dal cloud.

Misure per proteggere i dati nel cloud

	Già fatto	Pianificare di farlo	Non ho intenzione di farlo
Crittografia	62%	25%	12%
Controllo dell'attività dell'utente	58%	29%	12%
Backup cloud	58%	24%	18%
Formazione dei dipendenti	58%	31%	11%
Autenticazione a più fattori	57%	31%	13%
Revisione dei diritti di accesso (attestazione)	54%	34%	12%
Classificazione dei dati	49%	31%	20%
Rimuovere i dati sensibili dal cloud	35%	27%	38%
Broker di sicurezza per l'accesso al cloud	27%	33%	40%

Misure per proteggere i dati nel cloud in base alle dimensioni dell'organizzazione

Piccola

	Già fatto	Pianificare di farlo	Non ho intenzione di farlo
Backup cloud	58%	24%	18%
Autenticazione a più fattori	55%	30%	15%
Formazione dei dipendenti	54%	35%	11%
Crittografia	52%	33%	15%

Revisione dei diritti di accesso (attestazione)	49%	35%	16%
Controllo dell'attività dell'utente	45%	41%	14%
Classificazione dei dati	43%	30%	27%
Rimuovere i dati sensibili dal cloud	36%	25%	39%
Broker di sicurezza per l'accesso al cloud	26%	25%	49%

Media

	Già fatto	Pianificare di farlo	Non ho intenzione di farlo
Crittografia	62%	24%	14%
Backup cloud	58%	19%	23%
Formazione dei dipendenti	58%	29%	13%
Controllo dell'attività dell'utente	57%	29%	14%
Autenticazione a più fattori	53%	31%	16%
Revisione dei diritti di accesso (attestazione)	50%	39%	11%
Classificazione dei dati	44%	37%	19%
Rimuovere i dati sensibili dal cloud	28%	26%	46%
Broker di sicurezza per l'accesso al cloud	26%	37%	38%

Grande

	Già fatto	Pianificare di farlo	Non ho intenzione di farlo
Controllo dell'attività dell'utente	74%	18%	8%
Crittografia	73%	20%	7%
Revisione dei diritti di accesso (attestazione)	63%	28%	9%
Autenticazione a più fattori	62%	31%	7%
Formazione dei dipendenti	61%	29%	10%
Classificazione dei dati	59%	26%	15%
Backup cloud	58%	29%	13%
Rimuovere i dati sensibili dal cloud	40%	30%	30%
Broker di sicurezza per l'accesso al cloud	29%	38%	33%

Factoidi

- Il 92% delle organizzazioni di grandi dimensioni controlla già l'attività degli utenti o prevede di farlo per proteggere i dati nel cloud. È il principale controllo di sicurezza cloud nel settore enterprise.
- Il 64% dei CISO classifica i dati nel cloud e il 27% prevede di implementare questo controllo in futuro.
- Il 100% dei CIO conduce già una formazione sulla sicurezza dei dipendenti o prevede di farlo.

Budget per la sicurezza informatica e cloud

Quando abbiamo chiesto alle organizzazioni come la pandemia ha cambiato i loro budget per la sicurezza informatica, solo l'11% ha detto che il loro budget per la sicurezza informatica è diminuito; il 24% ha riferito che è cresciuto. Più di un terzo (36%) delle organizzazioni affermano che la pandemia li ha costretti a cambiare le loro priorità di sicurezza pur rimanendo entro il budget esistente.

Le aziende enterprise sono state tra le fortunate: il 30% delle grandi organizzazioni ha segnalato un aumento della spesa per la sicurezza informatica, che è il risultato più alto rispetto ad altre dimensioni organizzative.

Impatto della pandemia sulla spesa per la cybersecurity

Budget è rimasto lo stesso ma le priorità sono cambiate	36%
Budget aumentato	24%
Budget e priorità sono rimaste le stesse	21%
Budget diminuito	11%

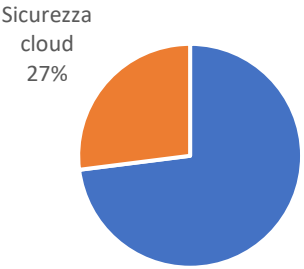
Impatto della pandemia sulla spesa per la sicurezza informatica in base alle dimensioni dell'organizzazione

	Piccola	Media	Grande
Budget è rimasto lo stesso ma le priorità sono cambiate	39%	35%	34%
Budget aumentato	17%	24%	30%
Budget e priorità sono rimaste le stesse	26%	20%	16%
Budget diminuito	8%	14%	12%

Factoidi

- I CISO hanno dovuto rivedere molto spesso le priorità in materia di sicurezza informatica a causa della pandemia.

Distribuzione del budget per la sicurezza informatica



Indipendentemente dalle dimensioni, le organizzazioni hanno riferito di aver allocato più di un quarto del loro budget totale per la sicurezza informatica alla sicurezza cloud quest'anno.

Consigli

Controllare continuamente l'attività dell'utente e classificare i dati per velocizzare il rilevamento degli incidenti.
La stragrande maggioranza degli intervistati che controllano l'attività degli utenti e classificano i propri dati sono stati in grado di rilevare incidenti in minuti o ore, mentre le altre organizzazioni hanno avuto bisogno di giorni, settimane o mesi. In effetti, avere un'ampia visibilità su quali dati l'organizzazione archivia e cosa sta accadendo intorno ad esso non solo accelera il rilevamento dei problemi, ma consente alle organizzazioni di trovare e correggere le lacune di sicurezza prima di subire una violazione.

Automatizzare e/o delegare per fare di più con meno.
Le tre principali sfide delle organizzazioni per proteggere i dati nel cloud risiedono nella mancanza di personale, risorse finanziarie e competenze. Queste difficoltà costringono i team di sicurezza a operare in modalità reattiva piuttosto che proattiva, quindi l'organizzazione è più a rischio di incorrere in incidenti e di non essere in grado di rilevarli e rispondere prontamente. Inoltre, anche se gli affari si stanno basando sempre di più sull'IT sulla scia della pandemia e degli ordini state-a-casa, la maggior parte dei team IT non ha aumentato il budget per la sicurezza. Di conseguenza, devono destreggiarsi tra risorse sempre limitate per far passare l'azienda attraverso un panorama di minacce più sofisticato, in modo da continuare a vivere nella realtà del "nuovo giorno, nuova violazione". Per superare la sfida delle risorse limitate, consigliamo alle organizzazioni di esternalizzare le attività IT agli MSSP e/o di investire in strumenti che automatizzano le attività IT di routine.
Attenzione agli attacchi della catena di approvvigionamento.
Gli incidenti che includevano la compromissione della catena di approvvigionamento hanno avuto il maggiore impatto sulle organizzazioni; avevano maggiori probabilità di comportare multe di conformità, diminuzione delle nuove vendite, cambiamento nella leadership senior e persino cause legali rispetto a qualsiasi altro tipo di incidente. Per evitare queste conseguenze, l'organizzazione deve prestare attenzione agli elementi meno sicuri nella pro-

pria rete di approvvigionamento. Le procedure consigliate per la sicurezza per mitigare questi rischi includono la segmentazione della rete, il controllo continuo per le attività dannose in tutto l'ambiente e alert di azioni sospette. Le organizzazioni devono chiedere ai partner di dimostrare di adottare tutte le misure di sicurezza necessarie, come audit di terze parti o conferma dell'utilizzo di determinati servizi e/o strumenti di sicurezza. Le organizzazioni possono anche limitare la loro responsabilità in base ai loro contratti con i partner e renderli responsabili nel caso in cui si registrino violazioni dei dati.

Pensa al business quando valuti i rischi per la sicurezza.

Per promuovere la sicurezza adattiva e garantire un'adeguata attenzione ai rischi reali, i professionisti IT devono identificare le coppie minaccia/vulnerabilità e determinare le conseguenze alle quali espongono l'azienda. La nostra ricerca ha dimostrato che è di fondamentale importanza guardare oltre le conseguenze classiche, come le spese non pianificate o le multe di conformità. Alcuni tipi di minacce (ad esempio la compromissione della catena di approvvigionamento e il furto di dati) possono avere esiti molto più gravi che influenzano il benessere finanziario dell'azienda, come un impatto negativo sulla valutazione o sui tassi di abbandono. Pertanto, quando si valutano i rischi per la sicurezza. si consiglia ai responsabili della sicurezza di includere le conseguenze a lungo termine delle violazioni dei dati sull'azienda nel suo complesso.

Appendice 1: Verticali

Finanza

Il 53% delle organizzazioni finanziarie archivia i dati dei clienti nel cloud e il 35% archivia i dati finanziari.

I 3 principali incidenti di sicurezza dei dati nel cloud

Attacchi di phishing	26%
Attacchi mirati all'infrastruttura cloud	22%
Ransomware o altri attacchi malware	15%

I primi 3 risultati della violazione dei dati

Spese non pianificate per colmare le lacune di sicurezza	20%
Ammende di conformità	19%
Abbandono dei clienti	17%

È ora di rilevare gli incidenti di sicurezza più comuni nel cloud

	Minuti	Ore	Giorni	Settimane	Mesi	Anni
Attacchi mirati all'infrastruttura cloud	17%	42%	21%	20%	0%	0%
Attacchi di phishing	58%	26%	16%	0%	0%	0%
Ransomware o altri attacchi malware	23%	49%	28%	0%	0%	0%

L'89% delle organizzazioni finanziarie ha avuto bisogno di mesi per scoprire il furto di dati privilegiati.

È ora di risolvere gli incidenti di sicurezza più comuni nel cloud

	Minuti	Ore	Giorni	Settimane	Mesi	Anni
Attacchi mirati all'infrastruttura cloud	28%	34%	21%	17%	0%	0%
Attacchi di phishing	41%	45%	14%	0%	0%	0%
Ransomware o altri attacchi malware	27%	46%	26%	0%	0%	0%

Il 52% delle organizzazioni finanziarie ha avuto bisogno di settimane per riprendersi dalla compromissione della catena di approvvigionamento.

Le 3 principali sfide in materia di sicurezza informatica

Team IT/sicurezza con personale	59%
Mancanza di esperienza nella sicurezza del cloud	44%
Negligenza dei dipendenti	37%

Le 3 principali misure di sicurezza

	Già fatta	Pianificare di farlo	Non ho intenzione di farlo
Formazione dei dipendenti	77%	23%	0%
Controllo dell'attività dell'utente	70%	22%	7%
Revisione dei diritti di accesso (attestazione)	65%	35%	0%

Il 37% delle organizzazioni finanziarie prevede di iniziare a classificare i dati e il 40% prevede di implementare l'autenticazione a più fattori (AMF).

Distribuzione del budget per la sicurezza informatica

In media, le organizzazioni finanziarie assegnano il 34% del loro budget per la sicurezza informatica alla sicurezza cloud.

Istruzione

Il 48% delle organizzazioni educational archivia i dati dei dipendenti nel cloud, mentre il 30% memorizza i dati degli studenti.

