Rapporto

2022

sulla sicurezza ICT
in Italia

SECURITY SUMMIT

Indice

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

Prefazione

Mentre scriviamo queste righe le bombe cadono in Ucraina e un conflitto allargato, da anni lontano dagli incubi di noi europei, è un rischio che non possiamo ignorare.

Una guerra cruenta, come tutte le guerre, che lascerà un mondo peggiore rispetto a prima.

Una guerra combattuta, per la prima volta nella storia in queste proporzioni, anche ben oltre il territorio in senso fisico e geografico, nello spazio cibernetico.
Nel cyber spazio una guerra allargata ben al di là di Russia e Ucraina già è esplosa.
Si confrontano stati, si confrontano gruppi organizzati conosciuti ai più per gli attacchi ad aziende e pubbliche amministrazioni.
Si parla di disconnessione dell'intera Russia, scelta che sarebbe epocale.

Una situazione estremamente complessa destinata a cambiare non solo gli assetti geopolitici mondiali ma anche la percezione dei rischi sottesi al digitale.
Mai come in questi giorni capiamo l'importanza della cybersecurity, mai come in questo periodo storico abbiamo bisogno di infrastrutture protette, sicure, resilienti.

Mai come in queste settimane, e nei prossimi mesi e anni, sarà importante rendersi conto della necessità di una scelta politica forte e possibilmente univoca a livello europeo, e mai come ora sarà importante usare al meglio le risorse del PNRR.

Uno sforzo politico e imprenditoriale collettivo che servirà non tanto per superare l'attuale crisi, ma di affrontare le prossime che prima o poi capiteranno.

Se il covid ci lascia in eredità una vita comune molto più connessa di prima, sia con riferimento alla nostra vita personale che alla vita professionale, in cui la sicurezza informatica è fondamentale per la difesa del valore e degli asset delle imprese e per la protezione della nostra vista quotidiana e del nostro essere digitali, la guerra Russia – Ucraina ci pone con brutalità davanti all'obbligo di avere infrastrutture che siano in grado di resistere ad attacchi esterni che potrebbero minare la capacità del Paese di erogare servizi essenziali ai cittadini.

In questo contesto le azioni degli ultimi anni del legislatore europeo e italiano sono, per me, assolutamente condivisibili e ci auguriamo, e ne sono certo, che la guida e l'azione della Agenzia per la cybersicurezza nazionale sarà decisa e fondamentale nel perseguimento di una strategia italiana ed europea che porti a una capacità di visione del tema sicurezza non più verticale e di paese, ma sistemica perlomeno a livello europeo.

La disgregazione imprenditoriale e della pubblica amministrazione italiana non aiuta. Ci rende deboli.
A piccole realtà corrispondono piccoli budget e visioni limitate.

È una visione gravemente miope, purtroppo tipicamente italiana.

Serve unire le forze.
Per questo mai come quest'anno l'associazionismo è fondamentale. La capacità di fare sistema e di unire competenze, esperienze, conoscenze.

Come CLUSIT, con il Consiglio Direttivo e il 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.
Come sempre, l'ultimo anno è stato il peggiore di tutti.
Vedremo come sarà il 2022 alla luce della guerra che si sta combattendo nel mondo cibernetico.

Sicuramente l'Europa sarà sempre più al centro del fenomeno, anche sul cybercrime in senso stretto, e i danni saranno sempre più gravi come testimonia l'aumento drammatico degli attacchi gravi ad alto impatto.

Uno scenario purtroppo destinato a consolidarsi e a diventare strutturale.
Questo è il mondo che ci aspetta.

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

Ringrazio, a nome di tutti gli Associati e di tutti coloro che lo leggeranno, i Colleghi che hanno dedicato tempo e sforzi alla stesura del Rapporto Clusit 2022.

Oltre 70.000 copie scaricate e più di 400 articoli pubblicati nel 2021, 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

Nel 2021 gli attacchi nel mondo sono aumentati del 10% rispetto all'anno precedente, e sono sempre più gravi. Le nuove modalità di attacco dimostrano che i cyber criminali sono sempre più sofisticati e in grado di fare rete con la criminalità organizzata. Questo è quanto emerge dal nuovo Rapporto Clusit.

Gli attacchi crescono in quantità e in "qualità": la classificazione dei ricercatori di Clusit si basa anche su una valutazione dei **livelli di impatto** dei singoli incidenti, che tiene in considerazione aspetti di immagine, economici, sociali e le ripercussioni dal punto di vista geopolitico.

La geografia degli attacchi. Gli attacchi classificati dai ricercatori di Clusit si sono verificati nel **45% dei casi** ancora nel continente americano (in leggero calo rispetto al 2020). Sono invece cresciuti gli attacchi verso l'**Europa**, che superano un quinto del totale (**21%**, contro il 16% dell'anno precedente), e verso l'**Asia** (**12%**, rispetto al 10% del 2020). Resta sostanzialmente invariata la situazione degli attacchi verso **Oceania** (**2%**) e **Africa** (**1%**).

Severità degli attacchi in forte aumento. Nel 2021 il **79% degli attacchi** rilevati ha avuto un **impatto "elevato"**, contro il 50% dello scorso anno. In dettaglio, il 32% è stato caratterizzato da una severity "critica" e il 47% "alta". A fronte di queste percentuali, sono diminuiti invece gli attacchi di impatto "medio" (-13%) e "basso" (-17%).

Gli attacchi cyber nel 2021: quali finalità? Il **cybercrime** si conferma la motivazione dell'**86% dei cyber attacchi**, in crescita rispetto all'81% del 2020 (+16% in termini assoluti), un trend che non accenna a diminuire. Tra gli attacchi gravi di dominio pubblico, l'**11%** è riferibile ad attività di Espionage e il **2%** a campagne di Information Warfare.

Cyber attacchi nel 2021: chi è stato colpito e perché. Per la prima volta dopo diversi anni i ricercatori di Clusit rilevano che l obiettivo più colpito non è più quello dei "Multiple targets", ovvero i cyber criminali non colpiscono più in maniera indifferenziata obiettivi molteplici, ma **mirano a bersagli ben precisi**: al primo posto c è l obiettivo **governativo/militare**, con il **15%** degli attacchi totali, in crescita del **36,4%** rispetto all'anno precedente; segue il settore **informatico**, colpito nel **14%** dei casi (**+3,3%** rispetto al 2020), gli **obiettivi multipli** (**13%**, in discesa dell'8%) e la **sanità**, che rappresenta al pari il **13%** del totale degli obiettivi colpiti, in crescita del **24,8%** rispetto ai dodici mesi precedenti. Segue l'**istruzione**, pari al **9%** del totale, sostanzialmente stabile rispetto al 2020.

Ci siamo avvalsi anche in questa edizione dei dati relativi agli attacchi rilevati dal **Security Operations Center (SOC) di FASTWEB**, che nel 2021 ha registrato oltre 42 milioni di eventi di sicurezza, con un aumento del 16% rispetto a quelli rilevati l'anno precedente**.** Tra i trend cybersecurity più rilevanti del 2021 per l'Italia, si osserva la continua crescita dei malware e botnet, con un numero di server compromessi che fa segnare un netto +58%. La penetrazione delle infezioni inizia ad essere rilevante anche nel mobile, con la presenza nelle prime posizioni di FluBot, un malware per **dispositivi** Android che si distribuisce attraverso link di phishing condivisi grazie a SMS o app di messaggistica. In Italia i settori più colpiti si confermano il **Finance/Insurance** e la **Pubblica Amministrazione**, obiettivi

che insieme costituiscono circa il **50%** dei casi. A questi si aggiunge quello dell'**Industria** che ha presentato l'**aumento più significativo, dal 7% del 2020 al 18% del 2021**.

Segue un'analisi realizzata da Libraesva sull'**evoluzione dell'e-mail security in Italia**, da cui emerge che le minacce si fanno sempre più subdole e che le tecniche di attacco evolvono in direzioni più difficili da monitorare, da quantificare e anche da intercettare. In questo scenario, le organizzazioni devono assolutamente restare al passo con l'evoluzione delle tecniche di attacco le quali seguono una naturale evoluzione verso lo sfruttamento dei punti di ingresso più deboli, inclusi gli individui. Il problema si fa meno tecnico, più metodologico e sempre più specialistico.
L'analisi degli attacchi in Italia è poi completata dalle rilevazioni e segnalazioni della **Polizia Postale e delle Comunicazioni**, che ci hanno fornito dati e informazioni estremamente interessanti su attività ed operazioni svolte nel corso degli ultimi 12 mesi.

Presentiamo a questo punto l'abituale capitolo dedicato al settore FINANCE, con un'analisi sul **Cyber-crime nel settore finanziario in Europa**, a cura di IBM, ed un contributo realizzato da quattro esperti del CERT di Banca d'Italia sull'**evoluzione delle tecniche di ingegneria sociale e il loro utilizzo negli attacchi contro gli utenti di servizi di pagamento online.**

Seguono due SURVEY.
La prima sulla **valutazione del livello di compliance e sicurezza dei Cloud Provider**, realizzata dagli Osservatori del Politecnico di Milano.
La seconda, realizzata da Netwrix tramite **interviste a 732 amministratori di sistema** di diverse aziende e di tutto il mondo, per capire in che modo Il 2021 è stato un anno caratterizzato da diversi avvenimenti importanti che hanno portato il mondo della sicurezza informatica a doversi adattare ai nuovi scenari.

Questi saranno infine i temi trattati nella sezione FOCUS ON:

- **"Pubbliche amministrazioni italiane sotto assedio"**, a cura di Fortinet
- **"Cybersecurity automotive : rischi, normative e mitigazioni"**, di Andrea Tomassi e Giuseppe Faranda Cordella
- **"L'importanza della incorporazione della Cybersecurity nelle strategie di Resilienza Operativa",** di Federica Maria Rita Livelli.

Analisi dei principali cyber attacchi noti del 2021 a livello globale

Introduzione

In questo aggiornamento del Rapporto CLUSIT, giunto ormai al suo undicesimo anno di pubblicazione, analizziamo i **2.049** cyber attacchi noti che abbiamo individuato e classificato nel 2021 a livello globale (Italia inclusa) e li confrontiamo con quelli del triennio precedente[1].
Nell'ambito di questa ricerca, in 11 anni abbiamo identificato, classificato e valutato oltre **14.000** attacchi informatici gravi (in media 1.274 all'anno, più di **100** al mese). Di questi, **7.144** si sono verificati negli ultimi 4 anni, dimostrando un'accelerazione impressionante nella frequenza delle minacce cibernetiche.
La metodologia utilizzata per svolgere questa analisi è stata raffinata ed aggiornata nel tempo, sia dal punto di vista del numero e della qualità delle fonti utilizzate, che della quantità di variabili impiegate per descrivere i diversi fenomeni e, a partire da questa edizione, delle tassonomie utilizzate per classificare i dati, che sono state completamente riviste ed aggiornate per aderire quanto più possibile a standard riconosciuti a livello internazionale.
In particolare il sistema di classificazione dei settori merceologici che da quest'anno abbiamo adottato per mappare le vittime di attacchi informatici è derivato dall'**ISIC** (International Standard Industrial Classification of All Economic Activities) delle Nazioni Unite e dalla **NACE** della Commissione Europea (Nomenclature statistique des activités économiques dans la Communauté Européenne)[2].
La classificazione delle tecniche di attacco è ora derivata dalla **Threat Taxonomy** dell'ENISA, dalla **Open Threat Taxonomy** e da diversi altri framework[3].
La classificazione degli attaccanti deriva invece dalla nostra esperienza sul campo e rappresenta una mappatura tra le principali famiglie di "bad actors" e le motivazioni degli attacchi osservati.
Oltre ad aver rivisto completamente il modello abbiamo anche riclassificato gli attacchi dell'ultimo triennio (**5.095**) per renderli confrontabili con quelli del 2021 (**2.049**) e non perdere così la visione "prospettica" dei fenomeni, che è una delle caratteristiche più distintive di questa ricerca.

---

1 Dal primo gennaio 2018 al 31 dicembre 2020

2 Utilizzata anche in Italia come tassonomia ATECO, redatta dall'ISTAT

3 "A Taxonomy of Cyber Events Affecting Communities", IEEE, 2011; "AVOIDIT: A Cyber Attack Taxonomy", Department of Computer Science University of Memphis; "Evaluation of Comprehensive Taxonomies for Information Technology Threats", SANS Institute

Considerazioni sul campione

Le nostre analisi ed i relativi commenti si riferiscono ad un campione necessariamente *parziale*, per quanto ormai corposo e statisticamente significativo, rispetto al numero degli attacchi gravi effettivamente avvenuti nel periodo in esame.
Questo accade sia perché *un buon numero* di aggressioni non diventano *mai* di dominio pubblico, oppure lo diventano *ad anni di distanza* (solitamente quanto più gli attacchi sono sofisticati), sia perché in molti casi è interesse delle vittime non pubblicizzare gli attacchi subiti, se non costretti dalle circostanze o da obblighi normativi particolari.
Ad ogni modo la natura delle fonti aperte utilizzate per realizzare questo studio introduce inevitabilmente un *bias*[4] nel campione, all'interno del quale sono certamente meglio rappresentati gli attacchi realizzati per finalità cyber criminali o di hacktivism rispetto a quelli derivanti da attività di cyber espionage ed information warfare, che emergono più difficilmente.
In sintesi, considerato che il nostro campione è realizzato esclusivamente a partire da notizie di pubblico dominio, e che al loro interno alcune classi di incidenti sono sistematicamente sottorappresentate, è plausibile supporre che questa analisi dipinga uno scenario *meno critico rispetto alla situazione sul campo*.

Origini ed evoluzione di questa analisi

Quando nell'ormai remoto 2012 abbiamo iniziato questa ricerca, poi pubblicata nella prima edizione del Rapporto Clusit, definendo (ingenuamente) il 2011 come "l'Annus Horribilis della sicurezza informatica", gli scenari erano radicalmente diversi e gli impatti geopolitici e socio-economici delle minacce cibernetiche rappresentavano ancora un problema relativamente minore, suscitando interesse e preoccupazione solo tra pochi esperti di ICT Security.
Giova qui ricordare che all'epoca i rischi "cyber" non erano nemmeno considerati all'interno del Global Risk Report del World Economic Forum[5] (nel quale sono stati introdotti solo nel 2015) ma che già dal 2019 sono assurti al primo posto per impatto e probabilità di accadimento, insieme ai disastri naturali ed agli effetti globali del *climate change*.
Lo scopo originario per il quale è nato questo lavoro era dunque di elevare la consapevolezza e migliorare la comprensione del pubblico italiano rispetto all'evoluzione delle minacce cibernetiche, nell'ipotesi (poi dimostratasi drammaticamente esatta) che il problema sarebbe inevitabilmente degenerato con grande rapidità nei mesi ed anni successivi, e che la pressoché totale mancanza di sensibilità in materia fosse *una delle principali ragioni* del peggioramento degli scenari.
Questa finalità rimane ancora oggi assolutamente centrale, ma data la criticità della situazione che si è venuta a creare nel frattempo, e considerati i rischi sistemici, esistenziali che

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

[5] https://www.weforum.org/reports/the-global-risks-report-2021

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 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 livelli crescenti di "*Severity*", il che ci consente di realizzare un'analisi dei differenti impatti causati dalle diverse categorie di attaccanti rispetto alle varie tipologie di vittime, 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.