I 3 principali incidenti di sicurezza dei dati nel cloud

Attacchi di phishing	60%
Compromissione dell'account	33%
Ransomware o altri attacchi malware	27%

I primi 3 risultati della violazione dei dati

Spese non pianificate per colmare le lacune di sicurezza	33%
Abbandono dei clienti	10%
Diminuzione della valutazione aziendale	9%

È ora di rilevare gli incidenti di sicurezza più comuni nel cloud

	Minuti	Ore	Giorni	Settimane	Mesi	Anni
Attacchi di phishing	44%	33%	23%	0%	0%	0%
Compromissione dell'account	18%	54%	28%	0%	0%	0%
Ransomware o altri attacchi malware	32%	19%	49%	0%	0%	0%

Il 93% delle organizzazioni educational ha avuto bisogno di giorni o settimane per scoprire perdite accidentali didati.

È ora di risolvere gli incidenti di sicurezza più comuni nel cloud

	Minuti	Ore	Giorni	Settimane	Mesi	Anni
Attacchi di phishing	29%	35%	36%	0%	0%	0%
Compromissione dell'account	34%	18%	48%	0%	0%	0%
Ransomware o altri attacchi malware	21%	46%	33%	0%	0%	0%

Il 33% delle organizzazioni educational aveva bisogno di settimane per riprendersi da perdite accidentali di dati.

Le 3 principali sfide in materia di sicurezza informatica

TeamIT/sicurezza con personale	53%
Mancanza di esperienza nella sicurezza del cloud	52%
Mancanza di bilancio	49%

Le 3 principali misure di sicurezza

	Già fatto	Pianificare di farlo	Non ho intenzione di farlo
Backup cloud	54%	25%	21%
Controllo dell'attività dell'utente	53%	20%	27%
Revisione dei diritti di accesso (attestazione)	53%	27%	20%

Il 40% delle organizzazioni educational prevede di distribuire la classificazione dei dati e il 36% distribuirà l'autenticazione a più fattori.

Distribuzione del budget per la sicurezza informatica

In media, le organizzazioni educative assegnano il 24% del loro budget per la sicurezza informatica alla sicurezza cloud.

Pubblica Amministrazione

Il 50% delle agenzie governative non memorizza dati nel cloud. Il 29% memorizza i dati dei dipendenti e il 25% memorizza informazioni finanziarie.

I 3 principali incidenti di sicurezza dei dati nel cloud

Attacchi di phishing	39%
Perdita accidentale di dati	24%
Attacchi mirati all'infrastruttura cloud	22%

I primi 3 risultati della violazione dei dati

Spese non pianificate per colmare le lacune di sicurezza	28%
Abbandono dei clienti	13%
Cambiamento nella leadership senior	11%

È ora di rilevare gli incidenti di sicurezza più comuni nel cloud

	Minuti	Ore	Giorni	Settimane	Mesi	Anni
Attacchi di phishing	33%	67%	0%	0%	0%	0%
Perdita accidentale di dati	31%	42%	27%	0%	0%	0%
Attacchi mirati all'infrastruttura cloud	12%	86%	2%	0%	0%	0%

Il 34% delle agenzie governative ha trascorso settimane a scoprire la perdita di dati.

È ora di risolvere gli incidenti di sicurezza più comuni nel cloud

	Minuti	Ore	Giorni	Settimane	Mesi	Anni
Attacchi di phishing	29%	67%	4%	0%	0%	0%
Perdita accidentale di dati	9%	25%	32%	11%	23%	0%
Attacchi mirati all'infrastruttura cloud	8%	47%	12%	14%	19%	0%

Il 67% delle agenzie governative ha avuto bisogno di mesi per riprendersi dalla compromissione del conto e dalla perdita di dati.

Le 3 principali sfide in materia di sicurezza informatica

TeamIT/sicurezza con personale	65%
Negligenza dei dipendenti	59%
Mancanza di bilancio	53%

Le 3 principali misure di sicurezza

	Già fatto	Pianificare di farlo	Non ho intenzione di farlo
Controllo dell'attività dell'utente	65%	24%	12%
Classificazione dei dati	56%	19%	25%
Revisione dei diritti di accesso (attestazione)	53%	29%	18%

Il 41% delle agenzie governative prevede di implementare la formazione dei dipendenti e la stessa percentuale prevede di implementare la crittografia.

Distribuzione del budget per la sicurezza informatica

In media, le agenzie governative assegnano il 14% del loro budget per la sicurezza informatica alla sicurezza cloud.

Sanità

Il 61% delle organizzazioni sanitarie archivia i dati dei clienti nel cloud e il 54% archivia i record sanitari personali.

I 3 principali incidenti di sicurezza dei dati nel cloud

Attacchi di phishing	44%
Ransomware o altri attacchi malware	39%
Furto di dati da parte di addetti ai lavori	35%

I primi 3 risultati della violazione dei dati

Spese non pianificate per colmare le lacune di sicurezza	24%
Ammende di conformità	23%
Cause	11%

È ora di rilevare gli incidenti di sicurezza più comuni nel cloud

	Minuti	Ore	Giorni	Settimane	Mesi	Anni
Attacchi di phishing	49%	38%	13%	0%	0%	0%
Ransomware o altri attacchi malware	42%	43%	15%	0%	0%	0%
Furto di dati da parte di addetti ai lavori	16%	32%	24%	28%	0%	0%

Il 32% delle organizzazioni sanitarie ha avuto bisogno di giorni per scoprire perdite accidentali di dati e compromettere la catena di approvvigionamento.

È ora di risolvere gli incidenti di sicurezza più comuni nel cloud

	Minuti	Ore	Giorni	Settimane	Mesi	Anni
Attacchi di phishing	37%	38%	25%	0%	0%	0%
Ransomware o altri attacchi malware	5%	67%	28%	0%	0%	0%
Furto di dati da parte di addetti ai lavori	4%	53%	43%	0%	0%	0%

Il 22% delle organizzazioni sanitarie ha avuto bisogno di settimane per riprendersi da attacchi mirati all'infrastruttura cloud.

Le 3 principali sfide in materia di sicurezza informatica

Mancanza di bilancio	61%
Il team IT/sicurezza è a corto di personale	56%
Negligenza dei dipendenti	39%

Le 3 principali misure di sicurezza

	Già fatto	Pianificare di farlo	Non ho intenzione di farlo
Crittografia	78%	17%	6%
Revisione dei diritti di accesso (attestazione)	75%	13%	13%
Formazione dei dipendenti	65%	29%	6%

Il 35% delle organizzazioni sanitarie prevede di implementare l'autenticazione a più fattori, mentre il 31% inizierà a controllare l'attività degli utenti.

Distribuzione del budget per la sicurezza informatica

In media, le organizzazioni sanitarie assegnano il 22% del loro budget per la sicurezza informatica alla sicurezza cloud.

Appendice 2: Italia

Il 47% delle organizzazioni Italiane archivia i dati dei clienti nel cloud.

I 3 principali incidenti di sicurezza dei dati nel cloud

Attacchi di phishing	38%
Perdita di dati	31%
Attacchi mirati all'infrastruttura cloud	23%

I primi 3 risultati della violazione dei dati

Abbandono dei clienti	17%
Ammende di conformità	11%
Perdita di vantaggio competitivo	8%

È ora di rilevare gli incidenti di sicurezza più comuni nel cloud

	Minuti	Ore	Giorni	Settimane	Mesi	Anni
Attacchi di phishing	76%	17%	7%	0%	0%	0%
Perdita di dati	48%	25%	27%	0%	0%	0%
Attacchi mirati all'infrastruttura cloud	33%	62%	5%	0%	0%	0%

Il 35% delle organizzazioni italiane ha avuto bisogno di settimane per scoprire la compromissione dell'account.

È ora di risolvere gli incidenti di sicurezza più comuni nel cloud

	Minuti	Ore	Giorni	Settimane	Mesi	Anni
Attacchi di phishing	54%	32%	14%	0%	0%	0%
Perdita di dati	11%	85%	4%	0%	0%	0%
Attacchi mirati all'infrastruttura cloud	24%	58%	18%	0%	0%	0%

Il 52% delle organizzazioni italiane ha avuto bisogno di settimane per riprendersi da perdite accidentali di dati.

Le 3 principali sfide in materia di sicurezza informatica

Negligenza dei dipendenti	75%
Il team IT/sicurezza è a corto di personale	56%
Mancanza di visibilità sui dati sensibili nel cloud	54%

Le 3 principali misure di sicurezza

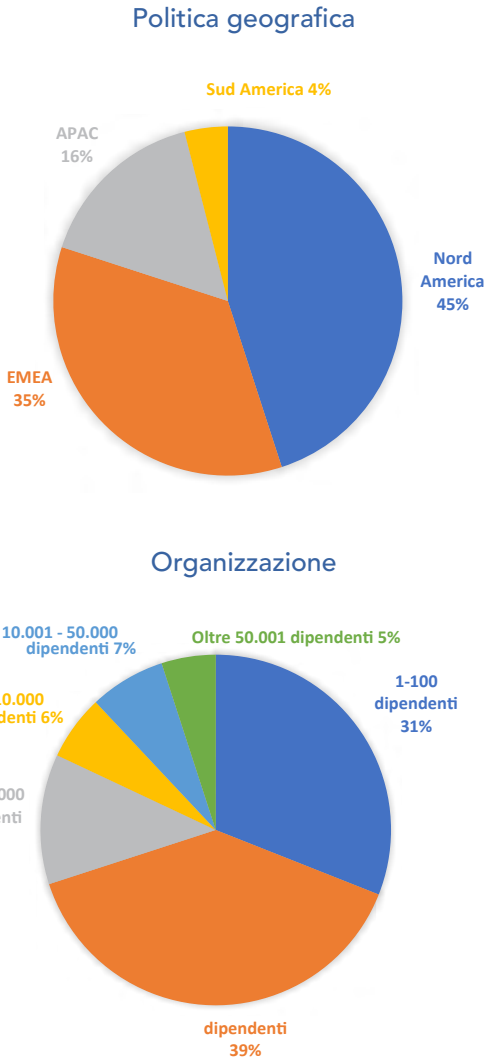
	Già fatto	Pianificare di farlo	Non ho intenzione di farlo
Controllo dell'attività dell'utente	54%	23%	23%
Crittografia	51%	32%	17%
Revisione dei diritti di accesso (attestazione)	50%	36%	14%

Il 58% delle organizzazioni italiane prevede di implementare l'autenticazione a più fattori, mentre il 42% prevede di implementare la classificazione dei dati.

Distribuzione del budget per la sicurezza informatica

In media, le organizzazioni italiane assegnano il 36% del loro budget per la sicurezza informatica alla sicurezza cloud.

Appendice 3: Indagine demografica



Le migliori industrie

Tecnologia/ Servizi	11%
Produzione	10%
Tecnologia/software	10%
Settore bancario efinanziario	9%
Istruzione	7%
Sanità	6%
Consulenza	6%
Governo	6%
Servizi	5%
Vendita al dettaglio e all'ingrosso	4%
Assicurazione	3%
Energia	3%
Tecnologia/hardware	3%
Telecomunicazioni	3%
Intrattenimento e assicurazione	3%

Top job titles

Amministratore IT/sistemi	30%
Responsabile IT	22%
Direttore CIO/IT	10%
CISO	9%
Consulente	8%
Responsabile dell'audit IT	2%
Altro	19%

Informazioni su questo report

Il report è stato presentato da Netwrix Research Lab, che conduce sondaggi di settore tra i professionisti IT di tutto il mondo per scoprire importanti cambiamenti e tendenze.