2021, "la festa è finita"

Anticipando alcune delle conclusioni che seguono possiamo affermare che se il 2020 era stato l'anno *peggiore di sempre* in termini di evoluzione delle minacce "cyber" e dei relativi impatti, evidenziando un trend persistente di crescita degli attacchi, della loro gravità e dei danni conseguenti, tale tendenza negativa si è confermata ampiamente anche nel 2021.
Osservando la situazione dal punto di vista quantitativo, confrontando i numeri del 2018 con quelli del 2021 la crescita degli attacchi gravi è stata quasi del **32%** (da 1.554 a 2.049). Detto diversamente, in 4 anni la media mensile di attacchi gravi a livello globale è passata da 130 a **171**.
Oltre a una maggiore frequenza, la valutazione della Severity media di questi attacchi (indice di gravità degli attacchi analizzati) nei confronti di alcune categorie di vittime è drasticamente peggiorata, agendo da significativo moltiplicatore dei danni.
L'osservazione di queste dinamiche conferma la nostra convinzione che a partire da 4 anni fa sia avvenuto un vero e proprio *cambiamento epocale* nei livelli globali di cyber-insicurezza, causato dall'evoluzione rapidissima degli attori di minaccia, delle modalità, della pervasività e dell'efficacia degli attacchi, al quale non è corrisposto un incremento sufficiente delle contromisure adottate dai difensori.
Come previsto pertanto si sono realizzate appieno le tendenze più pericolose descritte in questo Rapporto già nel 2017, che avevamo definito come "l'anno del trionfo del malware, degli attacchi industrializzati realizzati su scala planetaria contro bersagli multipli, dell'alterazione di massa della percezione e della definitiva discesa in campo degli Stati come attori di minaccia".
Allo stesso tempo dobbiamo tenere presente che Cybercrime, Cyber Espionage ed Information Warfare del 2021 non sono certamente più quelli del 2017, anche se continuiamo ad utilizzare le stesse denominazioni, e mostrano un cambiamento *qualitativo* straordinario.
A causa di ciò, già da anni siamo di fronte a problematiche che per natura, gravità e dimensione travalicano costantemente i confini dell'ICT e della stessa Cyber Security, ed hanno impatti profondi, duraturi e sistemici su ogni aspetto della società, della politica, dell'eco-

nomia e della geopolitica.
La crescita drammatica delle perdite derivanti da questa situazione di Far West digitale, stimate in 1 trilione di dollari per il 2020 e 6 trilioni per il 2021[6], dovrebbe far riflettere molto seriamente. Stiamo parlando di dinamiche deleterie, che rappresentano un'emergenza globale concreta, un "clear and present danger"[7] ed incidono ormai per una percentuale significativa del GDP mondiale, con un tasso di peggioramento annuale a 2 cifre ed un valore già pari a 4 volte il PIL italiano.

Bisogna ormai ammettere che in ambito ICT l'approccio basato sul *laissez-faire* da parte della politica, sulla mancanza di chiare responsabilità dei produttori di tecnologia e sul *"carpe diem"* degli utenti finali, ha definitivamente mostrato tutti i suoi limiti, ed oggi rappresenta *una minaccia in sè* per il benessere della società e dei suoi membri, generando rischi *inaccettabili* per una civiltà che ormai basa la sua sopravvivenza sul buon funzionamento del digitale.
Riassumendo le nostre impressioni sulle tendenze in atto, con una battuta affermiamo che "la festa è finita". I dati dimostrano che il tempo della sottovalutazione dei problemi, del rimandare l'adozione di contromisure efficaci (evitando di investire quanto necessario) è terminato.
In questo senso auspichiamo che il PNRR (Piano nazionale di ripresa e resilienza), che complessivamente alloca circa 45 miliardi di euro per la "transizione digitale", possa rappresentare per l'Italia l'occasione di mettersi al passo e colmare le proprie lacune (anche) in ambito cyber, e non abbia come esito un ampliamento della superficie di attacco esposta dal Paese, ma una sua complessiva, significativa riduzione.
Per realizzarsi, questo obiettivo (assolutamente prioritario e strategico) richiederà una governance stringente in ottica cyber security di tutti i progetti di digitalizzazione previsti dal piano, una vision politica che non accetti compromessi e pressioni esterne, e (finalmente) la valorizzazione delle risorse umane con competenze cyber (in termini di talenti e di esperienze) del Paese, ed il loro sviluppo in termini quantitativi e qualitativi.
Confidando che anche quest'anno il Rapporto CLUSIT possa apportare un contributo significativo al dibattito nazionale in merito all'accelerazione crescente delle problematiche globali di sicurezza cibernetica ed alle sue ricadute sul benessere del Paese, auguriamo a tutti una buona lettura.

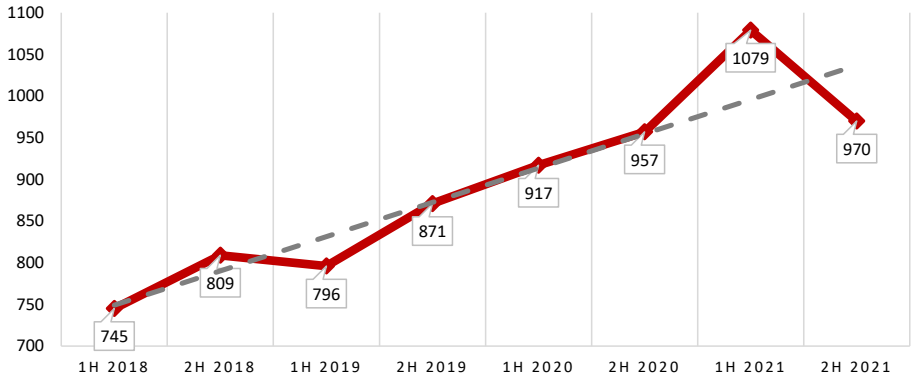
[6] https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

[7] "a risk or threat to safety or other public interests that is serious and imminent"

Analisi dei principali cyber attacchi noti a livello globale del 2018-2020 e del 2021

In questa sezione, come di consueto, offriamo una panoramica degli incidenti di sicurezza più significativi avvenuti a livello globale nell'anno precedente, confrontandoli con i dati raccolti nei 3 anni precedenti[8].
Lo studio si basa su un campione che al 31 dicembre 2021 è costituito da **14.010** attacchi noti di particolare gravità avvenuti nel mondo dal primo gennaio 2011, 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.

Attacchi per semestre 1H 2018 - 2H 2021

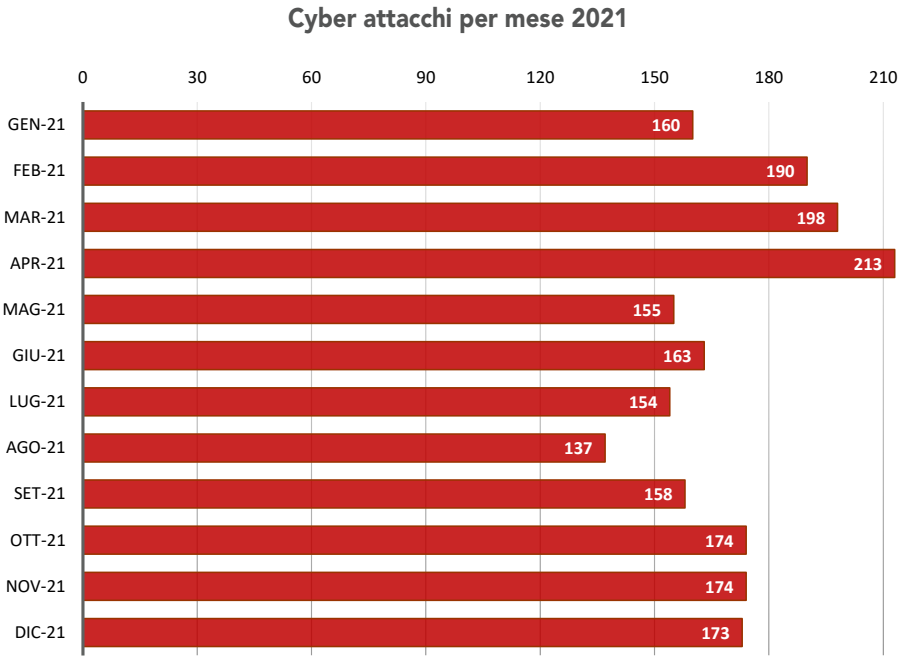


© Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia

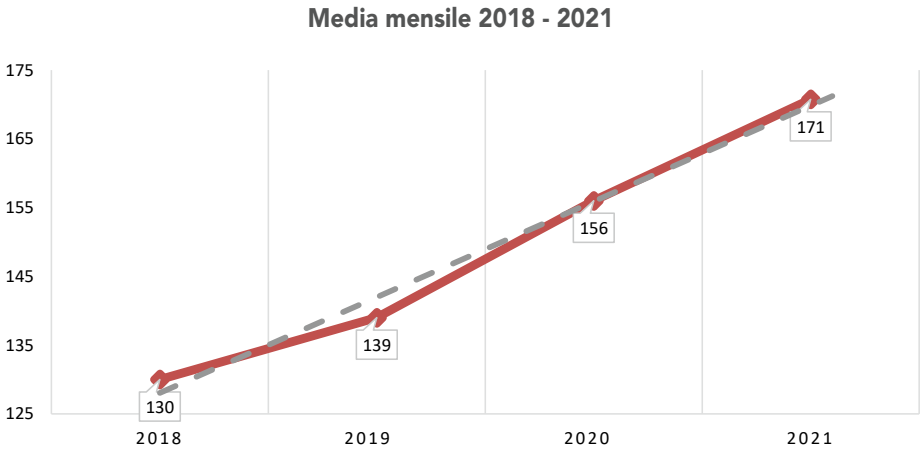
Il nostro campione comprende complessivamente **7.144** attacchi classificati tra il gennaio 2018 e il dicembre 2021 (oltre la metà del totale su 11 anni), di cui **1.874** nel 2020, **2.049** nel 2021, con una media complessiva è di 106 attacchi gravi al mese nell'intero periodo (erano 39 nel 2011, 130 nel 2018, e sono **171** nel 2021). Il picco massimo di sempre si è avuto ad aprile 2021 (213 attacchi).

[8] Pur avendo iniziato questa ricerca nel 2011, oggi ha poco senso fare confronti con gli anni precedenti al 2018

Questa la distribuzione mensile degli attacchi registrati nel 2021.



Di seguito una rappresentazione sintetica delle medie mensili negli ultimi 4 anni.



© Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia

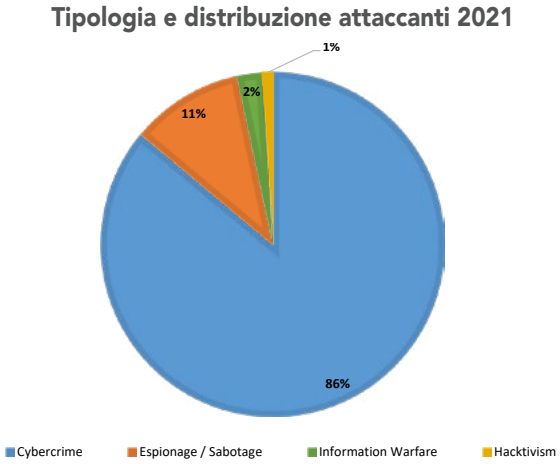
Le tre tabelle e i grafici seguenti rappresentano una sintesi dell'analisi dei dati che abbiamo raccolto. Come in passato abbiamo evidenziato nella colonna più a destra le tendenze osservate.

Avendo modificato a fondo le tassonomie utilizzate per la classificazione degli attacchi presentiamo il confronto dei dati a partire dal 2018, rimandando alle edizioni precedenti del Rapporto Clusit per i dati relativi al periodo 2011-2017.

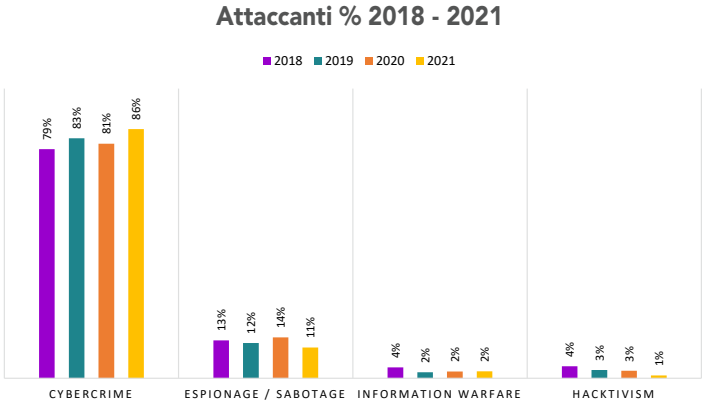
Distribuzione degli attaccanti per tipologia (2018 – 2021)

ATTACCANTI PER TIPOLOGIA	2018	2019	2020	2021	2021 su 2020	Trend 2021
Cybercrime	1.229	1.381	1.518	1.763	16.1%	↑
Espionage-Sabotage	203	203	264	217	-17.8%	↘
Information Warfare	58	35	44	49	11.4%	↗
Hacktivism	64	48	48	20	-58.3%	↓
Espionage-Sabotage + Inf. Warfare	261	238	308	266	-13.6%	↘
Totale	1.554	1.667	1.874	2.049	9.3%	

Per quanto riguarda de tipologie di attaccanti, la nuova tassonomia include le consuete **4** macro-categorie, suddivise però ulteriormente in **13** sottocategorie (qui non riportate per semplicità).
Rispetto al 2020 il numero di attacchi gravi di dominio pubblico che abbiamo raccolto nel 2021 è in crescita del **9,3%** (1.874 contro 2.049). In termini assoluti nel 2021 la categoria "Cybercrime" ha fatto registrare il numero di attacchi più elevato degli ultimi 11 anni.
Dal campione emerge chiaramente che rispetto al 2020 le attività riferibili ad attacchi della categoria "**Hacktivism**" diminuiscono ancora sensibilmente (**-58,3%** in termini percentuali), mentre nel 2021 sono in aumento sia gli attacchi compiuti per finalità di "**Cybercrime**" (**+16,1%**) che quelli riferibili a "**Information Warfare**" (**+11,4%**).
Diminuiscono gli attacchi classificati come attività di "**Cyber Espionage**" (**-17,8%**) dopo il picco straordinario del 2020 (dovuti principalmente a spionaggio relativo allo sviluppo di vaccini e cure per il Covid-19).
Va sottolineato che, rispetto al passato, oggi in alcuni casi risulta più difficile distinguere nettamente tra "Cyber Espionage" e "Information Warfare": sommando gli attacchi di entrambe le categorie, nel 2021 tali attacchi rappresentano il **13%** del totale (erano il 16% nel 2020).



© Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia



© Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia

L'**Hacktivism** diminuisce ulteriormente, passando dal 4% dei casi analizzati nel 2018 al **1%** del 2021.

Per quanto riguarda le attività di **Espionage** (anche a causa della scarsità di informazioni pubbliche in merito) la loro percentuale rispetto al totale degli attacchi rilevati nel 2021 si attesta al **11%**, mentre l'**Information Warfare** rimane stabile al **2%** (crescendo in numeri assoluti del 11.4%).

Percentualmente il **Cybercrime** nel 2021 sale al **86%** del totale (dal 81% del 2020), passando da 1.518 attacchi nel 2020 a 1.763 nel 2021.

Distribuzione delle vittime per categoria (2018 – 2021)

Come anticipato nell'introduzione, da quest'anno abbiamo introdotto una tassonomia delle vittime derivata da standard internazionali[9], articolata su **20** macro-categorie merceologiche e **141** sotto-categorie. Per consentire un confronto con gli anni precedenti, abbiamo riclassificato anche tutti gli attacchi già analizzati nel triennio 2018-2020.

VITTIME PER CATEGORIA	2018	2019	2020	2021	2021 su 2020	TREND 2021
Gov. / Mil. / LE	220	233	225	307	36.4%	↑
ICT	191	233	269	278	3.3%	↗
Multiple Targets	326	406	401	274	-31.7%	↓
Healthcare	161	186	210	262	24.8%	↗
Education	106	140	174	174	0.0%	-
Financial / Insurance	162	107	122	137	12.3%	↗
Professional / Scientific / Technical	18	19	65	82	26.2%	↑
Wholesale / Retail	33	45	54	82	51.9%	↑
Transportation / Storage	33	16	39	75	92.3%	↑
Manufacturing	34	36	65	72	10.8%	↗
News / Multimedia	70	69	43	69	60.5%	↑
Organizations	40	35	46	52	13.0%	↗
Energy / Utilities	24	25	39	43	10.3%	↗
Arts / Entertainment	68	55	40	42	5.0%	↗
Telco	13	19	32	36	12.5%	↗
Hospitability	44	27	22	30	36.4%	↑
Other Services	9	14	15	25	66.7%	↑
Agriculture / Forestry / Fishing	0	0	5	6	20.0%	↗

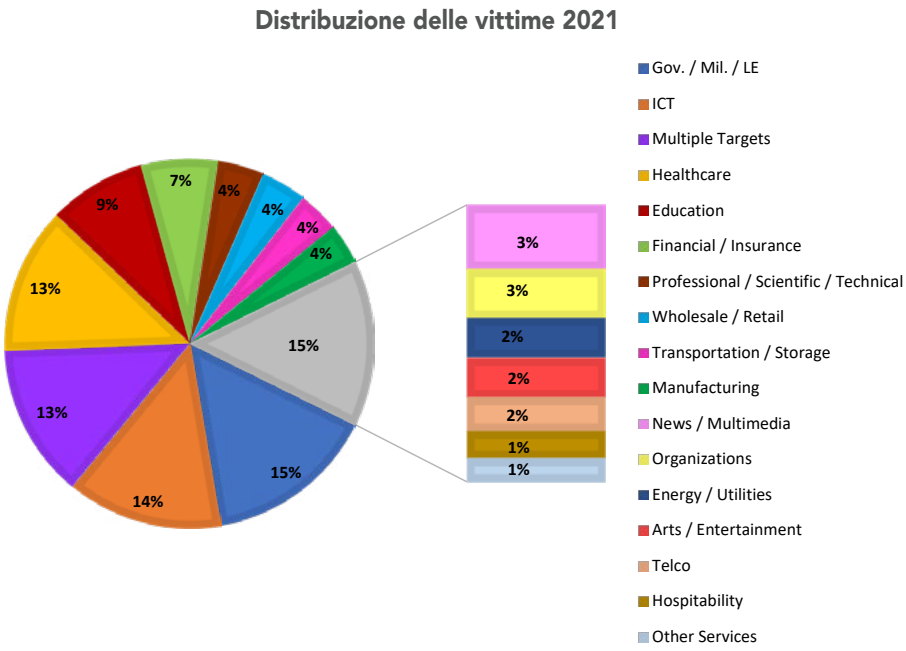
[9] **ISIC** (International Standard Industrial Classification of All Economic Activities) delle Nazioni Unite e **NACE** della Commissione Europea (Nomenclature statistique des activités économiques dans la Communauté Européenne)

Construction	1	2	7	3	-57.1%	↓
Mining / Quarrying	1	0	1	0	-100.0%	-
TOTALE	**1.554**	**1.667**	**1.874**	**2.049**		

Rispetto al 2020, nel 2021 la crescita maggiore nel numero di attacchi gravi si osserva verso le categorie "Transportation / Storage" (**+93,3%**), "Other Services" (**+66,7%**), "News / Multimedia" (**+60,5%**), "Wholesale / Retail" (**+51,9%**), "Gov / Mil / LE" (**+36,4%**), "Hospitability" (**+36,4%**), seguite da "Professional / Scientific / Technical" (**+26,2%**) ed "Healthcare" (**+24,8%**).

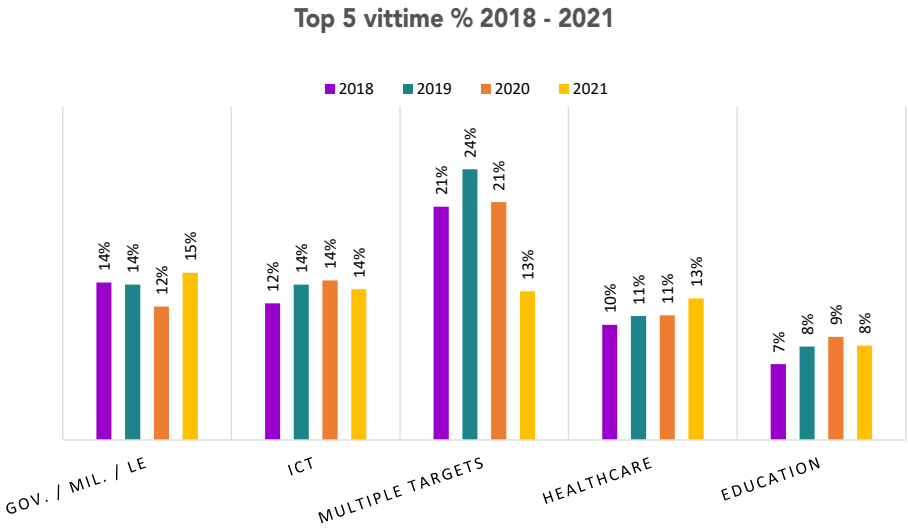
Crescono in misura minore anche quasi tutte le altre categorie, con l'esclusione di "Multiple Targets" (**-31,7%**), "Construction" (**-57,1%**) e "Mining / Quarring" (che non registra alcun attacco), mentre "Education" rimane invariata (al quinto posto assoluto per numero di attacchi).

La categoria "Multiple targets" è stata mantenuta anche nella nuova tassonomia delle vittime per rendere conto degli attacchi gravi compiuti in parallelo dallo stesso gruppo di attaccanti contro numerose organizzazioni appartenenti a categorie differenti. Di conseguenza una parte degli attacchi verso vittime appartenenti a tutte le altre categorie confluiscono in questa categoria, che nel 2021 rappresenta il **13%** del totale degli attacchi (-31,7% rispetto al 2020).
Il calo degli attacchi verso la categoria "Multiple Targets" rappresenta un cambio di strategia da parte degli attaccanti ed è un importante campanello di allarme, dal momento che deriva dall'aumento di attacchi gravi mirati verso singoli bersagli (in particolare di tipo ransomware con l'aggravante della "double extortion", cioè della minaccia di diffondere i dati rubati alle vittime qualora non paghino il riscatto).



In termini percentuali nel 2021 la categoria "Government" torna al primo posto assoluto (**15%** del totale).
Al secondo posto "ICT", con il **14%** degli attacchi totali, al terzo "Multiple Targets" al **13%**, in diminuzione rispetto al passato per le ragioni sopra esposte, ed al quarto il settore "Healthcare", sempre con il **13%**.

Le successive 6 categorie merceologiche (che sommate rappresentano il 32% degli attacchi rilevati) sono comprese tra il 9% ed il 4% degli attacchi, dimostrando ancora una volta che gli attaccanti si muovono a tutto campo, e che tutti sono potenziali bersagli. Le restanti 10 categorie rappresentano il 15% residuo sul totale.

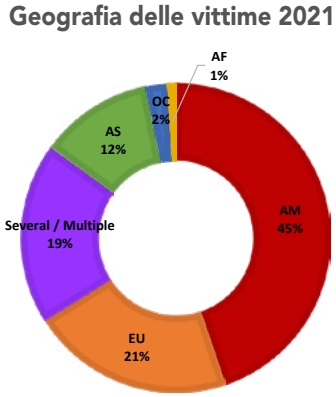


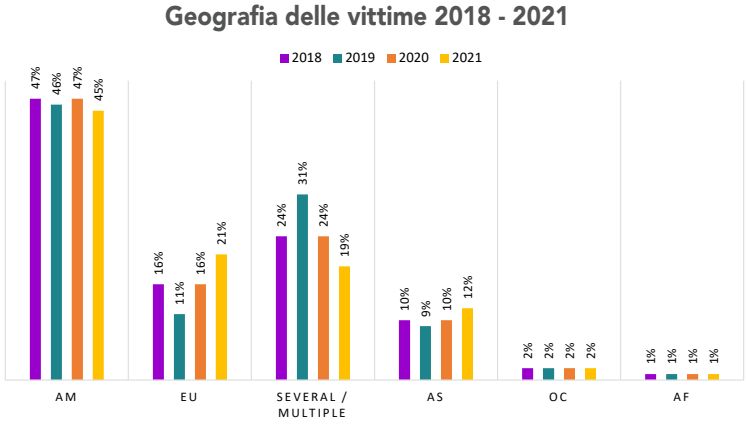
© Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia

Osservando questo grafico delle prime 5 categorie più colpite tra il 2018 ed il 2021, si può apprezzare la netta variazione della categoria "Multiple Targets" rispetto alle altre.

Distribuzione generale delle vittime per area geografica (2021)

La classificazione delle vittime per nazione di appartenenza viene qui rappresentata su base continentale.
Nel 2021 rimangono sostanzialmente invariate le vittime di area americana (dal 47% al **45%**), mentre gli attacchi verso realtà basate in Europa aumentano sensibilmente (dal 15% al **22%**) e crescono leggermente quelli rilevati contro organizzazioni asiatiche (dal 10% al 12%).
Percentualmente diminuiscono gli attacchi gravi verso bersagli con sedi distribuite in diversi Paesi (categoria "Several / Multiple"), che dal 24% del 2020 passano al **19%**.





Distribuzione delle tecniche di attacco (2018 – 2021)

Come già detto per la classificazione delle vittime, da quest'anno introduciamo una nuova tassonomia delle tecniche di attacco derivata da framework internazionali[10], articolata su **8** macro-categorie e **59** sotto-categorie.

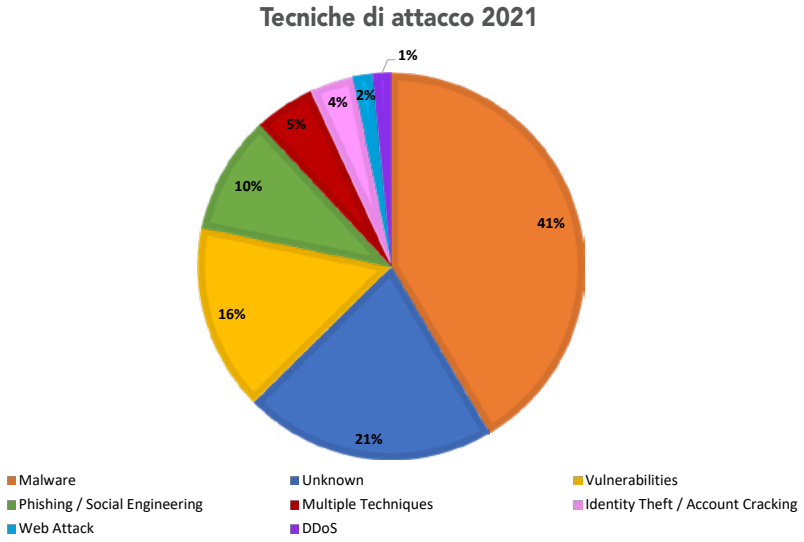
Tecniche di attacco	2018	2019	2020	2021	2021 su 2020	TREND
Malware	601	737	775	850	9.7%	↗
Unknown	429	309	372	433	16.4%	↗
Vulnerabilities	143	158	200	320	60.0%	↑
Phishing / Social Engineering	170	291	299	203	-32.1%	↓
Multiple Techniques	64	57	86	103	19.8%	↗
Identity Theft / Account Cracking	67	71	90	76	-15.6%	↘
Web Attack	43	21	18	33	83.3%	↑
DDoS	37	23	34	31	-8.8%	↘
TOTALE	**1.554**	**1.667**	**1.874**	**2.049**		

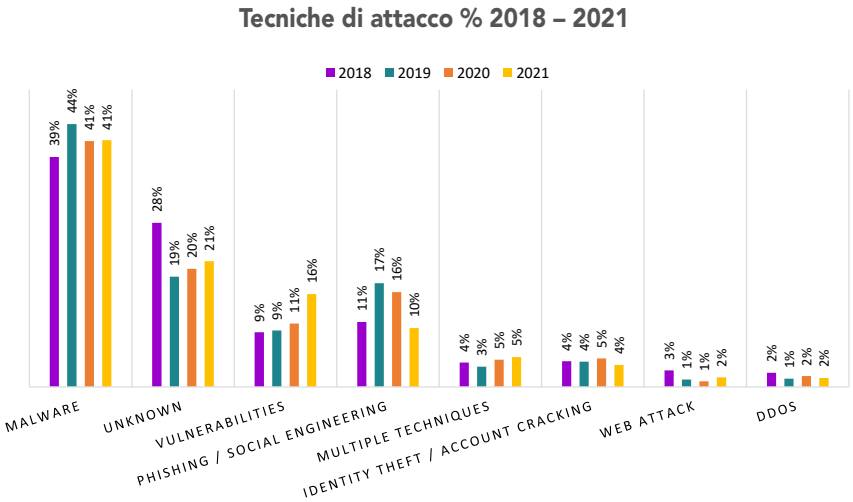
Nel 2021 la categoria che mostra numeri assoluti maggiori è "Malware" (**+9,7%**), che rappresenta il **41%** del totale. Le tecniche sconosciute (categoria "Unknown") tornano al secondo posto, con una aumento del **16,4%** rispetto al 2020, superando la categoria "Vulnerabilità" (che peraltro fa segnare un preoccupante **+60%**) e "Phishing / Social Engineering" (in calo, -**32,1%**), mentre "Tecniche Multiple" sale del **+19.8**%.
Rispetto al totale del campione gli attacchi gravi con finalità di "Distributed Denial of Service" diminuiscono del **8,8%**, così come quelli realizzati tramite "Identity Theft / Account Hacking" (**-15,6%**).

In sostanza gli attaccanti possono fare affidamento sull'efficacia del Malware, prodotto industrialmente a costi decrescenti, e sullo sfruttamento di Vulnerabilità (note o meno), per colpire più della metà dei loro obiettivi (**57%** dei casi analizzati).
Il **21%** di "tecniche sconosciute" (in crescita del **+16,4%**) è principalmente dovuto al fatto che molti attacchi (un quinto del totale) diventano di dominio pubblico a seguito di un

[10] Non esistendo una tassonomia standard per le tecniche di attacco, le 55 sotto-categorie delle nostre 8 macro categorie sono state derivate dall'analisi dalla Threat Taxonomy dell'ENISA, dalla Open Threat Taxonomy e di diversi altri framework.

"data breach", nel qual caso le normative impongono una notifica agli interessati, ma non di fornire una descrizione precisa delle modalità dell'attacco (che normalmente quindi non viene fornita).