Business Continuity & Cyber Security: la necessità di un approccio convergente

[A cura di Federica Maria Rita Livelli]

Scenario

Ammesso che ci fosse stato bisogno di una conferma, le quasi 600 risposte internazionali al sondaggio pubblicato lo scorso ottobre 2020 dal *Business Continuity Institute (BCI), UK* evidenziano come un sano mix di Business Continuity, IT, Information & Cyber Security - senza dimenticare Risk Management e altre funzioni di security - possa contribuire ad aumentare la resilienza organizzativa e a sviluppare un necessario approccio collaborativo/olistico necessario per affrontare le sfide dello scenario contingente in cui ci troviamo ad operare e quelle future. Come se non bastasse, le organizzazioni sono chiamate a difendersi da un crescente numero di minacce informatiche. Oggi più che mai, la convergenza di Cyber Security e Business Continuity è la *conditio sine qua non* per garantire la riduzione degli impatti finanziari, operativi, legali e reputazionali delle minacce informatiche.

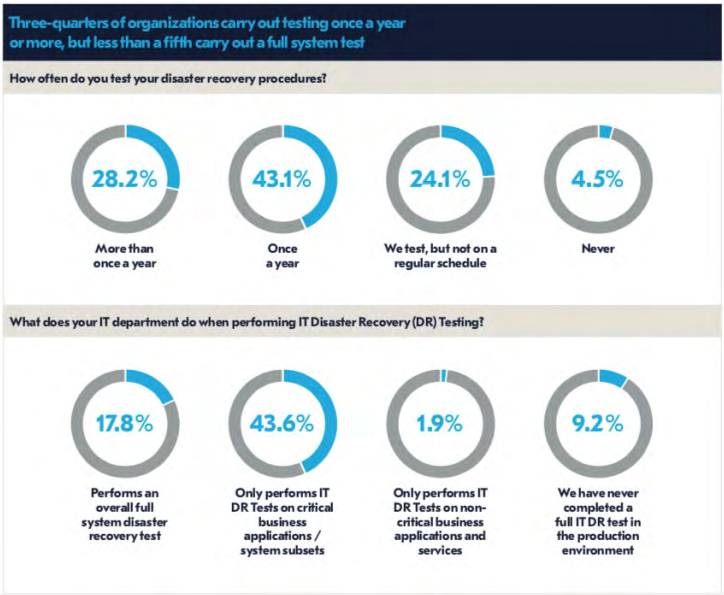
Il report "Technology & Business Continuity in Organizational Resilience 2020"

Il report sopra citato rivela che le organizzazioni che praticano un approccio senza silos tra i reparti - soprattutto in termini di Business Continuity, IT & Cyber Resilience - dispongono di processi e procedure molto più resilienti. Inoltre, viene altresì evidenziato come la mancanza e/o gli errori di comunicazione tra le funzioni possono impattare negativamente sui processi di resilienza: un'organizzazione su dieci, di fatto, non è riuscita a mappare i processi critici e molti intervistati hanno attribuito questo fallimento a una mancanza di comunicazione tra i reparti, con prodotti e servizi prioritari non concordati. Anche la presenza di sistemi legacy (i.e. insieme di applicazioni o un componenti obsoleti che, tuttavia, continuano ad essere usati) rimane una delle cause dei fallimenti del processo di resilienza.

Il report evidenzia, altresì, che la due diligence dei fornitori IT di terze parti non viene eseguita regolarmente: meno della metà degli intervistati dichiara che i KPI dei propri fornitori IT soddisfano i requisiti di continuità delle organizzazioni.
Inoltre, si evidenzia che le priorità risultano diverse quando si tratta di resilienza IT e di predisporre un Business Continuity Plan (BCP), ovvero: le funzioni IT Disaster Recovery (DR) o IT Service Continuity danno la priorità all'infrastruttura IT, mentre la funzione di Business Continuity da priorità alle applicazioni IT. Pertanto, è sempre più necessaria e strategica la sinergia e comunicazione tra queste funzioni soprattutto durante la predisposizione del BCP al fine di rispondere agli obiettivi prefissati.

Fonte: BCI, UK - "Technology & Business Continuity in Organizational Resilience" Report 2020

È interessante notare che meno di due terzi delle organizzazioni riferiscono di avere procedure DR aggiornate e meno di un quinto ammette di essere in grado di eseguire un test completo di ripristino di emergenza. Le principali ragioni di tale situazione sono dovute da un lato alla necessità di garantire tempi di attività continui e dall'altro ai vincoli finanziari soprattutto quando si tratta di organizzazioni di grandi dimensioni.



Fonte: BCI, UK- "Technology & Business Continuity in Organizational Resilience" Report 2020

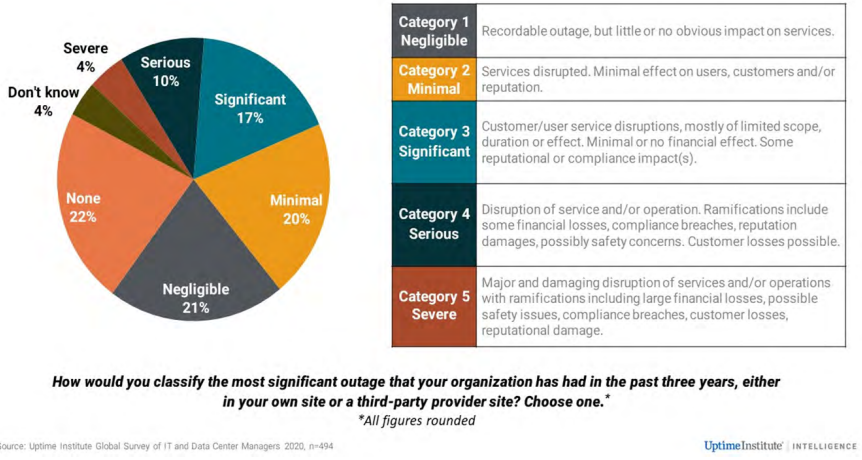
Man mano che le organizzazioni dipendono sempre più dalla tecnologia, la necessità di

sistemi IT resilienti diventa fondamentale e sempre più strategica. Inoltre, la pandemia ha amplificato l'importanza della IT & Cyber Resilience per le organizzazioni soprattutto a fronte del massivo impiego della modalità di *remote working* che ha esteso la superfice di attacco. Ne consegue che, il diffuso passaggio agli ambienti di lavoro virtuali ha posto maggiore enfasi sulla necessità di un'infrastruttura IT resiliente e sicura, oltre a far considerare ulteriori misure di sicurezza dei sistemi.
Una caratteristica dei massicci attacchi informatici che stiamo subendo è che sfruttano la nuova realtà creata dall'espansione del lavoro a distanza e il fatto che le soluzioni tradizionali di DR sono state progettate tenendo in considerazione soprattutto il "*failure*" dei data center, piuttosto che la corruzione dei dati a fronte di un attacco ransomware.

Il report rivela, altresì che, fortunatamente, laddove le funzioni di Business Continuity ed IT lavorano a stretto contatto, le organizzazioni possono superare questi *empasse* e garantire un'adeguata IT & Cyber Resilience. Ovvero, un approccio integrato permette alle organizzazioni di predisporre Piani di DR in termini sia di recupero dei data center (infrastruttura, applicazioni e rete) sia di recupero dei dati. In questo modo il Top Management sarà in grado di stabilire le priorità per la gestione del rischio di compromissione dei dati, considerando altresì la disponibilità delle risorse necessarie per Piani di DR riferiti ai dati sia di produzione sia di archiviazione. I professionisti di Business Continuity e IT & Cyber Security, pertanto, grazie ad un approccio coordinato/olistico saranno in grado di: acquisire le informazioni necessarie per la formulazione di strategie e di risposte alle sfide contingenti e future in termini di IT & Cyber Resilience; garantire, altresì, un più stretto allineamento dell'infrastruttura IT e del DR rispetto alle priorità organizzative; incoraggiare un approccio integrato della gestione dei rischi di Business Continuity, IT DR, Information & Cyber Security e Supply Chain.

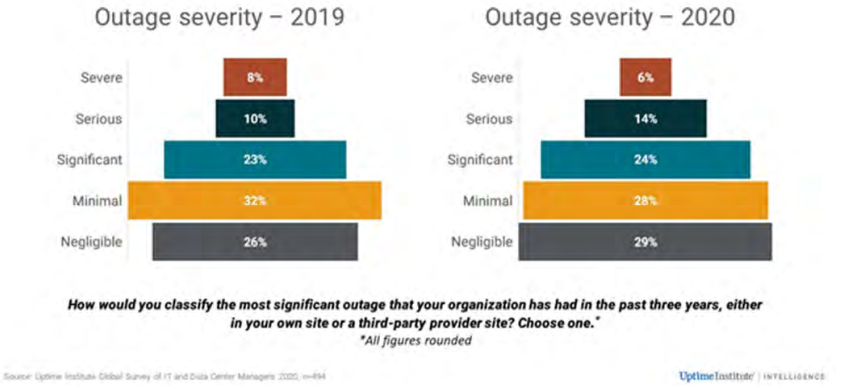
"Global Data Center Survey 2020" di Uptime Institute

Secondo il "*Global Data Center Survey 2020*" di Uptime Institute più di un terzo degli intervistati ha riferito di aver subito interruzioni gravi, con importanti ripercussioni finanziarie e reputazionali.



Fonte: Global Data Center Survey 2020", Uptime Institute

Inoltre, più di un quinto ha rivelato di aver subito grazi interruzioni negli ultimi 3 anni. Secondo Uptime Institute è doveroso evidenziare che queste interruzioni interessano sempre più data center e le *best practice* impongono revisioni complete e continue della resilienza di tutte le infrastrutture digitali di proprietà dell'azienda e di terze parti.