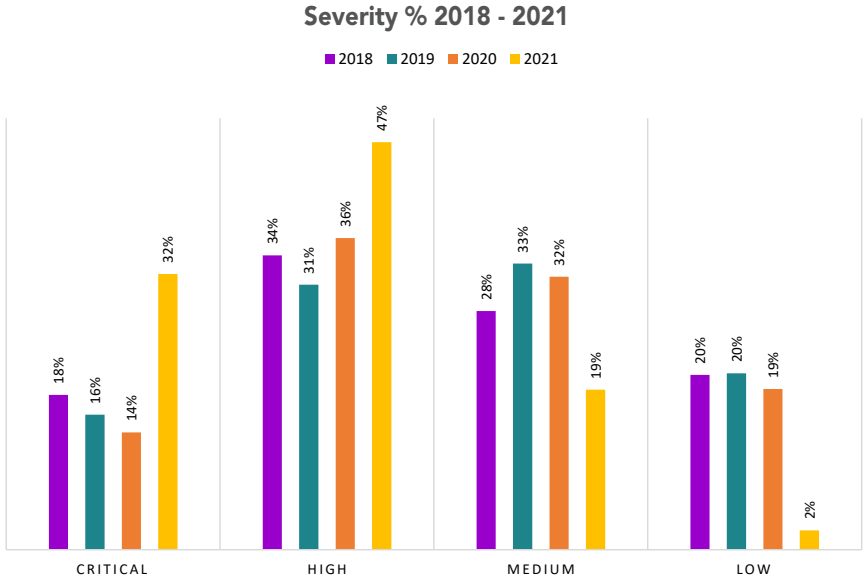




Analisi della "Severity" degli attacchi

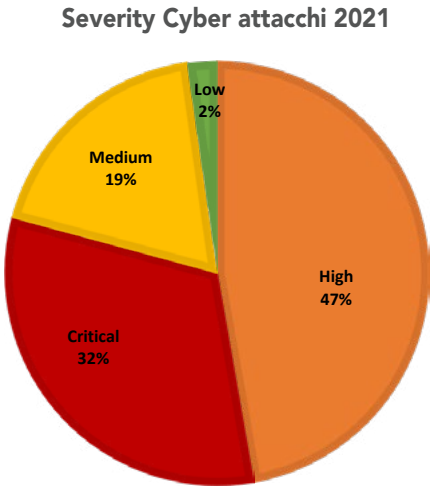
Come anticipato nell'introduzione, anche per il 2021 presentiamo una valutazione della Severity degli attacchi analizzati.
Obiettivo di questa analisi infatti è individuare non solo le categorie di attaccanti, vittime e tecniche di attacco che crescono maggiormente in termini assoluti nel periodo osservato, ma anche come evolvono gli **impatti** degli attacchi, partendo dalla constatazione che spesso queste due valutazioni non coincidono (p.es. in certi casi all'aumento del numero di attacchi da parte di una certa categoria di attaccanti non corrisponde un aumento della loro Severity media, etc).

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.
Nella nuova classificazione abbiamo definito quattro categorie o livelli di **impatto** (considerato che stiamo comunque analizzando un campione di attacchi già tutti definiti come "gravi"): Basso, Medio, Alto e Critico.
Applicando la nuova modalità di valutazione degli impatti ai dati degli ultimi 4 anni, emergono fenomeni molto interessanti:



© Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia

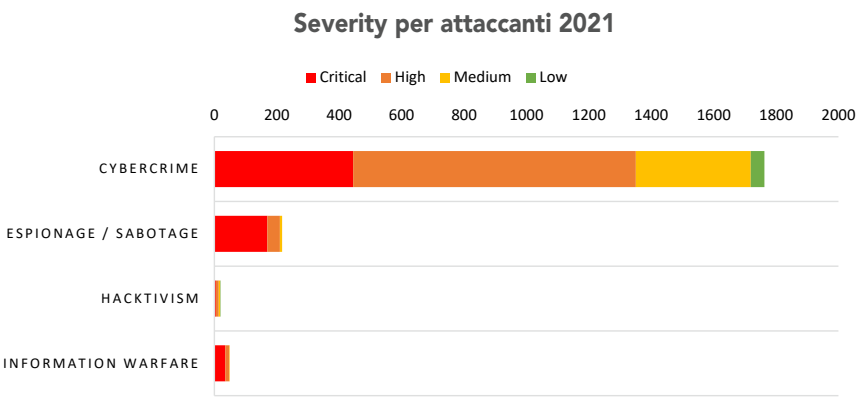
Nel 2020 gli attacchi con impatto "Critico" rappresentavano il **14%** del totale, quelli di livello "Alto" il **36%**, quelli di livello "Medio" il **32%** ed infine quelli di livello "Basso" il **19%**. Complessivamente, gli attacchi gravi con effetti molto importanti (High) o devastanti (Critical) nel 2020 erano il **50%** del campione.
Nel 2021 la situazione è molto diversa e francamente impressionante: gli attacchi gravi con effetti molto importanti (High) sono il **47%**, quelli devastanti (Critical) rappresentano il **32%**, quelli di impatto significativo (Medium) il **19%**, e quelli con impatto basso solo il **2%**. In questo caso gli attacchi con impatto Critical e High sono il **79%**.



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

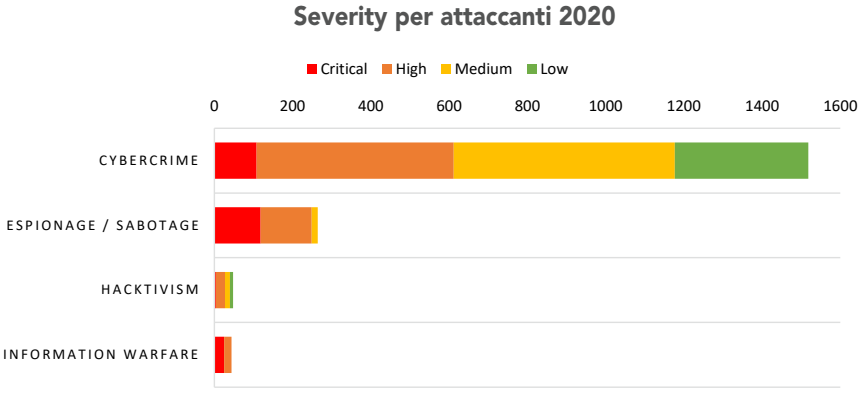
Severity per tipologia di attaccante

Di seguito il raggruppamento per tipologia di attaccante. In passato il maggior numero di attacchi classificati come "Critici" riguardava le categorie Espionage ed Information Warfare, mentre la prevalenza di attacchi con impatto di tipo "Alto" e "Medio" riferiti ad attività cybercriminali si spiegava con la necessità, per questi soggetti, di rimanere relativamente sottotraccia, guadagnando sui grandi numeri più che sul singolo attacco.



© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia - aggiornamento giugno 2021

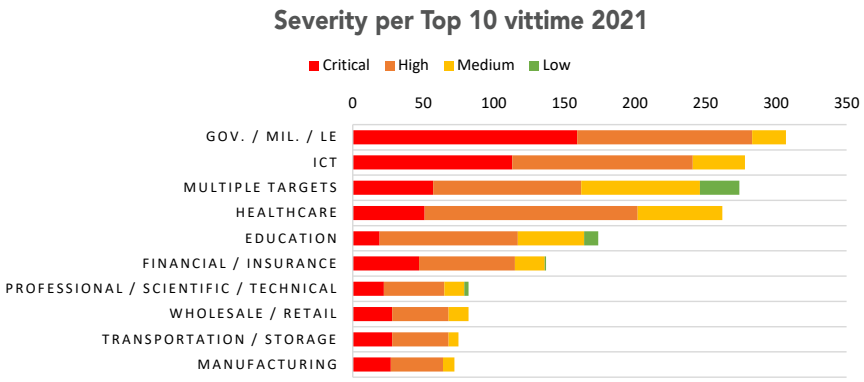
Come si evince confrontando i due grafici, nel 2021 gli attacchi con Severity "Critical" realizzati per finalità cybercriminali sono sensibilmente aumentati rispetto al 2020, il che desta grande preoccupazione e denota chiaramente un cambio di strategia da parte degli attaccanti.



© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia

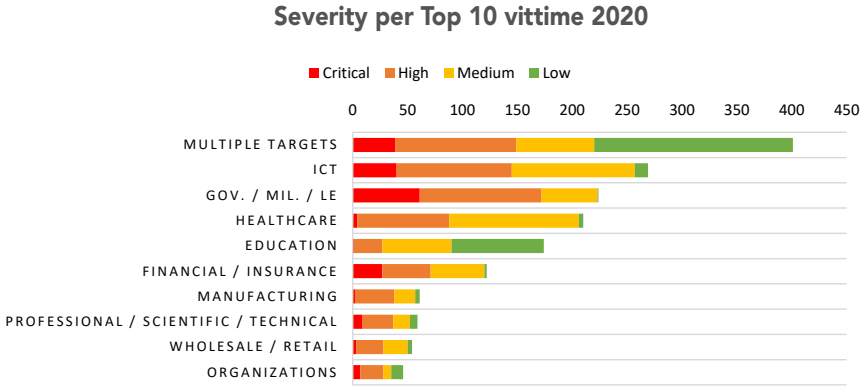
Severity per tipologia di vittima

Per quanto riguarda la distribuzione della Severity rispetto alle categorie di vittime più colpite da attacchi, si può notare come la categoria "Government" abbia subito il maggior numero di attacchi con Severity "Critical", seguita da "ICT", "Multiple Targets", "Healthcare" e "Financial / Insurance", mentre le categorie con il maggior numero di attacchi con impatti di livello "Alto" sono "Healthcare", "Gov", "ICT" e "Education".



© Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia

La situazione era diversa (e complessivamente molto meno grave) nel 2020:

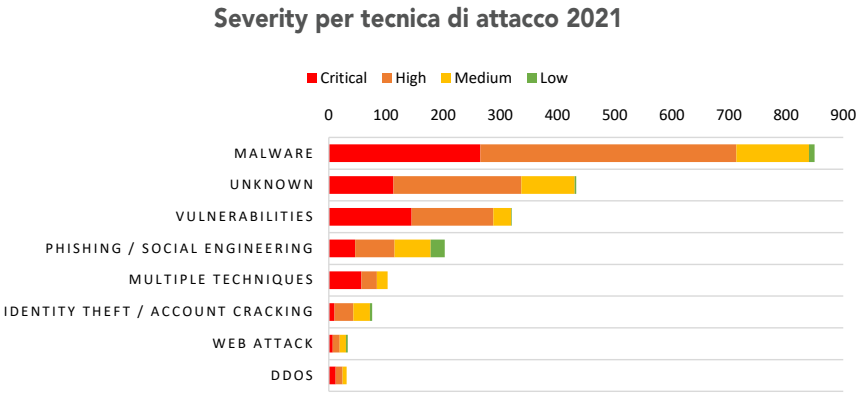


© Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia

L'aumento della Severity degli attacchi avvenuti nel 2021 verso tutte le categorie più colpite è evidente nel confronto tra i due grafici.

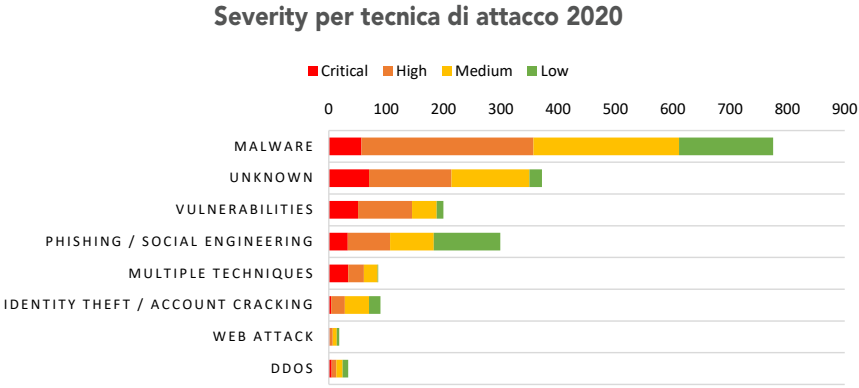
Severity per tecniche di attacco

Dal punto di vista delle tecniche di attacco nel 2021 gli incidenti con impatto più critico sono quelli realizzati tramite Malware, Vulnerabilità, Tecniche sconosciute e Tecniche Multiple.



© Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia

Anche in questo caso emerge chiaramente l'evoluzione negativa del trend, confrontando i dati del 2021 con quelli del 2020:



© Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia

In particolare colpisce l'incremento significativo di attacchi con impatto "Critical" realizzati tramite Malware e Vulnerabilità, compiuti principalmente per finalità cybercriminali.

L'analisi Fastweb della situazione italiana in materia di cyber-crime

Introduzione e visione d'insieme

Prosegue l'impegno di Fastweb nel contribuire a fotografare la situazione del cybercrime in Italia, attraverso un'analisi puntuale dei principali trend, elaborata dal proprio Security Operations Center (SOC) attivo 24 ore su 24 e dai centri di competenza di sicurezza informatica.

I fenomeni del cybercrime nel 2021 continuano a crescere e riprendono un andamento lineare durante l'anno a differenza delle discontinuità e momenti di picco che la pandemia aveva introdotto nel 2020. All'avanzata degli attacchi informatici si è contrapposta una maggiore efficacia delle misure di difesa, grazie anche ad una progressiva **consapevolezza da parte delle aziende rispetto ai rischi informatici** e i conseguenti investimenti indirizzati nell'area Security. Il maggior utilizzo di strumenti digitali ha infatti messo le imprese e la pubblica amministrazione di fronte alla necessità di gestire con attenzione la sicurezza dei propri sistemi informativi, a cui i dipendenti accedono sempre più in maniera remota e distribuita. Questa maggiore attenzione è stata sostenuta dalla diffusione di **programmi strutturati di formazione e awareness**, a cui la stessa Fastweb ha contribuito nel panorama italiano con i corsi erogati della **Fastweb Digital Academy** (FDA).

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, si sono registrati oltre **42 milioni di eventi di sicurezza**, con un **aumento del 16%** rispetto agli eventi rilevati nel Report 2020.

Tra i trend cybersecurity più rilevanti del 2021 si osserva la continua crescita dei **malware e botnet**, con un numero di server compromessi che fa segnare un netto **+58%**. Tra queste minacce, il 34% proviene da Andromeda, una piattaforma utilizzata per distribuire oltre 80 famiglie di malware, seguita da Downadup utilizzata per prendere il controllo totale di un server. La penetrazione delle infezioni inizia ad essere rilevante anche nel **mobile**, con la presenza nelle prime posizioni di FluBot, un malware per **dispositivi** Android che si distribuisce attraverso link di phishing condivisi grazie a SMS o app di messaggistica. Per gli **attacchi zero-day**, ovvero quelle vulnerabilità IT sconosciute dai gestori dell'infrastruttura, il trend è stato costante ma comunque rilevante se si considera la loro pericolosità, in quanto non rilevabili da sistemi di protezione tradizionali.
Rispetto alla distribuzione geografica dei malware, nel 2021 si rileva un aumento del **numero di attacchi da server ospitati in Europa rispetto agli Stati Uniti.** Si sposta dunque la geografia degli attacchi ma non la loro entità, che continua a crescere e va affrontata con l'adozione di sistemi di protezione specifici per singola minaccia e indipendenti dal paese di origine.

Sul fronte degli attacchi **DDoS** (Distributed Denial of Service), nel 2021 sono stati rilevati **2.500 eventi** e circa **18.000 anomalie** riconducibili a possibili attacchi diretti verso i clienti Fastweb. Dopo l'aumento che si era manifestato nel 2020, con un raddoppio degli eventi in alcuni periodi dell'anno a seguito dei forti cambiamenti nel mondo del digitale introdotti dalla pandemia, il dato complessivo del 2021 è tornato a crescere in maniera lineare. I settori più colpiti si confermano il **Finance/Insurance** e la **Pubblica Amministrazione**, obiettivi che insieme costituiscono circa il **50%** dei casi. A questi si aggiunge quello dell'**Industria** che ha presentato l'**aumento più significativo, dal 7% del 2020 al 18% del 2021**.
Nel 2021 sono stati rilevati **46.000 server e device privi di livelli minimi di protezione** e che ancora espongono servizi critici direttamente su Internet. **Il numero di questi server in un anno è però diminuito del 16%,** un trend che continua da diversi anni a dimostrazione che le aziende stanno progressivamente aumentando le proprie linee difensive di base.

Per quanto riguarda la vista sui tentativi di **attacco applicativo,** rivolto cioè ai software dei dispositivi e diretti verso i clienti Fastweb nel 2021, **SQL Injection** e **Cross Site Scripting** continuano ad essere utilizzati in quanto risultano tuttora efficaci. Questo fa emergere l'importanza di seguire le best practices tecnologiche per lo sviluppo di software sicuro e testare continuamente gli applicativi in produzione. Quello che invece è stato uno degli eventi di maggior spicco in ambito applicativo è legato alla vulnerabilità conosciuta come **Log4j,** con una rapida salita all'**83%** nell'ultimo mese del 2021 e che permette ad un attaccante di prendere il controllo remoto di un dispositivo. Si osserva infine che in termini di attacchi applicativi, la provenienza geografica è piuttosto distribuita, dove **l'Italia si posiziona al terzo posto con una percentuale dell'11%,** a conferma che le contromisure devono essere basate su tecnologie di protezione specifiche più che sui paesi di provenienza.
Quest'anno Fastweb ha monitorato anche le minacce afferenti ai **servizi Mail** che vedono una continua crescita, sintomo che gli attaccanti escogitano sempre nuove modalità per eludere i sistemi di protezione. Il vettore d'attacco principale è l'utilizzo di **URL malevoli, con l'87%** sul totale, in **crescita dell'11%**. Si osserva in generale, un incremento di tecniche organizzate in più fasi, variando dall'installazione di **software malevolo al furto dei dati personali degli utenti**. Tra queste, il «**Credential Phishing**», nonostante presenti un trend in lieve decrescita, rappresenta sempre la modalità di attacco più utilizzata, con un peso del **60%** sul totale.

Fastweb ha rilevato anche una **crescita** nel 2021 **di fenomeni fraudolenti che sfruttano il servizio SMS**, dovuti in particolare alla diffusione di malware, quali Flubot, veicolati attraverso **smishing** (il phishing via SMS) ed esponendo inoltre gli utenti a molteplici **rischi in ambito Privacy**. I fenomeni fraudolenti interessano anche le sottoscrizioni con **furto d'identità**, sempre più sofisticate e **in crescita anche per le imprese**, il CLI spoofing, ossia la **manipolazione del numero chiamante** e infine il "PBX hacking", in

cui i frodatori sfruttano le **vulnerabilità dei centralini** telefonici per generare traffico verso numerazioni ad alto costo. Di contro si riducono i costi complessivi associati a questo fenomeno ormai noto, grazie alla maggiore reattività degli strumenti e dei team antifrode.

In conclusione, le rilevazioni del 2021 mostrano un aumento generalizzato degli attacchi informatici ma dall'altra parte si registra una maggiore consapevolezza delle minacce da parte delle aziende e degli utenti che stanno gradualmente rafforzando le misure di difesa e il know-how in ambito Security per contenere l'avanzata del cyber-crime nella maniera più efficace.
Nei paragrafi a seguire è riportato il dettaglio dei singoli fenomeni rilevati.

Dati analizzati

I dati raccolti dal Security Operation Center Enterprise 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 (Computer Emergency Response Team) nazionali e internazionali. Le informazioni relative alle principali tipologie di minacce e agli attacchi riscontrati, sono state raccolte da piattaforme interne utilizzate nelle attività di Incident Management.
Ai dati analizzati dal SOC per il mercato Enterprise, quest'anno Fastweb ha aggiunto anche quelli elaborati in ambito Corporate Cybersecurity e Incident & Fraud Management, riguardanti rispettivamente la Mail Security e i trend sulle frodi, dettagliati nei prossimi paragrafi.
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.

Malware e Botnet

La rilevazione dei malware e botnet, che interessano i server appartenenti all'Autonomous System di Fastweb, nel 2021 ha continuato a far registrare un importante incremento rispetto a quanto visto nell'anno precedente. Infatti, quest'anno, nonostante siano state individuate un numero inferiore di famiglie di software malevoli rispetto all'anno precedente (163 vs 220, -26%), il numero di **server compromessi registrato fa segnare complessivamente un netto +58%** (Figura 1).

Il 34% delle minacce riscontrate provengono da Andromeda. A livello di comportamento Andromeda 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 l'ha resa 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 Downadup, conosciuta anche come Conficker. Si tratta di una famiglia di warm che, sfruttando vulnerabilità del sistema operativo Microsoft Windows, ha l'obiettivo di prendere il **controllo totale del server**, principalmente per finalità di esfiltrazione dati (anche attraverso funzionalità di keylogging). Scoperta per la prima volta nel 2009, nella primavera 2021 è tornata prepotentemente alla ribalta attraverso una variante silente distribuita in prima battuta, probabilmente attraverso circuiti P2P.

Di interesse anche la presenza nelle prime posizioni di FluBot: un malware che **infetta dispositivi mobili** Android e che si distribuisce attraverso link di phishing condivisi grazie a SMS o app di messaggistica. Anche nel settore delle infezioni, la penetrazione nel mobile inizia ad essere rilevante.
Infine, si è rilevata una piccola percentuale di software malevoli (1,15%) che non sono ancora stati catalogati e di cui non si conoscono tutti i dettagli.

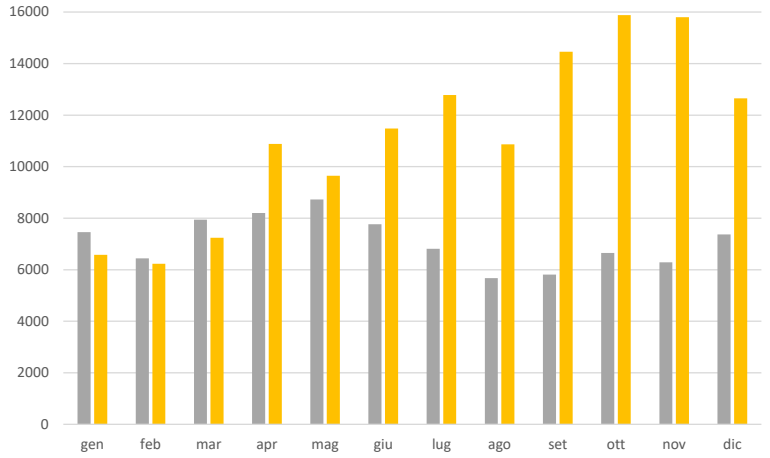


Figura 1 - *Distribuzione temporale del numero di infezioni rilevate (Dati Fastweb relativi all'anno 2020/2021)*

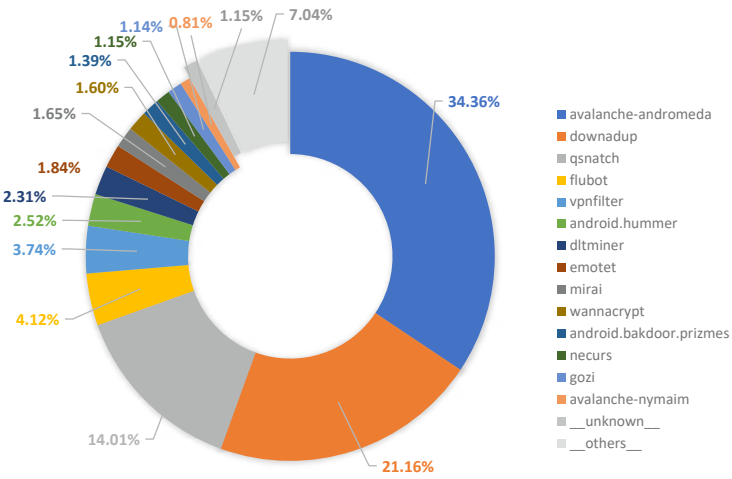


Figura 2 - *Analisi delle infezioni rilevate (Dati Fastweb relativi all'anno 2021)*

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 costante** rispetto al 2020 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 identificate (ad esempio gli antivirus).

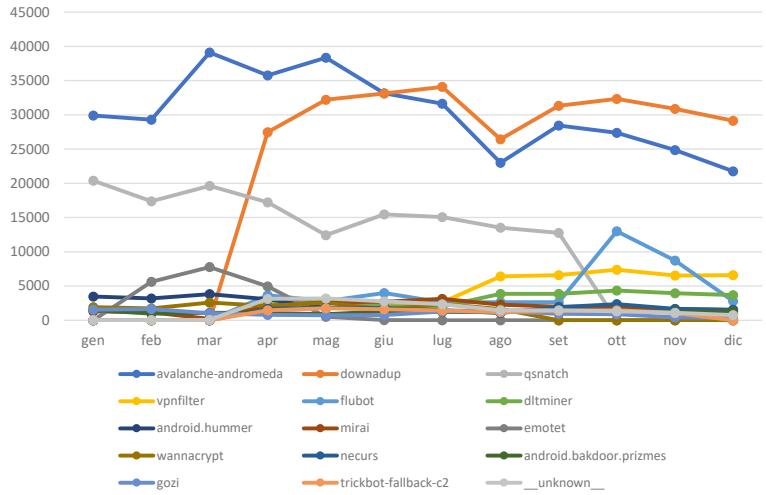


Figura 3 - *Rilevazione mensile dei Malware (Dati Fastweb relativi all'anno 2021)*

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 ai server infetti da malware (bot) utilizzate per la costruzione delle botnet.

La tendenza degli ultimi anni è stata quella di utilizzare come C&C server geograficamente posizionati in paesi tipicamente non considerati "a rischio" o che generano notevole mole di traffico. La logica è quella di rendere inefficaci meccanismi di difesa basati sulla caratterizzazione geografica dei flussi malevoli e nascondere il più possibile queste connessioni persistenti con il centro di controllo.

Dal 2019, almeno l'80% dei centri di C&C relativi a server infetti appartenenti all'AS di Fastweb si trovavano negli Stati Uniti. Questo principalmente a causa dell'alta presenza di datacenter che si concentravano quasi totalmente negli USA, soprattutto di proprietà dei grandi player cloud internazionali. Nel 2021 notiamo una inversione di tendenza che **riporta la provenienza di un buon numero di attacchi da server ospitati in Europa**. Il trend segue dunque i crescenti investimenti che si stanno moltiplicando in ambito Data Center nel vecchio continente. Sono infatti i Data Center a rappresentare i siti fisici da cui partono gli attacchi, secondo la nuova geografia illustrata nella figura seguente.

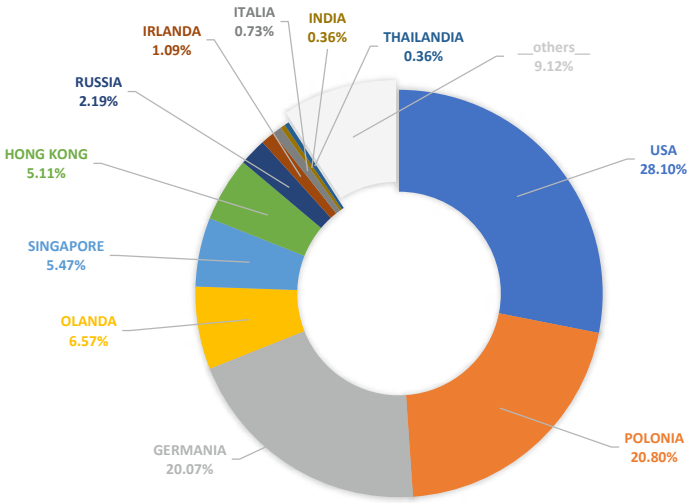


Figura 4 - *Dislocazione dei centri di Comando e Controllo (Dati Fastweb relativi all'anno 2021)*

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, 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.
In particolare, gli effetti di un attacco DDoS possono risultare estremamente dannosi 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) continua a crescere 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.

Durante tutto l'anno 2021 sono stati rilevati **2.500 eventi e circa 18.000 anomalie** riconducibili a possibili attacchi DDoS diretti verso i clienti Fastweb. Dopo l'aumento che si era manifestato nel 2020 a seguito dei forti cambiamenti nel mondo del digitale intro-

dotti dalla pandemia, il dato del 2021 è **tornato in linea con quanto rilevato nell'anno 2019**, come si evince nel grafico sottostante.

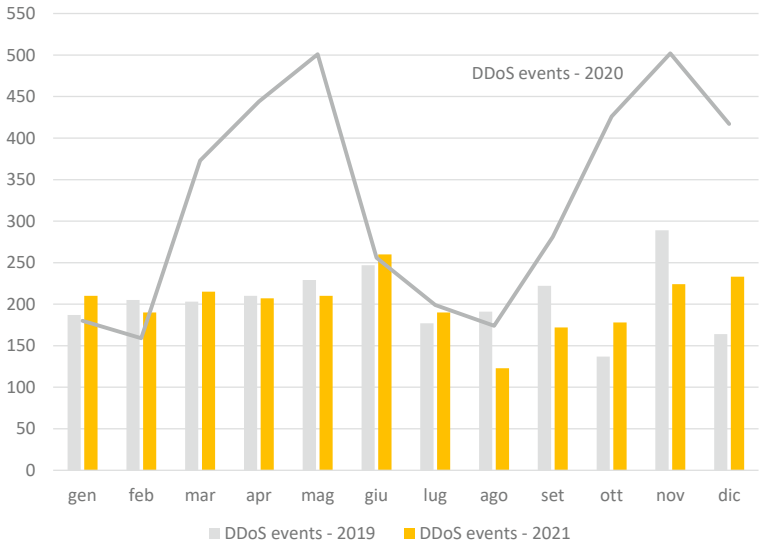


Figura 5 - *Distribuzione mensile delle anomalie DDoS*
(Dati Fastweb relativi agli anni 2019, 2020 e 2021)

Dall'analisi della distribuzione dei target degli attacchi DDoS, sono stati individuati i settori merceologici maggiormente colpiti da questo tipo di attacchi.

Come evidenzia il grafico successivo, il fenomeno riguarda un ampio numero di settori colpiti, tra i quali i più esposti si confermano essere il mondo del **Finance/Insurance e la pubblica amministrazione**, che sono obiettivo in circa il **50%** dei casi. A questi si aggiunge quello dell'**Industria** che ha presentato un **aumento significativo dal 7% al 18%**. Altri settori in forte aumento sono il Gambling (dal 2% al 9%) e Retail (da 1% a 6%).

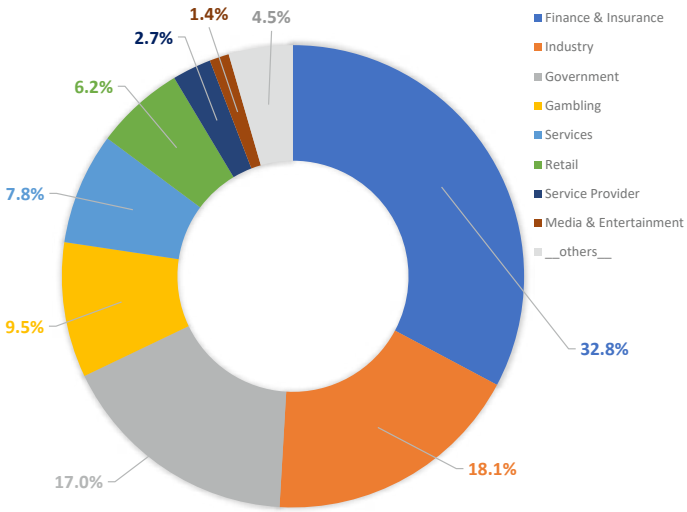


Figura 6 - *Target di possibili attacchi DDoS (Dati Fastweb relativi all'anno 2021)*

Di seguito viene riportata la distribuzione della banda media in Gbps di un attacco DDoS nel 2021.