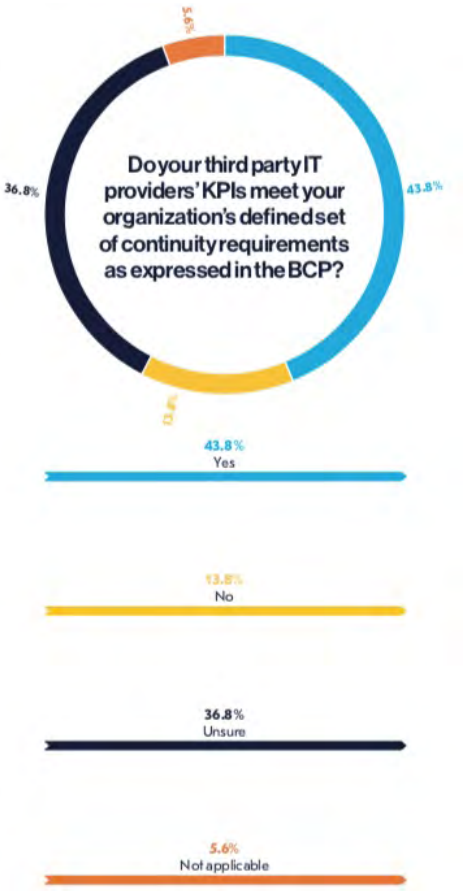


Fonte: Global Data Center Survey 2020", Uptime Institute

Alcuni fattori da considerare per garantire la Cyber Resilience & la Business Continuity

Un approccio olistico tra le funzioni di Business Continuity, IT & Cyber Security richiede una pianificazione e una preparazione approfondite al fine di progettare un'efficace strategia per il raggiungimento della resilienza organizzativa. Trattasi di un processo complesso che implica la conduzione di una Business Impact Analysis (BIA), un'analisi dei rischi, nonché lo sviluppo di piani, test, esercizi e formazione di Business Continuity e Disaster Recovery tenendo in considerazione alcuni fattori strategici, quali:

- ***La comunicazione tra i professionisti IT e di Business Continuity***: è fondamentale nello stabilire le priorità, evitando inutili tensioni in uno scenario di crisi.
- ***L'analisi delle diverse priorità dei reparti vs quelle della funzione di Business Continuity ed IT*** (i.e. applicazioni aziendali vs infrastruttura IT): vanno garantita in modo tale da avere una visione end-to-end sia a livello di servizio o di applicazione, includendo le dipendenze da altri servizi e applicazioni e tutti i componenti di infrastruttura dipendenti (i.e. hardware, storage e reti) indipendentemente da dove si trovino all'interno della catena di approvvigionamento, dato che se mancano parti del "puzzle", la resilienza sarà compromessa.
- ***La collaborazione:*** è fondamentale al fine di assicurarsi che i prodotti e i servizi prioritari siano concordati di comune accordo tra i reparti. Ciò può contribuire a garantire la continuità o il riavvio delle attività *"business critical"* concordate ed in linea con il BCP e altresì fornire una mappatura corretta dei processi critici concordati.
- ***La possibilità di avere un personale con un background di Business Continuity all'interno del Team di resilienza IT o viceversa***: dal report si evince che le persone con una buona comprensione dei processi e dei requisiti di entrambi i reparti sono state in grado di aiutare a generare le migliori pratiche per la resilienza IT & Cyber all'interno delle loro organizzazioni.
- ***La Due diligence su fornitori terzi***: non è sufficiente affidarsi ai soli indicatori di prestazione chiave (KPI); pertanto bisogna verificare l'esistenza di piani dei fornitori, le garanzie sui tempi di attività e le specifiche delle attrezzature prima della fase di approvvigionamento. Dato che sono sempre più le organizzazioni che dipendono dai servizi basati sul cloud e dall'hosting remoto, diventa fondamentale garantire che gli indicatori KPI di un provider IT soddisfino il set definito di requisiti di continuità dell'organizzazione (come espresso nel BCP) in modo tale da evitare tempi di inattività ed errori di sistema ingiustificati. Meno della metà (43,8%) degli intervistati afferma che i KPI dei propri fornitori IT soddisfano i requisiti di continuità dell'organizzazione, con il 13,8% che ammette non sono soddisfacenti. È interessante notare che la maggior parte di coloro che erano "incerti" in termini di soddisfazione dei requisiti di continuità dei fornitori erano professionisti della continuità aziendale, mentre coloro che lavoravano direttamente all'interno della resilienza IT o del rischio IT avevano maggiori probabilità di valutazione. Pertanto, diventa sempre più importante conoscere le criticità aziendali attraverso percorsi chiari per lo scambio di informazioni.



Fonte: BCI, UK - "Technology & Business Continuity in Organizational Resilience" Report 2020

- ***Il Test completo di DR:*** si rende indispensabile, dato che i test parziali non sono sufficienti per scoprire problemi all'interno dei sistemi che potrebbero causare problemi catastrofici per un'organizzazione.
- ***I Test degli scenari:*** fondamentale effettuarli prima che si verifica una crisi dato che possono aiutare a scoprire i problemi prima che tali misure di emergenza siano utilizzati in uno scenario reale. Per molte organizzazioni, la mancanza di test ed esercizi ha comportato carenze su larga scala dei sistemi IT durante la pandemia.

Inoltre, ogni organizzazione dovrà garantire:

- ***Consapevolezza*** dei normali requisiti aziendali di Business Continuity, delle dipendenze che potrebbero esistere, della criticità dei componenti e degli elementi del sistema IT e dei livelli operativi minimi accettabili. Inoltre, sarà fondamentale conoscere i requisiti di ripristino in termini di tempo, la capacità del sistema e delle prestazioni in caso di grave interruzione o guasto dei sistemi IT a supporto dei processi aziendali, come identificati attraverso la Business Impact Analysis (BIA).
- ***Protezione dell'organizzazione*** non solo in termini di controlli di sicurezza fisici e di accesso al sistema, ma anche in termini di riduzione del rischio di guasti del sistema, ad esempio rimuovendo i cosiddetti *Single Point of Failure (SPoF)*. Le potenziali esposizioni al rischio di sistemi ritenuti fondamentali per i processi aziendali dovrebbero essere identificate e gestite in modo prioritario.
- ***Capacità di intercettazione dei Single Point of Failures (SpoF)***, ovvero più velocemente il Team IT sa che un sistema è stato "interrotto", prima è possibile risolvere il problema. Le funzioni IT, attraverso l'impiego di *failure detection software* sono in grado di comprendere e risolvere i problemi prima che si traducano in gravi interruzioni.
- ***Piani dettagliati*** per affrontare gli effetti di un'interruzione, consentendo ai processi aziendali essenziali di continuare a funzionare senza interruzione del servizio o ad un livello minimo accettabile.
- ***Capacità di Recupero*** in termini di ripristino di servizi e processi a livelli business *as usual* entro tempi definiti e con una perdita di dati accettabile minima a seguito di un evento che causa interruzioni o guasti. Questo obiettivo sarà raggiunto solo con un piano di recupero efficace, ben testato e che soddisfi i requisiti aziendali.
- ***Revisione dei BCP*** per ogni programma di resilienza IT, includendo revisioni post-incidente per identificare le cause profonde delle interruzioni. Si tratta di un processo continuo che mira a consentire al team IT e all'azienda di comprendere potenziali problemi e di valutare e implementare azioni preventive per rimuovere, o almeno mitigare, il rischio di gravi interruzioni.
- ***Miglioramento continuo*** in modo da adottare misure per migliorare i sistemi e aumentare la resilienza, perfezionando continuamente i piani di DR e Business Continuity.

Conclusioni

Nel 2020 le organizzazioni hanno compreso quanto sia fondamentale e strategico essere preparate a qualsiasi circostanza per evitare incidenti/crisi/interruzioni soprattutto in un contesto altamente erratico, ambiguo, complesso e incerto. Le organizzazioni dipendono fortemente dalla loro infrastruttura tecnologica e devono essere in grado di affrontare attacchi informatici e violazioni della sicurezza (che stanno aumentando di frequenza e gravità a tal punto che dobbiamo presumere che, in futuro, saremo sempre meno in grado di difenderci se non attuiamo i necessari cambi di paradigma e non garantiamo la resilienza organizzativa). Ne consegue che la Funzione IT & Cyber Security e quella di Business Continuity dovranno sempre più collaborare, senza dimenticare le interazioni con le altre funzioni di Security ed il Risk Management al fine di garantire la salvaguardia ed il ripristino dei processi e ambienti fisici e virtuali in termini di tecnologia operativa ed informatica. Ricordiamoci che gli obiettivi di Business Continuity e Information & Cyber Security sono strettamente correlati e, di fatto, non vi può essere strategia di Business Continuity di successo senza coinvolgere la Information & Cyber Security e viceversa soprattutto in un contesto sempre più caratterizzato dal un processo di digitalizzazione ed automatizzazione accelerato come quello che stiamo vivendo.

Fonti *(in ordine alfabetico)*

- BCI, UK – "*Technology & Business Continuity in Organizational Resilience*" Report 2020
- "*Global Data Center Survey 2020*", Uptime Institute

GLOSSARIO

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

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

Blockchain	Tecnologia che consente la registrazione di transazioni, in uno scenario trustless, fra gli attori della stessa blockchain mediante l'utilizzo di un registro digitale immodificabile presente su vari nodi della rete, costituito da blocchi (block) fra loro concatenati (chain).
Booter-stresser	Strumenti a pagamento che consentono di scatenare attacchi *DDOS*.
Botnet	Insieme di dispositivi (compromessi da *malware*) connessi alla rete utilizzati per effettuare, a loro insaputa, un attacco ad esempio di tipo *DDOS*.
Buffer overflow	Evento che ha luogo quando viene superato il limite di archiviazione predefinito di un'area di memorizzazione temporanea.
Business continuity	Soluzioni di natura tecnica ed organizzativa predisposte per garantire la continuità dell'erogazione di un servizio (eventualmente con uno SLA ridotto).
BYOD (Bring You Own Device)	Politica che consente l'uso di dispositivi personali anche per finalità aziendali.
Captatore informatico	Software che viene immesso in dispositivi elettronici portatili al fine di intercettare comunicazioni o conversazioni tra presenti, il cui uso è specificatamente regolamentato dal Codice Penale, nel corso di indagini su alcuni specifici crimini.
Carding	Scambio e compravendita di informazioni riguardanti carte di credito, debito o account bancari, che vengono poi utilizzate per eseguire truffe di carattere finanziario acquistando beni o trasferendo fondi ai danni dei legittimi proprietari.
CEO Fraud	Tipi di attacco phishing mirati verso figure aziendali ad altissimo profilo, generalmente amministratori delegati, presidenti dell'azienda, direttori finanziari, etc.

CERT (Computer Emergency Response Team)	Struttura destinata a rispondere agli incidenti informatici e alla rilevazione e contrasto alle minacce. Fra i principali obiettivi di un CERT (vedi CERT Nazionale): fornire informazioni tempestive su potenziali minacce informatiche che possano recare danno a imprese e cittadini; incrementare la consapevolezza e la cultura della sicurezza; cooperare con istituzioni analoghe, nazionali ed internazionali, e con altri attori pubblici e privati coinvolti nella sicurezza informatica promuovendo la loro interazione; facilitare la risposta ad incidenti informatici su larga scala; fornire supporto nel processo di soluzione di crisi cibernetica.
Cifratura "at rest" o "a riposo"	Cifratura dei dati nello storage.
Cifratura omomorfa	Tecnica utilizzata nell'ambito dell'*e-voting*. Con questo sistema di cifratura è possibile sommare due numeri cifrati o compiere altre operazioni algebriche senza decifrarli.
CISP (Card-based Payment Instrument Issuing Service Provider)	Prestatori di servizi di pagamento emittenti strumenti di pagamento basati su carta, che potranno emettere carte di debito a valere su conti di pagamento detenuti dai clienti presso Istituti di Credito diversi.
Cloud weaponization	Tipo di attacco nel quale l'attaccante ottiene un primo punto d'ingresso nell'infrastruttura cloud attraverso la compromissione e il controllo di alcune machine virtuali. L'attaccante utilizza poi questi sistemi per attaccare, compromettere e controllare migliaia di altre macchine, incluse altre appartenenti allo stesso service provider cloud dell'attacco iniziale, e altre appartenenti ad altri service provider pubblici.
CNOs (Computer Network Operations)	Tipologia di *Information warfare* finalizzato all'attacco e distruzioni delle informazioni presenti sui sistemi informativi avversari, alla distruzione delle reti e dei sistemi stessi e alla difesa delle proprie.
CNP (Card-Not-Present)	Indica un pagamento effettuato senza la presenza fisica di una carta di pagamento, ad esempio su Internet.

Cognitive Security	Applicazione all'ambito della sicurezza delle soluzioni di Cognitive Computing.
Context-based access	Tecnica che condiziona l'accesso alla valutazione dinamica del rischio della singola transazione, modulando eventuali azioni aggiuntive di verifica. Ad esempio le soluzioni di autenticazione e autorizzazione, sia nel caso di login che di disposizione di operazioni, non si limitano più ad autorizzare o bloccare un'operazione, ma offrono una gamma intermedia di possibilità, come ad esempio autorizzare un'operazione, ma con dei limiti, oppure richiedere verifiche aggiuntive.
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.
C&C (Command &Control)	I centri di comando e controllo (C&C) sono quegli host utilizzati per l'invio dei comandi alle macchine infette (bot) dal *malware* utilizzato per la costruzione della *botnet*. Tali host fungono da ponte nelle comunicazioni tra gli host infetti e chi gestisce la botnet, al fine di rendere più difficile la localizzazione di questi ultimi.
Credential Stuffing	Attacco nel quale vengono utilizzate coppie di user id/password raccolte in precedenza in modo fraudolento.
Cryptovaluta	Token digitale che costituisce uno strumento di pagamento. È possibile includere nei messaggi di pagamento ulteriori informazioni cosichè i token possono rappresentare digitalmente anche altri asset materiali o immateriali.

CTW (Check-the-Web)	Piattaforma tecnologiche appositamente creata in ambito IRU a supporto del monitoraggio e delle indagini nell'ambito di terrorismo in Internet, il cui ruolo principale è di anticipare e prevenire l'abuso terroristico di strumenti online, nonché di svolgere un ruolo consultivo proattivo a tale riguardo nei confronti degli Stati membri dell'UE e del settore privato.
CVSS versione 3 (Common Vulnerability Scoring System)	Sistema di valutazione delle vulnerabilità che fornisce un modo per acquisire le principali caratteristiche di una vulnerabilità e per produrre un punteggio numerico che rifletta la sua gravità, nonché una rappresentazione testuale di tale punteggio. Il punteggio numerico può quindi essere tradotto in una rappresentazione qualitativa (come bassa, media, alta e critica) per aiutare le organizzazioni a valutare e prioritizzare in modo adeguato i loro processi di gestione delle vulnerabilità. (https://www.first.org/cvss/specification-document)
Constituency	Nell'ambito di un *CERT* indica a chi è rivolto il servizio (ad esempio Pubblica Amministrazione Centrale, Regioni e Città metropolitane).
Course of action matrix	Metodologia per l'identificazione, la prioritizzazione e la rappresentazione sinottica delle azioni da intraprendere, in caso di possibili intrusioni. È composta da: due azioni passive: Discover e Detect cinque attive - *Deny*, *Disrupt*, *Degrade*, *Deceive*, *Destroy*).
Cryptojacking	Processo che sfrutta illegalmente le risorse informatiche di una vittima per generare criptovaluta. In sostanza gli aggressori sottraggono potenza di calcolo installando un'applicazione di mining di criptovaluta sul sistema della vittima, che sia un PC o uno smartphone. La generazione di valuta virtuale, nota anche come criptovaluta, è molto dispendiosa in termini di potenza di elaborazione, motivo per cui gli aggressori devono infettare un vasto numero di vittime e utilizzarne la potenza di calcolo per generare nuove unità monetarie virtuali.

CSIRT (Computer Security Incident Response Team)	Struttura sostanzialmente simile ad un *CERT*.
CTI (Cyber Threat Intelligence)	Disciplina che si occupa di raccogliere e analizzare dati eterogenei - provenienti da diverse sorgenti informative interne ed esterne -per estrarre informazioni utili a conoscere le caratteristiche dell'attore della minaccia, in modo da poter attribuire un profilo di rischio specifico per i propri asset e sviluppare azioni di contrasto efficaci. In particolare, le attività di CTI si esplicano attraverso un processo di raccolta, classificazione, integrazione e analisi di dati grezzi relativi a minacce che operano nel cyberspazio.
Cyber intelligence	Attività volte a raccogliere e rielaborare informazioni al fine prevedere possibili minacce (non esclusivamente di natura informatica) agli asset oggetto di tutela.
Cybersquatting	Attività volta ad appropriarsi di nomi di dominio di terzi, in particolare di marchi commerciali di rilievo, al fine di trarne profitto.
Cyber crime	Attività criminali effettuate mediante l'uso di strumenti informatici.
Cyber espionage	Attività di spionaggio effettuata mediante l'uso di tecniche informatiche illecite.
Cyber Kill Chain	La cyber kill chain è un modello definito dagli analisti di Lockheed Martin come supporto decisionale rispetto alla rilevazione e risposta alle minacce. Esso include le seguenti fasi: reconnaissance, weaponization, delivery, exploitation, installation and persistence, command and control (C2), actions.
Cyber resilience	Capacità di un'organizzazione di resistere preventivamente o ad un attacco e di ripristinare la normale operatività successivamente allo stesso.

Cyber security	Gruppo di attività e competenze multidisciplinari, complesse e sofisticate, molte delle quali non informatiche, che sono oggettivamente di difficile integrazione con le prassi esistenti di gestione dell'ICT e di allocazione dei budget relativi, poiché la loro implementazione richiede di superare paradigmi tecnologici e silos organizzativi costruiti negli anni a partire da esigenze di compliance e da metodi e strumenti propri della sicurezza informatica "tradizionale". lo scopo complessivo di questo insieme di discipline è il proteggere tutti quegli asset materiali ed immateriali che possono essere aggrediti tramite il "cyberspazio" ovvero che dipendono da esso, garantendo allo stesso tempo la governance, l'assurance e la business continuity di tutta l'infrastruttura digitale a supporto.
Cyber Diplomacy	"Incoraggiamo tutti gli Stati a impegnarsi in comportamenti rispettosi delle leggi e delle norme e che concorrano al rafforzamento della fiducia nel rispettivo uso delle TIC. Approcci collaborativi contribuirebbero anche a lottare contro l'uso del cyberspazio ad opera di attori non-Stato, a scopo terroristico e criminale". *(Dichiarazione del G7 sul comportamento responsabile degli stati nel cyberspazio) www.esteri.it/mae/resource/doc/2017/04/declaration_on_cyberspace_ita.doc*
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.
Cryptolocker	*Malware* che ha come finalità criptare i file presenti nel dispositivo infetto al fine di richiedere un riscatto alla vittima per renderli nuovamente intellegibili.

CVV2 (Card Verification Value 2)	Codice di sicurezza utilizzato sulle carte di pagamento.
Dark web	Parte oscura del World Wide Web, sottoinsieme del deep web, accessibile mediante l'uso di apposite applicazioni software.
Data Leakage	Trasferimento non autorizzato di informazioni riservate.
Data breach	La violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati. *(Art. 4.12 GDPR)* Alcuni possibili esempi: l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati; il furto o la perdita di dispositivi informatici contenenti dati personali; la deliberata alterazione di dati personali; l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.; la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità; la divulgazione non autorizzata dei dati personali. *(Garante per la protezione dei dati personali)*
Deep Fake	Algoritmi di deep learning in grado di creare foto o video falsi.
Deep Web	L'insieme dei contenuti presenti sul web e non indicizzati dai comuni motori di ricerca (Google, Bing…).
Defacement	Manipolazione del contenuto di una pagina web (tipicamente la home page) a scopi dimostrativi.
DES (Data Encryption Standard)	Algoritmo per la cifratura dei dati a chiave simmetrica.

Diamond Model	Framework strutturato per l'analisi tecnica di possibili intrusioni. *(Adversary, Infrastructure, Victim, Capability).*
DNS (Domain Name System)	Indica sia l'insieme gerarchico di dispositivi, sia il *protocollo*, utilizzati per associare un indirizzo IP ad un nome di dominio tramite un database distribuito.
DNS Open Resolver	Sistemi vulnerabili utilizzati come strumento per perpetrare attacchi informatici di tipo *DDOS* amplificati.
DNSSEC (Domain Name System Security Extensions)	Insieme di specifiche per garantire alcuni aspetti di sicurezza delle informazioni fornite dai *DNS*.
Dos (Denial of Service)	Attacchi volti a rendere inaccessibili alcuni tipi di servizi. Possono essere divisi in due tipologie: • applicativi, tesi a generare un numero di richieste maggiore o uguale al numero di richieste massimo a cui un server può rispondere (ad esempio numero di richieste web HTTP/HTTPS concorrenti); • volumetrici, tesi a generare un volume di traffico maggiore o uguale alla banda disponibile in modo da saturarne le risorse. Se vengono utilizzati più dispositivi per l'attacco coordinati da un centro di *C&C* si parla di *DDOS* (Destribuited Denial of Service).
DDoS (Distributed Denial of Service)	Attacchi *DOS* distribuiti, cioè basati sull'uso di una rete di apparati, costituenti in una botnet dai quali parte l'attacco verso l'obiettivo.
DDoS-for-hire	Letteralmente servizio DDoS da noleggiare.
DGA (Domain generation algorithms)	Algoritmo utilizzato da alcuni *malware* per la generazione di migliaia di nomi di dominio alcuni dei quali sono utilizzati dai loro server *C&C*.

Digital Scarcity	In una blockchain la capacità di rendere non riproducibili informazioni digitali come file o pagamenti.
DNS cache poisoning	Tipo di attacco nel quale l'attaccante inserisce corrispondenze Indirizzo-IP alterate all'interno della cache del meccanismo di risoluzione degli indirizzi IP. Come risultato la cache userà l'indirizzo IP alterato in tutte le successive transazioni. L'indirizzo che comparirà nella barra URL di un browser sarà quello corretto e desiderato, ma il corrispondente indirizzo IP utilizzato sarà quello alterato e tutto il traffico di rete sarà quindi reindirizzato verso il sito replica controllato dai cyber criminali e nel quale si simulano log in per tracciare tutti i fattori di autenticazione inseriti.
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.
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).
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).
GRE (Generic Routing Encapsulation)	Protocollo di tunneling che incapsula vari protocolli di livello rete all'interno collegamenti virtuali point-to-point.
Info Stealer	Software orientati a rubare informazioni all'utente compromesso.
Hacktivism	Azioni, compresi attacchi informatici, effettuate per finalità politiche o sociali.
Hit & Run (o Pulse wave)	Attacchi di breve durata, ma frequenti nell'arco di poche ore.
HMI (Human Machine Interface Systems)	Componente fondamentale dei sistemi IT industriali, che permette all'operatore umano di interagire con gli ambienti di controllo, supervisione e acquisizione dati (supervisory control and data acquisition - SCADA).