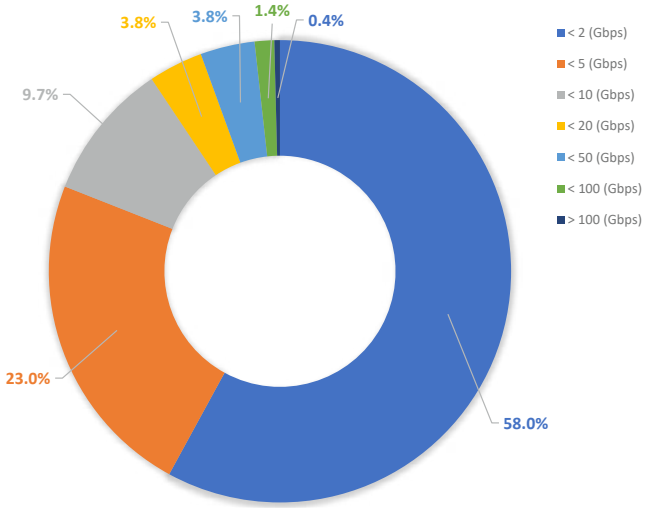


Figura 7 - *Distribuzione della dimensione di un attacco DDoS (Dati Fastweb relativi all'anno 2021)*

Nel corso degli anni, con la maggiore efficacia delle tecniche di difesa, la durata degli attacchi è mediamente diminuita. Anche quest'anno tale trend è confermato, dimostrando 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 infatti che quest'anno circa il **97% degli attacchi è durato meno di 3 ore**, rispetto al 93% dello scorso anno, mentre i rimanenti casi sono principalmente riconducibili a diversi tentativi effettuati in sequenza ravvicinata. È importante evidenziare che solo una piccola parte degli attacchi ha una durata di oltre 24 ore consecutive.

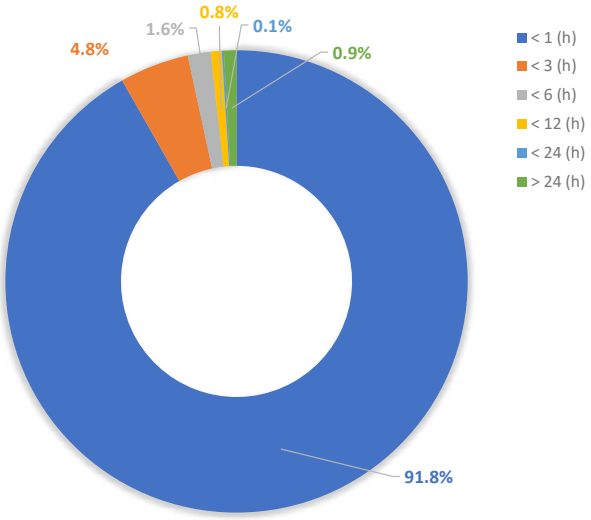


Figura 8 - *Durata dei possibili attacchi DDoS (Dati Fastweb relativi all'anno 2021)*

Le tecniche di attacco utilizzate in ambito DDoS possono essere diverse e nel 2021 le tre principali tipologie ricorrenti rilevate sono "**NTP amplification" che sale dal 6,6% del totale nel 2020 al 26,7%** nel 2021, "IP Fragmentation" (dal 17% al 10,2%) e "DNS amplification" (dal 15% al 8,9%). Questi ultimi sono stati posti a maggiore attenzione in quanto più critici per le organizzazioni Enterprise.
La tecnica di attacco "IP Fragmentation" è 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'eccessiva dispersione di questi pacchetti nella fase di ricezione causa un rallentamento o blocco nel riassemblaggio.

Gli attacchi più diffusi rimangono quelli che sfruttano il protocollo UDP, 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 rimasti in prima misura quelli più sfruttati**. Gli attacchi diversificati infatti hanno maggiore probabilità di essere efficaci a causa della maggiore complessità e variabilità nel corso dell'attacco per gestire la controparte difensiva.
In tale tipologia di eventi rientrano gli attacchi che variano nel tempo a seconda delle contromisure messe in atto; in questi scenari si crea un'interazione indiretta tra attaccante e defense center.

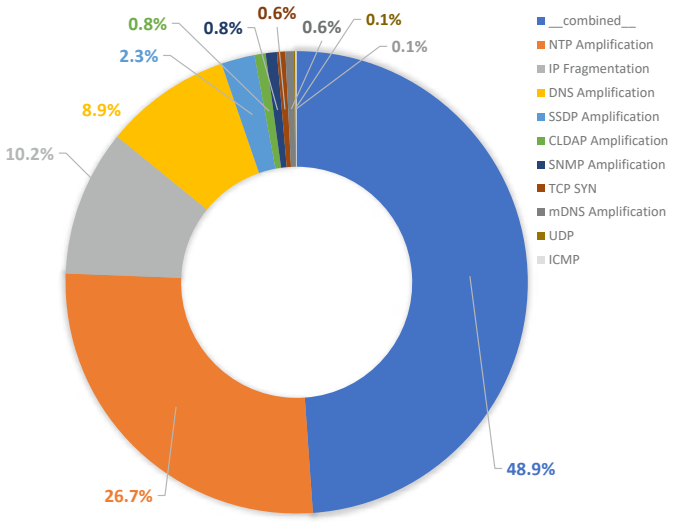


Figura 9 - *Tipologie di attacchi DDoS (Dati Fastweb relativi all'anno 2021)*

Servizi critici esposti su Internet

Questa sezione esplora il fenomeno dei **server e device che espongono servizi direttamente su Internet e che risultano privi dei livelli minimi di protezione.** Ciò significa che questi dispositivi sono facilmente attaccabili ed esposti a rischi elevati di compromissione.

Nel 2021 sono stati rilevati ben **46.000 server** e device "esposti" in rete ma **il loro numero è in costante diminuzione (- 16% nel 2021 rispetto al 2020 e - 18% rispetto al 2019)** a conferma che le aziende stanno progressivamente incrementando le linee difensive di base e pongono sempre più attenzione ai servizi esposti, chiudendo quelli critici e implementando policy adeguate ad abilitare lo smartworking e garantire l'accesso sicuro ai dati da remoto.
Al primo posto troviamo sempre Telnet, protocollo utilizzato per la gestione di server remoti, accessibile da riga di comando. Al secondo posto ancora l'RDP, utilizzato per la connessione remota ad un PC. Un attaccante potrebbe sfruttare questo protocollo per prendere il controllo completo di un apparato.
Di rilievo è anche la quantità di server 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.

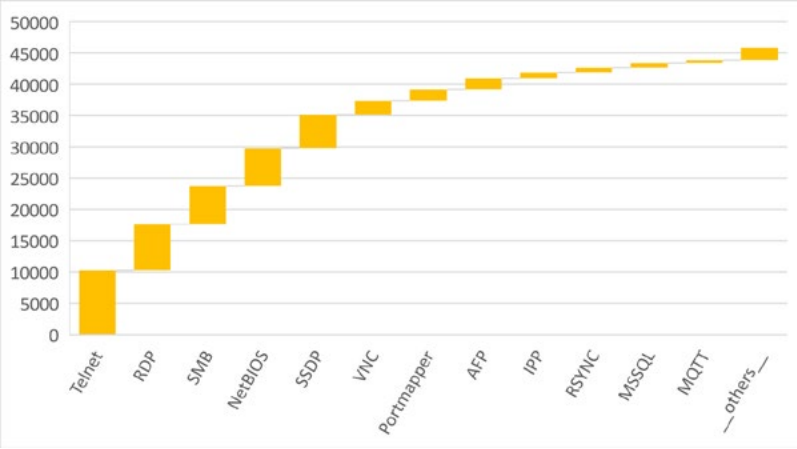


Figura 10 -*Servizi esposti direttamente su Internet (Dati Fastweb relativi all'anno 2021)*

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 venir 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 **5.300 IP** sono stati inseriti almeno una volta nelle blocklist durante il 2021. Il dato è in **crescita del 14%** rispetto al 2020 dove si erano registrate circa 4.700 azioni di blocklisting. Il grafico di seguito rappresenta la distribuzione delle città italiane maggiormente colpite.

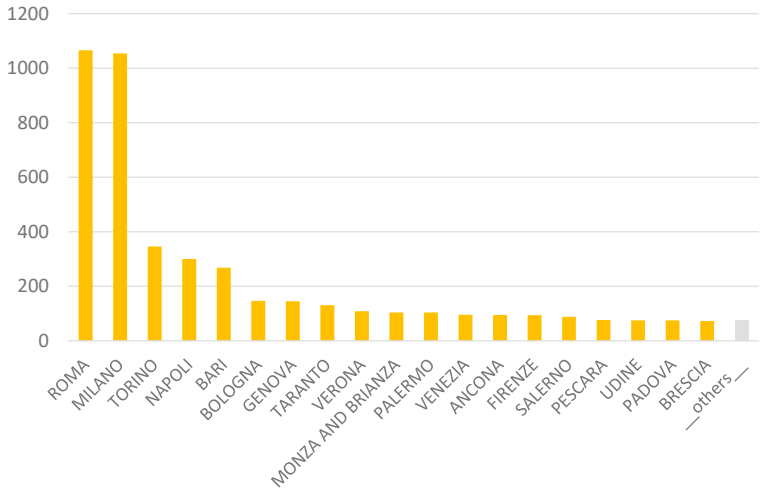


Figura 11 - *Dispositivi in Blocklist per città (Dati Fastweb relativi all'anno 2021)*

Sicurezza Applicativa Web

Di seguito un'analisi sul mondo delle vulnerabilità e degli attacchi indirizzati ai software e ai sistemi applicativi delle aziende clienti del settore Enterprise e della Pubblica Amministrazione rilevati attraverso tecnologie di tipo Web Application Firewall. Dalle evidenze raccolte nel campione analizzato del 2021, possiamo constatare che buona parte delle rilevazioni fa riferimento ad attività cyber correlate alla raccolta di informazioni (**Information Gathering**). Tale attività non essendo legata direttamente ad uno specifico attacco è spesso legata ad attività preparatorie, in ottica di raccogliere informazioni di dettaglio sui sistemi applicativi aziendali per sferrare attacchi in un secondo momento.

Di impatto rilevante sono gli eventi di tipologia **SQL Injection** (attacco diretto ad avere accesso ai dati, sfruttando le debolezze del linguaggio di programmazione per la gestione dei database), Directory Traversal (attacco utile ad avere accesso a file in directory in cui non si è autorizzati ad accedere), OS and Web Server Command Injection Attack e di Cross Site Scripting o XSS (iniezione di codice finalizzato all'esecuzione di azioni non previste dallo sviluppatore che costringe l'utente a eseguire azioni non volute).

Nella categoria Denial of Service sono state raccolte quelle tipologie di attacco che hanno il fine di rendere il servizio applicativo indisponibile. Negli attacchi di tipo File Injection, l'attaccante prova ad inserire nel sistema file malevoli con l'obiettivo di prenderne il controllo.

Invece in azioni riconducibili alla categoria CMS Application Attack, troviamo tentativi di sfruttamento vulnerabilità note, verso applicativi Web come, ad esempio, alcuni tra i più diffusi CMS: Joomla, Drupal o Wordpress. In Generic Attack sono state inserite tutte quelle tipologie di attacchi che sfruttano exploit comuni ma non rientrano nelle tipologie precedenti, come LFI (Local File Inclusion).

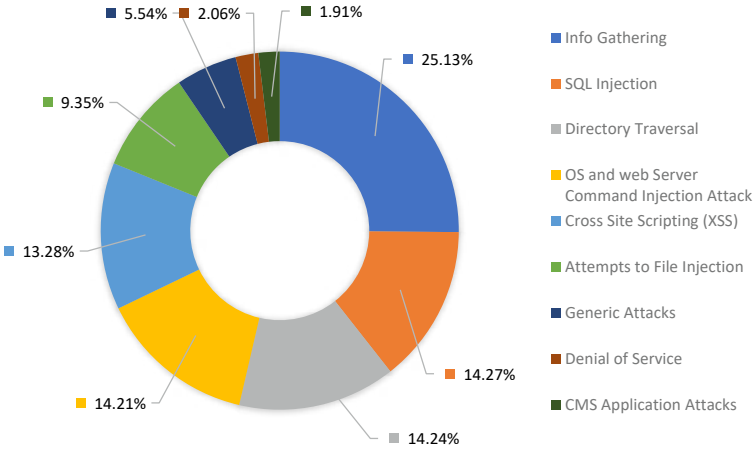


Figura 12 - *Tecniche di attacco applicativo rilevate dai WAF del segmento Enterprise (Dati Fastweb relativi all'anno 2021)*

Dalla rilevazione risulta evidente che le sorgenti di attacco applicativo rilevate dai WAF, gestiti dal Security Operation Center di Fastweb, provengano in gran parte dagli Stati Uniti. Un dato importante è quello proveniente dall'**Italia che risulta essere al terzo posto** in questa classifica: questo sottolinea quanto contromisure basate sulla provenienza geografica perdano di valore e sia sempre più importante mettere in campo sistemi di protezione basati su tecnologie all'avanguardia e affidarsi a centri di competenza specifici come Cyber Defense Center e personale specializzato.

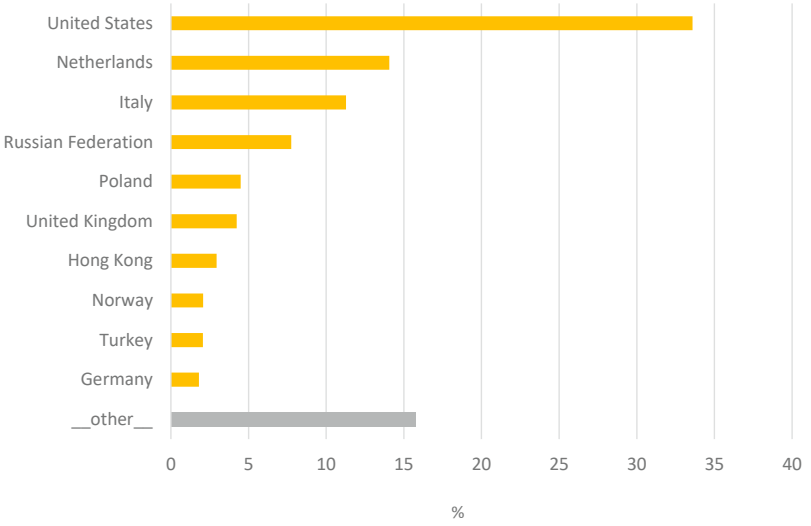


Figura 13 - *Dislocazione delle sorgenti di attacco applicativo rilevate dai WAF del segmento Enterprise (Dati Fastweb relativi all'anno 2021)*

Nel grafico seguente invece possiamo vedere la distribuzione, basata sul campione analizzato degli IP con bassa reputazione e dei BOT riconosciuti come non leciti. Si presentano i dati delle 10 nazioni con i valori più elevati. Anche qui da sottolineare l'importante presenza di server ospitati in Italia.