Honeypot	Letteralmente barattolo del miele. Indica un asset esca isolato verso cui indirizzare e raccogliere informazioni su eventuali attacchi, al fine di tutelare il reale sistema informativo.
HTTP POST DoS Attack	Attacco che sfrutta un difetto di progettazione di molti server web. L'attaccante inizia una connessione http del tutto lecita verso un server web andando ad abusare del campo 'Content-Lenght'. Visto che la maggior parte dei server web accetta dimensioni del payload del messaggio anche di 2Gb, l'attaccante comincia ad inviare il corpo del messaggio ad una ridottissima velocità (anche 1byte ogni 110 secondi). Ciò comporta che il server web resta in ascolto per molto tempo, lasciando aperti i canali http (del tutto leciti) andando quindi a saturare tutte le sue risorse visto che le connessioni restano aperte.
HUMINT (HUMan INTelligence)	Disciplina intelligence consistente nella ricerca ed elaborazione di notizie di interesse per la sicurezza nazionale provenienti da persone fisiche. Le sue specificità sono legate alla tipicità della fonte e si sostanziano soprattutto in particolari modalità di gestione. (Tratto da: Glossario intelligence – Il linguaggio degli Organismi informativi - www.sicurezzanazionale.gov.it)
Kill Switch	Termine generico per indicare un dispositivo che serve a bloccare in modo forzato un'attività.
ICMP (Internet Control Message Protocol)	Protocolli che consentono ai dispositivi di una rete di comunicare informazioni di controllo e messaggi.
IDS (Intrusion detection system)	Dispositivo in grado di identificare modelli riconducibili a possibili attacchi alla rete o ai sistemi.
IMEI (International Mobile Equipment Identity)	Codice univoco che identifica un terminale mobile

IMSI (International Mobile Subscriber Identity)	Codice univoco internazionale che combina SIM, nazione ed operatore telefonico.
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.
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.
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.
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)
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… e i relativi pagamenti, indipendentemente dalla forma o dal media utilizzato per la loro rappresentazione.
Phising	Tecnica che induce la vittima, mediante una falsa comunicazione in posta elettronica, a collegarsi verso un sito bersaglio simile all'originale (ad esempio il sito di una banca) al fine di intercettare informazioni trasmesse, quali le credenziali di accesso.
Phone hacking	Attività di hacking che ha come oggetto i sistemi telefonici; ad esempio mediante l'accesso illegittimo a caselle vocali.
Ping flood:	Attacco basato sul continuo ping dell'indirizzo della macchina vittima. Se migliaia e migliaia di computer, che fanno parte di una botnet, effettuano questa azione continuamente, la vittima esaurirà presto le sue risorse.
Ping of Death	Attacco basato sull'inoltro di un pacchetto di ping non standard, forgiato in modo tale da mandare in crash lo stack di networking della macchina vittima.

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).
PHI (Protected Health Information)	Tipo di informazioni sanitarie protette.
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.
Rootkit	*Malware* che consente sia il controllo occulto di un dispositivo, sia di nascondere la presenza propria e di altri malware.
Sandboxing	Ambiente protetto nel quale è possibile testare applicazioni senza compromettere l'intero sistema informatico.
Scrubbing center	Letteralmente centro di pulizia. In uno Scrubbing center il traffico di rete viene analizzato e "ripulito" delle componenti dannose.

Service Abuse	Tecniche di attacco in ambito VOIP in cui si utilizza l'infrastruttura della rete VOIP della vittima per generare traffico verso numerazioni particolari a tariffazione speciale.
Side-channel attacks	Tecnica di attacco nella quale l'attaccante tenta di posizionare una macchina virtuale sullo stesso server fisico della potenziale vittima.
SIEM (Security information & event management)	Sistema per la raccolta e normalizzazione dei log e per la correlazione degli eventi finalizzato al monitoraggio della sicurezza.
SIGINT (SIGnals INTelligence)	Disciplina intelligence consistente nella ricerca ed elaborazione di notizie di interesse per la sicurezza originate da segnali e/o emissioni elettromagnetiche provenienti dall'estero. Le principali branche della SIGINT sono la COMINT e la ELINT. (Tratto da: Glossario intelligence – Il linguaggio degli Organismi informativi - www.sicurezzanazionale.gov.it)
Sinkhole	Tecnica per reindirizzare il traffico di rete verso uno specifico server al fine, ad esempio, di analizzarlo.
SIRIUS	Piattaforma tecnologiche appositamente creata in ambito IRU a supporto del monitoraggio e delle indagini nell'ambito di terrorismo in Internet. In particolare consente ai professionisti delle forze dell'ordine, di condividere conoscenze, migliori prassi e competenze nel campo delle indagini sulla criminalità agevolata da Internet, con particolare attenzione all'antiterrorismo.
Smart contracts	Programmi per computer in esecuzione sul registro generale; sono diventati una caratteristica fondamentale delle *blockchain* di seconda generazione come Ethereum o NEO. Questo tipo di programmi sono attualmente utilizzati per facilitare, verificare o applicare regole tra le parti in occasione delle ICO o nella fruizione dei servizi offerti dagli operatori del settore, consentendo l'elaborazione diretta e le interazioni con altri contratti intelligenti.

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.
SOC (Security Operations Center)	Centro la gestione delle funzionalità di sicurezza e per il monitoraggio degli eventi che potrebbero essere una fonte di minaccia.
Social engineering	Tecniche di attacco basate sulla raccolta di informazioni mediante studio/interazione con una persona.
Social Threats	Versione VOIP del furto d'identità finalizzata a impersonare un utente e perpetrare azioni malevole con lo scopo di arrecare danni; ad esempio, furto di informazioni aziendali riservate.
Spear phishing	*Phishing* mirato verso specifici soggetti.
Spoofing	Modifica di una informazione, ad esempio l'indirizzo mittente di un pacchetto IP.
Spyware	*Malware* che raccoglie informazioni sul comportamento della vittima trasmettendole all'attaccante.
SQL injection	Tecnica di attacco basata sull'uso di query indirizzate a database SQL che consentono di ricavare informazioni ed eseguire azioni anche con privilegi amministrativi.
SSDP (Simple Service Discovery Protocol)	*Protocollo* che consente di scoprire e rendere disponibili automaticamente i dispositivi di una rete.
SSH (Secure Shell)	*Protocollo* cifrato che consente l'interazione remota con apparati di rete o di server permettendone, ad esempio, l'amministrazione.

STIX (Structured Threat Information eXpression)	Linguaggio strutturato che consente la descrizione e condivisione automatizzata di cyber threat intelligence (CTI) fra organizzazioni, utilizzando il protocollo *TAXII*.
Tampering	An intentional but unauthorized act resulting in the modification of a system, components of systems, its intended behavior, or data.
TAXII (Trusted Automated eXchange of Indicator Information)	Protocollo che consente lo scambio (in HTTPS) di CTI (cyber threat intelligence) descritti mediante *STIX*.
TCP Synflood	Tipo di attacco nel quale tramite pacchetti SYN in cui è falsificato l'IP mittente (spesso inesistente) si impedisce la corretta chiusura del three-way handshake, in quanto, nel momento in cui il server web vittima invia il SYN/ACK, non ricevendo alcun ACK di chiusura, essendo l'IP destinatario inesistente, lascerà la connessione "semi-aperta". Con un invio massivo di pacchetti SYN in concomitanza ad un alto tempo di timeout delle connessioni, il buffer del server verrebbe presto saturato, rendendo il server impossibilitato ad accettare ulteriori connessioni TCP, anche se legittime.
TDM (Time-division multiplexing)	Tecnica che consente la condivisione, da parte di più dispositivi, di un canale di comunicazione per un tempo limitato predefinito.
Tecniche di riflessione degli attacchi (DRDoS – Distributed Reflection Denial of Service)	La tecnica più diffusa sfrutta host esposti sulla Big Internet come riflettori del traffico a loro indirizzato sfruttando le vulnerabilità intrinseche ad alcuni protocolli quali NTP o DNS.

Tecniche di amplificazione degli attacchi	Sfruttando lo *spoofing* dell'indirizzo IP di una vittima, un utente malintenzionato può inviare piccole richieste ad un host vulnerabile inducendolo ad indirizzare le risposte alla vittima dell'attacco. Ad esempio nel caso del *protocollo NTP* si può amplificare la potenza dell'attacco anche di 600 volte.
Telnet	Protocollo utilizzato per la gestione di host remoti, accessibile da riga di comando.
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.
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.
XSS (Cross Site Scripting)	Vulnerabilità che sfrutta il limitato controllo nell'input di un form su un sito web mediante l'uso di qualsiasi linguaggio di scripting.
Zero-day attach	Attacco compiuto sfruttando *vulnerabilità* non ancora note/risolte.
Zero Trust	Paradigma i cui principi fondamentali sono: si assuma che l'ambiente sia ostile, non si distingua tra utenti interni ed esterni, non si assuma "trust" (da cui il nome), si eroghino applicazioni solo a device e utenti riconosciuti e autenticati, si effettuino analisi dei log e dei comportamenti utente. In pratica occorre trattare tutti gli utenti nello stesso modo, utenti della stessa azienda o esterni, che siano nel perimetro della rete aziendale o meno, che i dati a cui vogliono accedere siano dentro l'azienda o da qualche parte nel cloud.

Gli autori del Rapporto Clusit 2021

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

Liviu Arsene è Global Cybersecurity Researcher per Bitdefender, con un forte background in sicurezza e tecnologia. Facendo ricerche sulle tendenze e sugli sviluppi globali della sicurezza informatica, Arsene si concentra sulle minacce persistenti avanzate e sugli incidenti di sicurezza, valutando il loro impatto nelle infrastrutture critiche sia pubbliche che private. Le sue passioni ruotano attorno a tecnologie e gadget innovativi, in particolare sulle loro applicazioni di sicurezza e sull'impatto strategico a lungo termine.

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

Giancarlo Butti ha acquisito un master in Gestione aziendale e Sviluppo Organizzativo presso il MIP Politecnico di Milano. Si occupa di ICT, organizzazione e normativa dai primi anni 80. Auditor ed esperto di sicurezza e privacy ha all'attivo oltre 800 articoli e collaborazioni con oltre 30 testate. Ha pubblicato 25 fra libri e white paper alcuni dei quali utilizzati come testi universitari; ha partecipato alla redazione di 17 opere collettive. Già docente del percorso professionalizzante ABI - Privacy Expert e Data Protection Officer in Banca è docente/relatore presso eventi di ISACA/AIEA, ORACLE/CLUSIT, ITER, INFORMA BANCA, CONVENIA, CETIF, IKN, UNISEF, Università Statale di Milano, Università degli Studi Suor Orsola Benincasa Napoli…, Politecnico di Milano, Cefriel. Partecipa ai gruppi di lavoro di ABI LAB, ISACA/AIEA, Oracle Community for Security, UNINFO, Assogestioni... È fra i coordinatori di europrivacy.info e socio di CLUSIT, ISACA, BCI. Ha inoltre acquisito le certificazioni/qualificazioni LA BS7799, LA ISO/IEC27001, CRISC, CDPSE, ISM, DPO, CBCI, AMBCI.