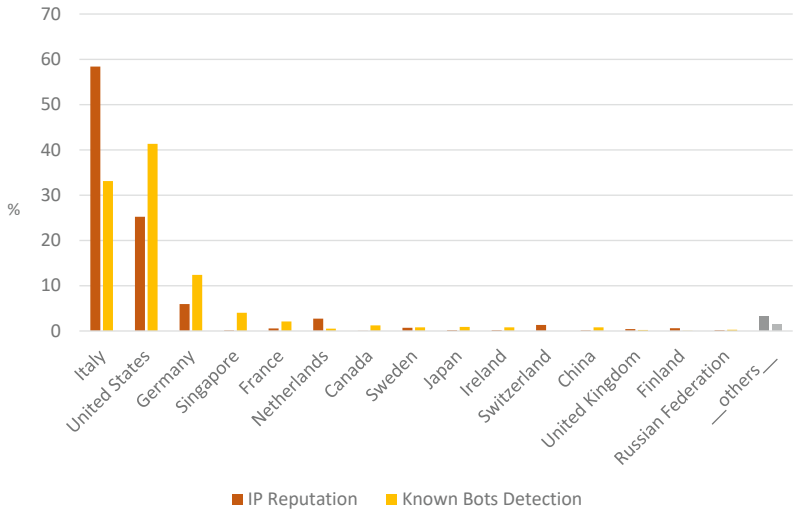


Figura 14 - *Dislocazione delle sorgenti con IP Reputation e BOT riconosciuti come non leciti, rilevati dai WAF del segmento Enterprise (Dati Fastweb relativi all'anno 2021)*

Sicuramente uno degli eventi di maggior interesse in ambito sicurezza delle applicazioni Web del 2021 è la **vulnerabilità che affligge il software Apache Log4j**, una delle librerie più diffuse in ambito sviluppo applicativo web-based per la gestione dei log. Questa debolezza permette ad un attaccante di prendere il controllo remoto di un dispositivo.
Da quando è stata resa nota il 9 dicembre, la vulnerabilità è diventata protagonista della maggior parte dei tentativi rilevati di sfruttamento. Di seguito (Figura 19) è illustrato l'andamento dei tentativi bloccati dai sistemi di protezione, dell'ultimo mese dell'anno in relazione al CVE (Common Vulnerabilities and Exposure).
La numerosità è giustificata anche dall'alto numero di dispositivi in rete che utilizza questa libreria.

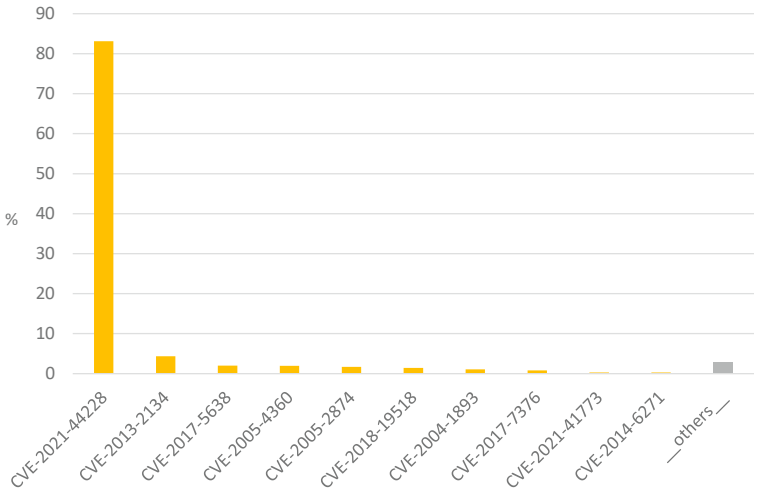


Figura 15 - *Evidenza della rilevazione dell'attacco conosciuto come Log4J nell'ultimo mese di dicembre rilevato dai WAF del segmento Enterprise (Dati Fastweb relativi all'anno 2021)*

Trend e minacce in ambito Mail

In questa sezione sono riportati i principali trend rilevati da Fastweb nel 2021 in ambito Mail Security.

Il vettore d'attacco principale utilizzato per veicolare attacchi tramite mail è l'utilizzo di **URL malevoli con l'87% sul totale**, in **crescita dell'11%,** come illustrato nella figura sotto. Considerando l'andamento annuo, la presenza diretta di allegati malevoli all'interno della mail risulta in diminuzione. Il dato è apparentemente in controtendenza rispetto al trend di crescita delle compromissioni malware e ransomware. La principale spiegazione di questo fenomeno è data dal fatto che la minaccia mail, tramite URL, può condurre l'utente a scaricare file malevoli in una seconda fase dell'attacco.

Gli attacchi mail sono sempre più spesso organizzati tramite campagne dedicate, dove il fattor comune è il tema e/o l'identità dei soggetti da colpire. Resta comunque salda un'importante percentuale relativa alle «Minacce Individuali». Quest'ultima può dipendere dalla mancanza di visibilità per attribuire l'evento malevolo ad un Threat Actor, e/o di determinare gli elementi in comune di una minaccia.

In generale risulta evidente che le tipologie di minaccia sono in continua crescita, sintomo che gli attaccanti escogitano sempre nuove modalità per eludere i sistemi di monitoraggio.

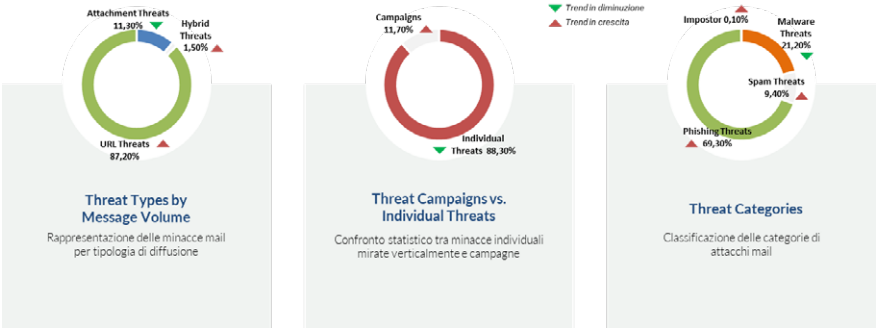


Figura 16 - *KPI minacce Mail 2021*

Ad eccezione del malware Tordal, che riprende il **trend in crescita associato alle compromissioni di tipo ransomware**, la distribuzione delle restanti tipologie di malware è relativa a quelle forme di codice malevolo che hanno come finalità l'esfiltrazione di informazioni e dati delle vittime (credenziali di accesso). Ad esempio, nel caso del malware Dridex ad essere interessati sono le informazioni bancarie, nel caso di Formbook invece le informazioni sono recuperate da vari browser web. Quest'ultimo è in grado altresì di monitorare e registrare le attività della tastiera.

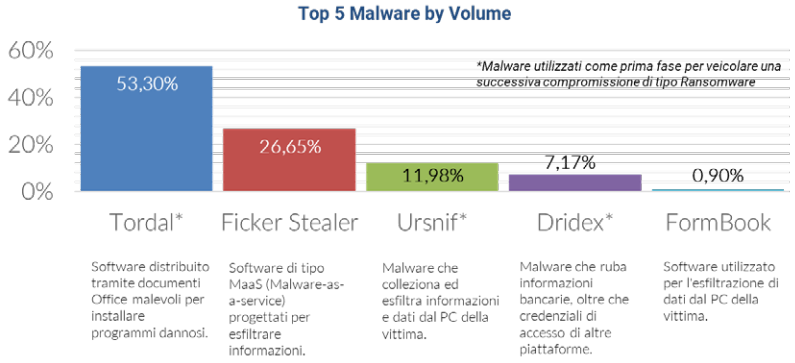


Figura 17 - *Top 5 Malware by volume 2021*

Sempre in ambito Mail, il grafico successivo riporta le tecniche utilizzate dagli attori maligni per veicolare una minaccia.
È di recente attualità (Febbraio 2022) che Microsoft bloccherà di default l'esecuzione di macro VBA all'interno di Access, Excel, PowerPoint, Visio e Word.
Gli utenti non saranno in grado di abilitare macro all'interno di documenti non attendibi-

li scaricati da Internet. La modifica inizierà a essere introdotta nella versione 2023, a partire da Current Channel (Preview) all'inizio di aprile 2022. In seguito, sarà disponibile anche negli altri canali di aggiornamento.

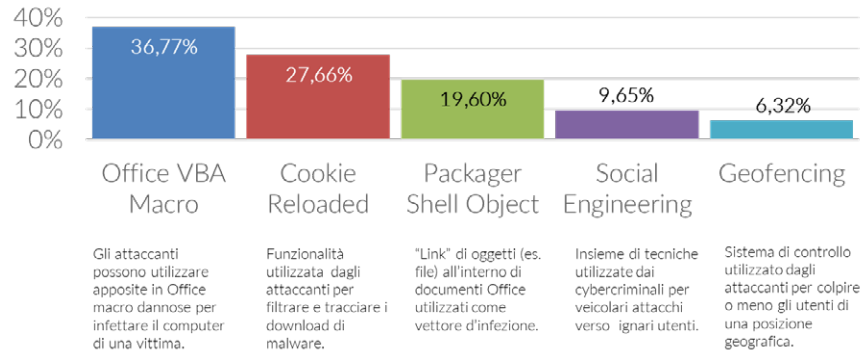


Figura 18 - *Top 5 Techniques by Volume 2021*

Il prossimo grafico rappresenta una classificazione delle minacce mail le cui **modalità di attacco variano dall'installazione di software malevolo al furto dei dati personali degli utenti**. Il dato sul «Credential Phishing», nonostante presenti un Trend in lieve decrescita nell'anno 2021, rappresenta comunque la modalità di attacco più utilizzata. Crescono invece nuove modalità come il downloader (+10%), lo Stealer (+6%) e il Banking (+9%).

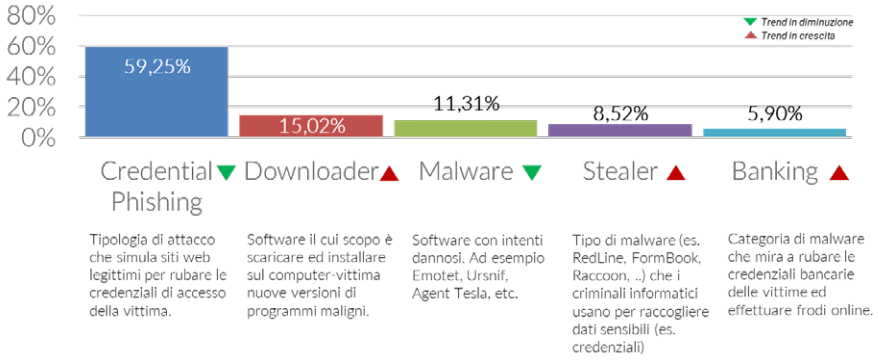


Figura 19 - *Top 5 Families by Volume 2021*

Trend e nuovi fenomeni in ambito Frodi

Nel 2021 Fastweb ha rilevato una **crescita di fenomeni fraudolenti che sfruttano il servizio SMS**. In particolare, si è osservato la diffusione di malware, quali, Flubot, veicolati attraverso **smishing**, il phishing via SMS. Questi malware, oltre a comportare potenziale perdita di dati per gli utenti, si propagano inviando nuovi SMS agli indirizzi che trovano nella rubrica dell'utente e a numerazioni decise da "command & control". Volumi molto elevati di messaggi inviati in un breve intervallo di tempo possono arrivare a saturare temporaneamente la rete, con un conseguente possibile rallentamento nell'erogazione del servizio stesso.

Una versione di smishing ad alto costo per l'utente ma a minor rischio di violazione, è quella dei messaggi che invitano a chiamare numerazioni a pagamento (es 899).
Sempre tra i nuovi fenomeni c'è l'ampia diffusione di app che, se installate, riconoscono agli utenti un **importo (pochi centesimi) per ogni SMS inviato** sfruttando il plafond di messaggi gratuiti inclusi nell'offerta commerciale, o per ogni SMS ricevuto. Il guadagno, infinitesimale, per l'utente corrisponde ad una perdita per gli operatori sui costi di interconnessione e wholesale. L'utente, tuttavia, si espone a **molteplici rischi in ambito Privacy**, in quanto i messaggi vengono inviati con il numero di telefono dell'utente stesso.
Per sensibilizzare gli utenti a saper riconoscere ed evitare queste minacce, sempre più aggressive e frequenti, Fastweb invia newsletter ai propri clienti e pubblica periodicamente informazioni sul proprio sito istituzionale nella sezione "Sicurezza in rete" e sul Digital Magazine.

Tra i fenomeni sempre attuali è utile ricordare:

- Le **frodi da sottoscrizione con furto d'identità**, che diventano sempre più sofisticate e costose, quando scoperte. Se negli anni precedenti questi fenomeni interessavano in prevalenza l'ambito residenziale, nel periodo 2020 e 2021 risultano **in crescita anche per le Partita IVA**.
- Il CLI spoofing, ossia la **manipolazione del numero chiamante** per camuffare la reale provenienza della chiamata. Questo fenomeno è associato in modo molto importante con il telemarketing "selvaggio" e il robocalling, ossia il fenomeno delle chiamate automatiche.
- Ricordiamo che il "CLI spoofing" o refilling è anche associato al bypass dei costi di interconnessione, a danno degli operatori riceventi. Si tratta di una frode che sfrutta le differenze nelle tariffe di interconnessione e che trasforma una chiamata originata extra-UE in una chiamata che sembra provenire da un Paese UE, o peggio ancora, in una chiamata Nazionale / locale
- Il "PBX hacking", in cui i frodatori sfruttano le **vulnerabilità dei centralini** stessi o l'esposizione di servizi in rete per "attaccarsi" al centralino di un cliente di tipo business, per generare traffico verso numerazioni ad alto costo. Il fenomeno affligge sia i centralini fisici, sia i centralini virtuali. In crescita il volume di PA colpite dal fenomeno.

Di contro si riducono i costi associati al fenomeno, sia per la maggiore reattività degli strumenti e dei team antifrode su un fenomeno noto, sia per la natura stessa del traffico che vede, spesso, chiamate di breve durata. Tra le direttrici internazionali maggiormente sfruttate, si confermano alcuni Paesi dell'Africa e Paesi dell'Europa orientale.

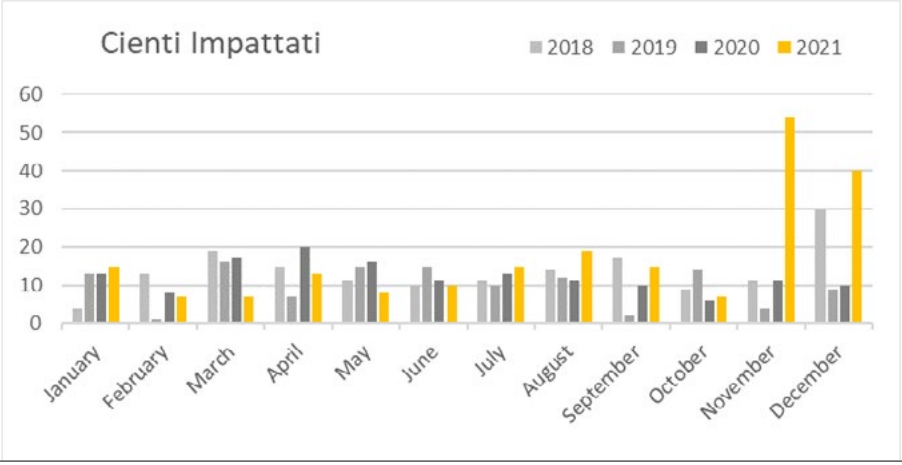


Figura 20 - *Numero di clienti impattati da PBX Hacking dal 2018 al 2021*

Attività e segnalazioni della Polizia Postale e delle Comunicazioni nel 2021

L'anno 2021 è stato caratterizzato dal prolungarsi dell'emergenza sanitaria da Covid19, che diversamente dall'anno precedente, ha avuto un andamento più discontinuo, ad ondate, ed ha visto, nell'avvio della campagna vaccinale di massa, uno degli elementi primari di miglioramento. I cambiamenti repentini nelle abitudini di vita, di socializzazione e di lavoro imposti dall'avvio della pandemia nel corso del 2020 si sono, in parte, stabilizzati, aprendo la strada a nuove consuetudini: molte aziende hanno proseguito con forme di telelavoro e smartworking, mantenendo quindi alta la frequenza di navigazione in rete da parte dei soggetti adulti; dall'altro versante, le diverse ondate di contagi e le conseguenti misure di precauzione hanno inciso sull'organizzazione della vita scolastica, mantenendo elevato il trend del ricorso allo strumento informatico ad opera dei minori, anche ben al di sotto dei tredici anni.
Questo stato di cose ha trasformato quella che tutti speravano fosse un'emergenza contingente in un processo irreversibile per il quale si è assistito ad una forzosa anticipazione dell'approccio di bambini e ragazzi alla rete, in un processo che non ha tardato a mostrare aspetti di criticità.
L'impegno della Polizia Postale e delle Comunicazioni nell'anno 2021 è stato costantemente indirizzato all'adeguamento degli interventi preventivi e repressivi, orientandosi da una parte verso un più puntuale "pattugliamento" del web alla ricerca di contenuti illegali, e dall'altra attraverso l'affinamento delle tecniche investigative sotto copertura che si sono concentrate su quei circuiti riservati e tecnicamente complessi nei quali si sono riversati sexoffender e pedofili avvezzi all'uso del web e dei suoi servizi di comunicazione. Uno sforzo ulteriore è stato fatto per l'adeguamento dell'offerta formativa diretta ai bambini e ai ragazzi, con l'obiettivo di sensibilizzarli ai pericoli della rete proprio utilizzando il mezzo stesso attraverso il quale erano esposti al rischio: gli incontri, di solito svolti in presenza presso gli istituiti scolastici, sono proseguiti anche quando le classi erano in DAD, in quarantena o in zona rossa, allo scopo di mantenere alto il livello di attenzione in un momento in cui vi era la necessità di ricorrere al mezzo informatico per proseguire le attività didattiche.