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

Nunzia CIARDI, Dirigente Superiore della Polizia di Stato, è il Direttore del Servizio Polizia Postale e delle Comunicazioni. Laureata in giurisprudenza, con anni di esperienza nel contrasto al cybercrime, coordina attualmente le unità specializzate della Polizia di Stato nel contrasto al cyberterrorismo, al financial cybercrime, alla pedopornografia on-line nonché di tutti i reati che coinvolgono i minori on-line, alla tutela delle infrastrutture critiche informatiche nazionali, all'hacking e ai crimini informatici in generale. Partecipa, come membro nazionale in rappresentanza dell'Italia, alle riunioni dell'European Union Cybercrime Taskforce di Europol; ha preso parte alla realizzazione del progetto europeo EU-

OF2CEN per l'adozione di strategie comuni contro il crimine organizzato nel settore delle frodi on-line. E'rappresentante del Ministero dell'Interno in seno al Nucleo Sicurezza Cibernetica ed al Tavolo Tecnico Cyber. E'coordinatore di una Struttura di missione per la realizzazione di un polo centrale della sicurezza cibernetica del Ministero dell'Interno. E'membro dell'Unità Informativa Scommesse Sportive, del "Gruppo Nazionale di Cybersecurity per i Servizi Sanitari". E'membro componente del Consiglio del "*Women4Cyber*", iniziativa avviata dall'Organizzazione Europea per la Sicurezza Cibernetica (ECSO), volta a implementare il coinvolgimento delle donne nel settore della sicurezza cibernetica. E'componente dell'Organismo permanente di supporto al "Centro di coordinamento per le attività di monitoraggio, analisi e scambio permanente di informazioni sul fenomeno degli atti intimidatori nei confronti dei giornalisti". Svolge attività di docenza presso diverse scuole di Polizia, presso la scuola Ufficiali dei Carabinieri, presso il Centro Alti Studi per la Difesa, nonché presso diverse università ed enti, sulle principali attività di competenza della Specialità. Autrice di libri e pubblicazioni a carattere scientifico in materia di cybercrime, ha collaborato alla redazione del Rapporto Clusit 2018, 2019 e 2020.

Luisa Colucci ha conseguito la laurea in Informatica presso l'Università degli Studi di Pisa. Attualmente ricopre il ruolo di Solution Design Manager nella unit di CyberSecurity di Exprivia. Precedentemente ha ricoperto il ruolo di Security Architect nella divisione Security di IBM. Ha lavorato negli ultimi 10 anni nel campo della CyberSecurity acquisendo un'ampia conoscenza dei processi, delle tecnologie e del mercato. Nel suo passato ha ricoperto ruoli di leadership in un contesto lavorativo europeo ed è stata speaker in eventi nazionali e internazionali sulla Cybersecurity come ITASEC e Cybertech Tel Aviv.

Pasquale Digregorio è un ex-Ufficiale d'Accademia, attualmente Vice Capo Divisione del Computer Emergency Response Team della Banca d'Italia, dove mette al servizio dell'Istituto la sua esperienza in cyber intelligence e cybersecurity, sviluppata in 20 anni di servizio, svolti presso il Ministero della Difesa e la Presidenza del Consiglio. Dopo la laurea magistrale in ingegneria delle telecomunicazioni presso il Politecnico di Torino ha conseguito un master di secondo livello in Sistemi avanzati di comunicazione e localizzazione satellitare presso l'Università Tor Vergata ed uno in Protezione Strategica del Sistema Paese presso la SIOI. Nel corso della sua carriera ha fatto parte di commissioni e organismi permanenti in seno alla NATO; svolge attività formative e di docenza presso enti universitari e Istituzioni. È autore di diverse pubblicazioni e inventore di un brevetto internazionale.

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 e a gennaio del 2020 Manager System Engineering per il centro/sud Italia. Oggi è il responsabile di un team di System Engineer che coprono il territorio del centro/sud Italia e Malta nei settori Telco, PAC/Defense, PAL/Industry, Energy/Utilities. Nel 2005 si è laureato in informatica all'università La Sapienza di Roma con una tesi sperimentale sulla sicurezza di rete, lavorando tra il 2014 e il 2012 per due tra i più importanti System Integrar italiani nella sicurezza informatica in qualità di Systems Engineer, Security Consultant, Sr. Security Engineer and Team Leader. In questi anni di lavoro ha maturato importanti 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 tre brevetti con Fortinet presso USPTO (United States Patent and Trademark Office's) su: Security Fabric Cooperation; End-point protection; Deception.

Giorgia Dragoni si è laureata nel 2014 in Ingegneria Gestionale al Politecnico di Milano, indirizzo Manufacturing & Management, e nello stesso anno ha iniziato a lavorare negli Osservatori Digital Innovation occupandosi di trasformazione digitale e cybersecurity. Attualmente è ricercatrice sui temi della Cybersecurity & Data Protection e dei Big Data Analytics e dal 2020 è Direttore dell'Osservatorio Digital Identity. Sta frequentando l'Executive Master in Management presso il MIP.

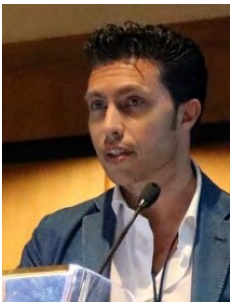
Gabriele Faggioli, legale, è amministratore delegato di Digital360 e di Partners4Innovation, Presidente del Clusit e Responsabile Scientifico dell'Osservatorio Cybersecurity & Data Protection del Politecnico di Milano. Gabriele inoltre è Adjunct Professor del MIP – Politecnico di Milano ed è stato membro 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 amminstrativa 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.

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.

Federica Maria Rita Livelli è In possesso della certificazione Business Continuity - AMBCI BCI, UK e 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. Membro del Board del BCI Italy Chapter, socia ANRA, AIPSA, CLUSIT ed UNI. Membro di diversi Comitati: CLUSIT-Artificial Intelligence, UNI/CT 016/GL 02 «Sistemi di gestione per la qualità» (ISO/TC 176/SC 2), UNI/CT 016/GL 09 «Governance delle organizzazioni» (ISO/TC 309) e UNI/CT 016/GL 89 «Gestione dell'innovazione» (ISO/TC 279) (Commissione Tecnica UNI/CT 016 «Gestione per la qualità e metodi statistici»). Membro della Community: Women for Cyber Security e Ambassador della Community Donne 4.0. Docente di moduli di introduzione di: ISO 22301 - Business Continuity & Resilience (Università POLIMI–BOCCONI e Università di Verona); ISO 31000 - Risk Management (Università Statale di Milano). Relatrice e moderatrice in diversi seminari, conferenze nazionali ed internazionali. Autrice di numerosi articoli su diverse riviste online, (i.e.: AgendaDigitale, Cybersecurity360, AI4Business, Risk Management360, EnergyUp, Blockchain4Innovation, Internet4Things, Industry4Business, ANRA - RM Magazine, ISPI online, Insurance Review, UNI Magazine online, The BCI Blog). Partecipato, in qualità di co-autrice alle edizioni 2020 del Rapporto Clusit - Cyber Security.

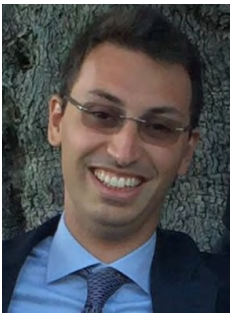
Roberto Obialero è Cybersecurity & Data Protection Advisor, in possesso di una esperienza ventennale in ruoli, manageriali, di sviluppo business e tecnici nell'ambito dell'offerta di servizi di sicurezza informatica. Collabora a titolo di advisor freelance nel ruolo CISO e nella realizzazione di importanti progetti sulle tematiche cybersecurity e data protection svolgendo attività di gestione del rischio, definizione strategie e roadmap cybersecurity, business continuity e vulnerability management, gestione di incidenti informatici, training & awareness. È in possesso delle certificazioni indipendenti GSTRT, GPPA e GCFA ottenute attraverso il programma SANS-GIAC americano, della certificazione ISO 27000 Lead Auditor e si è perfezionato in "Computer Forensics & Data Protection" e "Data Protection & Data Governance" presso l'Università Statale di Milano. Membro del Comitato Direttivo Clusit collabora attivamente alla realizzazione di progetti di ricerca nell'ambito Cybersecurity & Data Protection con le principali community di settore; è stato speaker in occasione di diversi eventi di rilevanza nazionale, oltre ad aver contribuito alla redazione di diverse pubblicazioni ed articoli per conto di riviste specializzate.



Marco Pericò ha conseguito la Laurea Magistrale in Ingegneria Informatica presso l'Università degli Studi di Palermo e successivamente un Master in Cybercrime e Informatica Forense presso l'Università degli Studi di Roma "La Sapienza". Lavora nel CERT della Banca d'Italia occupandosi di cyber threat intelligence e ricoprendo anche il ruolo di esperto nell'ambito del sistema di gestione del rischio operativo. In precedenza, in qualità di Funzionario Informatico del Dipartimento dell'Amministrazione Generale del Personale e dei Servizi del Ministero dell'Economia e delle Finanze, si è occupato di gestione della sicurezza e governance pianificando, progettando, sviluppando e acquisendo architetture e infrastrutture informatiche per il Dipartimento e per il Ministero. Nel suo precedente incarico in ISTAT ha progettato e realizzato sistemi di sicurezza informatica, curandone la gestione e l'evoluzione tecnologica.

Alessandro Piva, laureato in Ingegneria delle Telecomunicazioni e in Ingegneria Gestionale al Politecnico di Milano nel 2006, ha conseguito in seguito un Executive Master in Business Administration (EMBA) presso il MIP Politecnico di Milano. Alla School of Management del Politecnico di Milano, dove lavora da circa 15 anni, è Direttore degli Osservatori Cybersecurity & Data Protection, Cloud Transformation, Artificial Intelligence e Responsabile della Ricerca dell'Osservatorio Big Data & Business Analytics.

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



Marco Raimondi, nato nel 1987, si laurea in Ingegneria delle Telecomunicazioni presso il Politecnico di Milano. Ha iniziato la sua carriera nell'ambito IT per poi orientare la sua attività nel mondo commerciale, con un focus particolare sul mercato Enterprise. Dal 2012 ha lavorato presso Vodafone Italia dove ha ricoperto nella Business Unit Enterprise dapprima il ruolo di Presales e successivamente il ruolo di Marketing Product Manager nel mercato delle PMI. Dal 2017 in Fastweb ricopre dapprima il ruolo di Marketing Product Manager in ambito security, quindi il ruolo di Marketing Manager responsabile dello sviluppo dei prodotti di Sicurezza, Cloud e IoT.

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

Stefano Russo ha conseguito nel 2015 la laurea magistrale in Ingegneria Informatica presso l'Università degli Studi Roma Tre, con una tesi riguardante lo sviluppo di un framework per la modellazione automatica e l'interrogazione di basi di dati a grafo distribuite. Da sempre appassionato di IT Security, sin dall'inizio della sua carriera si è focalizzato su questo ambito occupandosi di diverse attività: progettazione e sviluppo backend di sistemi di monitoraggio e log management, system integration, penetration testing e cyber threat intelligence. Dal 2019 ricopre il ruolo di Cyber Security Analyst nel CERT della Banca d'Italia.

Rodolfo Saccani, Security R&D Manager in Libra Esva, vive l'IT dal 1994, in qualità di sviluppatore, sistemista, consulente e project manager. Ha vissuto e lavorato negli USA e in Danimarca. Da sempre interessato al mondo della *security*, ha un'esperienza tecnica eterogenea: sistemi linux embedded, avionica sperimentale, telecomunicazioni sicure in ambienti ostili, TV connessa, controllo di processo e automazione industriale, ricerca clinica, piattaforme web SaaS. Per passione si occupa anche di sicurezza nel volo libero: consigliere alla sicurezza in FIVL (Federazione Italiana Volo Libero) dal 2007, è expert presso il CEN (Comitato Europeo di Normazione) e partecipa alla stesura delle norme europee di certificazione delle attrezzature da volo libero. In Libraesva coordina la ricerca e sviluppo per l'e-mail security.

Sofia Scozzari si occupa con passione di informatica dall'età di 16 anni. Ha lavorato come consulente di sicurezza presso primarie aziende italiane e multinazionali, curando gli aspetti tecnologici ed organizzativi di numerosi progetti. Già Chief Executive Officer de iDIALOGHI, società milanese dedicata alla formazione e alla consulenza in ambito Cyber Security, è Founder e Managing Director di Hackmanac, società che elabora dati sulle minacce Cyber a supporto di attività di Risk Management. Negli anni si è occupata di Social Media Security, ICT Security Consulting & Training e della gestione di progetti di Sicurezza Gestita, quali Vulnerability Management, Penetration Testing, Mobile Security e Threat Intelligence. Membro del Comitato Scientifico di CLUSIT, è autrice di articoli e guide in tema di Social Media Security. È tra gli autori dei papers "La Sicurezza nei Social Media", pubblicato nel 2014 dalla Oracle Community for Security, e «Blockchain & Distributed Ledger: aspetti di governance, security e compliance», pubblicato nel 2019 da Clusit. Fin dalla prima edizione contribuisce alla realizzazione del "Rapporto Clusit sulla Sicurezza

ICT in Italia" curando l'analisi dei principali attacchi a livello internazionale.

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

Enrico Tonello, laureato in ingegneria a Padova, è socio co-fondatore di TG Soft S.r.l. Cyber Security Specialist. Da sempre attento agli aspetti di sicurezza informatica ed in particolare ad attacchi da virus&malware. Autore di numerosi articoli su virus&malware informatici pubblicati su alcune delle principali riviste italiane del settore. Co-autore della suite AntiVirus-AntiSpyware-AntiMalware Vir.IT eXplorer PRO per Windows® Microsoft, con motore proprio dotata di tecnologie AntiRansomware protezione Crypto-Malware. Relatore in conferenze e seminari sui virus&malware informatici e su come difendersi come Security Evangelist.

Gianfranco Tonello, laureato in ingegneria informatica a Padova, è CEO di TG Soft S.r.l. Cyber Security Specialist. Malware Analyst, riconosciuto a livello internazionale quale analista di virus&malware di nuova generazione e sviluppatore di tecnologie AntiMalware. Dal 1990 analista di Virus/Malware con pubblicazione di analisi tecniche presso il VTC (Virus Test Center) dell'Università di Amburgo e numerose riviste italiane. Autore/Sviluppatore software specializzato nella produzione di tecnologie AntiVirus-AntiSpyware-AntiMalware: dal 1992 sviluppa software di identificazione euristica e dal 1993 il software AntiVirus VirIT per l'univoca identificazione, la corretta rimozione dotato di scudo residente in tempo reale per S.O. DOS; dal 1997 sviluppa la suite AntiVirus-AntiSpyware-AntiMalware Vir.IT eXplorer PRO per Windows® Microsoft, con motore proprio dotata di tecnologie AntiRansomware protezione Crypto-Malware; Dal 2013 sviluppa il software AntiMalware per Androd[TM] VirIT Mobile Security. Docente CLUSIT Associazione Italiana per la Sicurezza Informatica. WildList reporter (www.wildlist.org): analista/reporter della WildList, che individua i virus/malware on the wild cioè realmente circolanti a livello mondiale.

Membro AMTSO Anti-Malware Testing Standards Organization (www.amtso.org). Membro VIA Virus Information Alliance di Microsoft. Membro MVI Microsoft Virus Initiative.

Alessandro Vallega, Dirigente in Partners4Innovation, si occupa dei programmi di innovazione della capogruppo Digital 360 (scouting, acquisizioni, contratti di partnership), di cybersecurity e della linea d'offerta GRC della società. Prima del novembre 2018, è stato Business Development Director, Security e GDPR, in Oracle EMEA con la responsabilità di un team centrale e regionale sul tema del GDPR. Alessandro è nel direttivo di Clusit dal 2010, ed è il fondatore e chairman della Clusit Community for Security. È coautore, editor e team leader di undici pubblicazioni su diversi temi legati alla sicurezza (misure, rischio, frodi, ritorno dell'investimento, compliances, privacy, cloud...) liberamente scaricabili dal sito Clusit (http://c4s.clusit.it). Al momento è impegnato nella produzione della 12esima pubblicazione che tratterà il tema della sicurezza, rischio e compliance dell'Intelligenza Artificiale (previsto per marzo 2021). Contribuisce fin dal 2012 ai Rapporti Clusit sulla Sicurezza ICT in Italia. Quest'anno insegna Analisi e gestione del rischio all'Università Statale di Milano. Ha una laurea in Scienza Politiche conseguita all'Università degli Studi di Miano.

Andrea Zapparoli Manzoni si occupa con passione di ICT dal 1997 e di Information Security dal 2003, mettendo a frutto un background multidisciplinare in Scienze Politiche, Computer Science ed Ethical Hacking. È stato membro dell'Osservatorio per la Sicurezza Nazionale (OSN) nel 2011-12 e del Consiglio Direttivo di Assintel dal 2012 al 2016, coordinandone il GdL Cyber Security. Dal 2012 è membro del Consiglio Direttivo di Clusit, e Board Advisor del Center for Strategic Cyberspace + Security Science (CSCSS) di Londra. Per oltre 10 anni è stato Presidente de iDialoghi, società milanese dedicata alla formazione ed alla consulenza in ambito ICT Security. Nel gennaio 2015 ha assunto il ruolo di Head of Cyber Security Services della divisione Information Risk Management di KPMG Advisory. Dal giugno 2017 è Managing Director di un centro di ricerca internazionale in materia di Cyber Defense. È spesso chiamato come relatore a conferenze ed a tenere lezioni presso Università, sia in Italia che all'estero. Come docente Clusit tiene corsi di formazione su temi quali Cyber Crime, Mobile Security, Cyber Intelligence e Social Media Security, e partecipa come speaker alle varie edizioni del Security Summit, oltre che alla realizzazione di white papers (FSE, ROSI v2, Social Media) in collaborazione con la Oracle Community for Security. Fin dalla prima edizione (2011) del "Rapporto Clusit sulla Sicurezza ICT in Italia", si è occupato della sezione relativa all'analisi dei principali attacchi a livello internazionale e alle tendenze per il futuro.

Il Clusit, nato nel 2000 presso il Dipartimento di Informatica dell'Università degli Studi di Milano, è la più numerosa ed autorevole associazione italiana nel campo della sicurezza informatica. Oggi rappresenta oltre 600 organizzazioni, appartenenti a tutti i settori del Sistema-Paese.

Gli obiettivi

- Diffondere la cultura della sicurezza informatica presso le Aziende, la Pubblica Amministrazione e i cittadini.
- Partecipare alla elaborazione di leggi, norme e regolamenti che coinvolgono la sicurezza informatica, sia a livello nazionale che europeo.
- Contribuire alla definizione di percorsi di formazione per la preparazione e la certificazione delle diverse figure professionali operanti nel settore della sicurezza.
- Promuovere l'uso di metodologie e tecnologie che consentano di migliorare il livello di sicurezza delle varie realtà.

Le attività e i progetti in corso

- Formazione specialistica: i Webinar CLUSIT.
- Ricerca e studio: Premio "Innovare la Sicurezza delle Informazioni" per la migliore tesi universitaria arrivato alla 16a edizione.
- Le Conference specialistiche: i Security Summit Streaming Edition, i Security Summit On Site (che riprenderanno speriamo presto a Milano, Treviso, Verona e Roma), 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, sula sicurezza ICT in Italia, in produzione dal 2012.
- Il Mese Europeo della Sicurezza Informatica, iniziativa di sensibilizzazione promossa e coordinata ogni anno nel mese di ottobre in Italia da Clusit, in accordo con l'ENISA e con l'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione del Ministero dello Sviluppo Economico (ISCOM).

Il ruolo istituzionale

In ambito nazionale, Clusit opera in collaborazione con: Presidenza del Consiglio, numerosi ministeri, Banca d'Italia, Polizia Postale e delle Comunicazioni, Arma dei Carabinieri e Guardia di Finanza, Agenzia per l'Italia Digitale, Autorità Garante per la tutela dei dati personali, Autorità per le Garanzie nelle Comunicazioni, CERT Nazionale e CERT P.A., Università e Centri di Ricerca, Associazioni Professionali e Associazioni dei Consumatori, Confindustria, Confcommercio e CNA.

I rapporti internazionali

In ambito internazionale, Clusit partecipa a svariate iniziative in collaborazione con: i CERT, i CLUSI, Università e Centri di Ricerca in oltre 20 paesi, Commissione Europea,

ENISA (European Union Agency for Network and Information Security), ITU (International Telecommunication Union), OCSE, UNICRI (Agenzia delle Nazioni Unite che si occupa di criminalità e giustizia penale), le principali Associazioni Professionali del settore (ASIS, CSA, ISACA, ISC², ISSA, SANS) e le associazioni dei consumatori.

Security Summit è il più importante appuntamento italiano per tutti coloro che sono interessati alla sicurezza dei sistemi informatici e della rete e, più in generale, alla sicurezza delle informazioni.

Progettato e costruito per rispondere alle esigenze dei professionals di oggi, Security Summit è un convegno strutturato in momenti di divulgazione, di approfondimento, di formazione e di confronto. Aperto alle esperienze internazionali e agli stimoli che provengono sia dal mondo imprenditoriale che da quello universitario e della ricerca, il Summit si rivolge ai professionisti della sicurezza e a chi in azienda gestisce i problemi organizzativi o legali e contrattuali dell'Ict Security.

La **partecipazione è libera e gratuita**, con il solo obbligo dell'iscrizione online.
Il Security Summit è organizzato dal Clusit e da Astrea, agenzia di comunicazione ed organizzatore di eventi di alto profilo contenutistico nel mondo finanziario e dell'Ict.

Certificata dalla folta schiera di relatori (più di 700 sono intervenuti nelle scorse edizioni), provenienti dal mondo della ricerca, dell'Università, delle Associazioni, della consulenza, delle Istituzioni e delle imprese, la manifestazione è stata frequentata da oltre 18.000 partecipanti, e sono stati rilasciati circa 14.000 attestati validi per l'attribuzione di oltre 46.000 crediti formativi (CPE).

L'edizione 2021

La 13esima edizione del Security Summit parte con una edizione interamente in streaming, che si terrà dal 16 al 18 marzo. Hanno ripreso gli **Atelier della Security Summit Academy**, che si terranno tutto l'anno. Abbiamo inoltre messo in campo una nuova iniziativa: una serie di Eventi Verticali programmati in maggio (Energy & Utilities), giugno /Health Care), settembre (Finance) e ottobre (Manufacturing). Tra i temi più in evidenza per il 2020: Cyber Crime, Sicurezza del e nel Cloud, Intelligenza Artificiale, Supply Chain, IoT, Industria 4.0., Compliance, GDPR, Certificazioni (professionali, di sistema, di prodotto).

Informazioni

- **Agenda e contenuti:** info@clusit.it, +39 349 7768 882
- **Altre informazioni:** info@astrea.pro
- **Informazioni per la stampa:** press@securitysummit.it
- **Sito web:** www.securitysummit.it/
- **Foto reportage:** www.facebook.com/groups/64807913680/photos/?filter=albums
- **Video riprese e interviste:** www.youtube.com/user/SecuritySummit

In collaborazione con

www.securitysummit.it