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

Il Centro Nazionale per il Contrasto alla Pedopornografia Online (C.N.C.P.O.) nel 2021, ha confermato il suo ruolo di punto di riferimento nazionale nella lotta alla pedofilia e pornografia minorile online.

Nel corso dell'anno è proseguita l'attività di osservazione e valutazione dei dati relativi alle vittimizzazioni online di minori: all'aumento complessivo dei casi trattati, e all'incremento esponenziale delle segnalazioni pervenute da organismi internazionali di protezione dei minori in rete, si è associato anche un aumento del numero degli arresti di individui adulti che

hanno usato il web per ottenere e scambiare materiale pedopornografico, più spesso usando la rete per condividere con un pubblico potenzialmente globale, gli abusi che stavano perpetrando ai danni di piccole vittime. Numerosi quindi i casi che hanno visto pedofili italiani mettere in atto azioni di abuso reale in danno di bambini anche piccolissimi, traditi dalla perizia investigativa della Specialità e dalla ricerca di notorietà all'interno degli ambienti di scambio del materiale illecito.
Il trend di aggravamento della minaccia cibernetica nei confronti dell'infanzia e all'adolescenza non accenna ad attenuarsi, come dimostrano i dati dell'anno in corso e la frequenza e significanza delle operazioni svolte dal C.N.C.P.O. e dalle articolazioni territoriali dipendenti.
In particolare, nell'ambito dell'attività di contrasto svolta dal Centro sono stati trattati complessivamente 5613 casi, che hanno consentito di indagare 1421 soggetti, di cui 139 tratti in arresto per reati connessi con abusi tecnomediati in danno di minori, con un aumento di circa il 73% rispetto all'anno precedente.
Prosegue il lavoro di valutazione puntuale dei dati relativi alla vittimizzazione dei bambini e dei ragazzi in rete, avviato in occasione del primo lockdown, al fine di monitorare la minaccia cibernetica in un momento di fragilità nazionale.

Il confronto dei dati rilevati tra il 2020 ed il 2021 ha evidenziato un incremento pari al 47%. Per tale motivo, lungo tutto il secondo anno di diffusione pandemica del virus Sars-Cov-2, la Polizia Postale e delle Comunicazioni, con l'impiego di tutte le sue articolazioni territoriali (coordinate attraverso l'azione strategica assicurata da questo Servizio), ha:

- intensificato il monitoraggio della rete, estendendo l'attenzione ad ogni forma di aggressione contro bambini e ragazzi presenti sul web e sui social network;
- mantenuto elevata la qualità dei rapporti di cooperazione internazionale giudiziaria e di polizia, quali presupposti strategici fondamentali per innalzare i livelli globali e nazionali di protezione dei bambini e dei ragazzi e favorire la distruzione di comunità virtuali e associazioni atte a favorire lo sfruttamento sessuale dei minori;
- aumentato l'impegno funzionale all'individuazione di un numero sempre maggiore di siti che contengono materiale pedopornografico, da inserire nella blacklist gestita dal C.N.C.P.O., l'accesso ai quali viene inibito per legge a coloro che utilizzano risorse di connettività presenti sul territorio italiano.

Tutto ciò è stato realizzato mediante un costante adattamento delle strategie di prevenzione e contrasto proprie della Specialità nella tutela dei minori attivi in rete, rispetto alle tipiche dinamiche connesse all'emergenza sanitaria, protrattasi lungo tutto l'anno appena trascorso.

L'adescamento on line

Particolarmente significativi sono i dati relativi all'**adescamento on line: 533 su 5613, i casi trattati dal Centro nel 2021**; si riconferma un trend in crescita, già osservato nell'anno precedente. A livello generale si è registrato un incremento del 33% rispetto al 2020, evidenziando che la fascia di età 10-13 rimane anche per quest'anno quella più coin-

volta, con la maggior parte di casi (306 su 533) con una tendenza in aumento pari al 38% rispetto ai 221 casi del 2020.
Nell'ambito delle indagini riguardanti il fenomeno dell'adescamento di minori online, sono state eseguite 183 perquisizioni domiciliari ed informatiche, con un esito complessivo di ben 208 soggetti indagati per questo reato nel 2021.

Cyberbullismo

Nello stesso anno di riferimento, sono stati trattati 464 casi di cyberbullismo[1], con un aumento percentuale pari al 13%.
Sono 136 i minori denunciati all'Autorità Giudiziaria perché autori di reati online connessi con il cyberbullismo, con un aumento percentuale pari al 15%, rispetto all'anno precedente.
Anche in questo ambito la complessità del rapporto tra giovani e tecnologia mostra direttive di aggravamento: sono sempre più frequenti i casi in cui l'uso di immagini sessuali, la loro realizzazione, la circolazione di queste in chat e messaggistica istantanea sono spesso i primi passi per vere e proprie campagne diffamatorie avviate contro coetanei, "colpevoli" di essere a qualche titolo "diversi".
Il cyberbullismo assume in modo progressivamente consistente un connotato multidimensionale in cui le distorsioni cognitive proprie della tecnomediazione (anonimato, impunità, irrintracciabilità), gli effetti concreti dell'immaturità cognitiva ed emotiva dei ragazzi (impulsività, reattività, non accuratezza delle valutazioni degli effetti delle azioni) si scontrano con la potenza amplificatoria del web, con la sua ubiquità spazio-temporale e con la contingenza del momento evolutivo critico che vivono ogni vittima e il suo giovane carnefice.

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

Si riportano di seguito, le attività investigative di maggior rilievo del Centro Nazionale per il Contrasto alla Pedopornografia online:

- nell'ambito di un'attività di indagine sottocopertura, denominata "**WILD TELEGRAM – FASE FINALE**" condotta dal Compartimento Polizia Postale di Genova, sono stati individuati sul territorio nazionale 12 utenti della Rete, che attraverso la piattaforma Telegram, si sono resi responsabili dei reati di cui agli artt. 600 ter e 600 quater c.p., nei cui confronti l'A.G. ligure ha emesso altrettanti decreti di perquisizione. **L'attività si è conclusa con 10 denunciati e 2 arrestati.**

[1] Ai sensi dell'art. 1 co. 2° della Legge nr.71/2017 per <<cyberbullismo>> si intende qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo.

nell'ambito dell'operazione **"LOLITA"** condotta dalla Sezione Polizia Postale di Brescia, unitamente alla locale Squadra Mobile, inerente la veicolazione di video e immagini pedopornografiche autoprodotte da una minore e divulgate attraverso la piattaforma Whatsapp ad altri utenti, l'A.G. procedente ha emesso nr. 16 decreti di perquisizione espletati sul territorio nazionale nei confronti di altrettanti soggetti ritenuti responsabili dei reati di cui agli artt. 600 ter e 600 quater c.p.

L'attività si è conclusa con 16 denunciati

- All'esito di un'indagine denominata **"BORGHETTO"**, condotta dal Compartimento Polizia Postale di Catania, sono stati individuati 11 soggetti maggiorenni e 16 soggetti minorenni, tutti sedenti nel territorio di Catania e provincia, responsabili di aver divulgato attraverso la piattaforma di messaggistica WhatsApp contenuti pedopornografici, nei cui confronti la locale Procura ordinaria e quella per i Minorenni hanno emesso altrettanti decreti di perquisizione.

  L'attività si è conclusa con 27 denunciati.
- Nell'ambito dell'operazione **"THE PUNISHER"** svolta dal Compartimento di Firenze, sono stati individuati 7 soggetti che attraverso la piattaforma WhatsApp, si sono resi responsabili di condotte illecite ai sensi degli artt. 600 ter e quater c.p. e nei cui confronti la locale A.G. ha emesso altrettanti decreti di perquisizione.

  L'attività si è conclusa con 6 denunciati.
- **Nell'ambito dell'operazione "CANADA 2.0"** svolta dal Compartimento di Reggio Calabria, su impulso del Servizio Polizia Postale e delle Comunicazioni, l'A.G. di Catanzaro ha emesso nr. 119 decreti di perquisizione nei confronti di altrettanti soggetti ritenuti responsabili di condotte illecite ai sensi dell'art. 600 ter e 600 quater c.p. che sono statti eseguiti disgiuntamente sul territorio nazionale.

  L'attività si è conclusa con 116 denunciati e 3 arrestati.
- Nell'ambito dell'operazione **"COMETA"** condotta dalla Sezione Polizia Postale di Brescia inerente la diffusione sui Social Network di immagini intime ritraenti una minore affetta da ritardo cognitivo, sono stati individuati 5 utenti nei cui confronti l'A.G. bresciana ha emesso 5 decreti di perquisizione.

  L'attività si è conclusa con 5 denunciati.
- All'esito dell'operazione "**MAPLE MAZE"** svolta dal Compartimento Polizia Postale di Milano, su segnalazione del collaterale organo di polizia canadese, sono stati individuati 31 utenti della Rete, responsabili attraverso la piattaforma KIK Messenger dei reati di cui agli artt. 600 ter e 600 quater nei cui confronti la locale Procura ha emesso altrettanti decreti di perquisizione personale ed informatica che sono stati espletati sul territorio nazionale.

  L'attività si è conclusa con 27 denunciati e 4 arrestati.
- Nell'ambito dell'operazione **"BIG SURPRISE"** condotta dal Compartimento Polizia Postale di Firenze, su segnalazione del collaterale organo di polizia canadese, sono stati individuati 24 utenti della Rete, responsabili attraverso la piattaforma KIK Messenger dei reati di cui agli artt. 600 ter e 600 quater nei cui confronti la locale Procura ha

emesso altrettanti decreti di perquisizione personale ed informatica che sono stati eseguiti sul territorio nazionale.

L'attività si è conclusa con 22 denunciati e 2 arrestati.

- Tra le indagini più significative condotte direttamente dal C.N.C.P.O., si segnala una delicata attività svolta nell'ambito delle darknet, che ha consentito di trarre in arresto un libero professionista 50enne, produttore di materiale di pornografia minorile. L'operazione è stata condotta con la cooperazione internazionale di polizia con altre Agenzie investigative estere attivata da Europol. L'uomo abusava in via continuativa di due minori di 6 e 8 anni. Avvalendosi delle sue capacità manipolatorie, era riuscito a carpire l'affetto e la totale fiducia dei bambini e, in soli due anni, ha filmato le violenze ai loro danni per un totale di circa 9.000 video. In virtù della fiducia in lui riposta da parenti e amici, riusciva a ottenere la disponibilità dei minori anche per diversi giorni.
- All'esito di un'indagine **"ONTARIO 2"** svolta dal Compartimento Polizia Postale di Milano, su segnalazione del collaterale organo di polizia canadese, sono stati individuati 17 utenti della Rete, responsabili attraverso la piattaforma KIK Messanger dei reati di cui agli artt. 600 ter e 600 quater nei cui confronti la locale Procura ha emesso altrettanti decreti di perquisizione personale ed informatica che sono stati espletati sul territorio lombardo.

  L'attività si è conclusa con 16 denunciati e 1 arrestato.
- Nell'ambito dell'operazione **"DICTUM"** condotta dal Compartimento Polizia Postale di Milano sono stati individuati 29 utenti della Rete, responsabili attraverso la piattaforma Mega.NZ dei reati di cui agli artt. 600 ter e 600 quater nei cui confronti la locale Procura ha emesso altrettanti decreti di perquisizione personale ed informatica che sono stati espletati sul territorio lombardo.

  L'attività si è conclusa con 19 denunciati 7 arrestati e 3 irreperibili.
- Al termine di un'indagine avviata a seguito di una segnalazione dell'Organizzazione statunitense NCMEC dal Compartimento Polizia Postale di Catania, sono stati individuati 7 utenti della Rete, responsabili dei reati di cui agli artt. 600 ter e 600 quater nei cui confronti la locale Procura ha emesso altrettanti decreti di perquisizione personale ed informatica.

  L'attività si è conclusa con 7 denunciati.
- All'esito di un'indagine sotto copertura denominata **"MEET UP"**, svolta dal Compartimento Polizia Postale Piemonte e Valle d'Aosta sulla piattaforma Telegram, la Procura della Repubblica di Torino ha emesso 26 decreti di perquisizione.

  L'operazione si è conclusa con **23 denunciati e 3 arrestati.**
- Nell'ambito dell'operazione **"GREEN OCEAN"** condotta anche in modalità sotto copertura dal Compartimento di Palermo su canali di file sharing, su piattaforme di chat e nel dark web, la Procura della Repubblica di Palermo ha emesso 34 decreti di perquisizione

  L'operazione si è conclusa con 21 denunciati e 13 arrestati**.**

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 29.847 siti, di cui 2.543 inseriti in black list e oscurati, in quanto presentavano contenuti pedopornografici.**
Di seguito una Tabella riassuntiva dei principali risultati operativi raggiunti durante l'anno 2021 a confronto con quanto rilevato nell'anno precedente.

C.N.C.P.O.	2020	2021	Incremento rispetto anno precedente
Casi trattati	3.243	5.613	+73%
Persone denunciate in stato di libertà	1.192	1282	+8%
Arrestati	69	139	+101%
Perquisizioni	757	1467	+94%

Inoltre, tra le indagini più significative avviate direttamente dal C.N.C.P.O. nell'ambito dei reati di sfruttamento sessuale dei minori, si segnala una delicata attività svolta nell'ambito delle darknet, che ha consentito di trarre in arresto un libero professionista 50enne, produttore di materiale di pornografia minorile. L'operazione è stata condotta con la cooperazione internazionale di polizia con altre Agenzie investigative estere attivata da Europol. L'uomo abusava in via continuativa di due minori di 6 e 8 anni. Avvalendosi delle sue capacità manipolatorie, era riuscito a carpire l'affetto e la totale fiducia dei bambini e, in soli due anni, ha filmato le violenze ai loro danni per un totale di circa 9.000 video.
In virtù della fiducia in lui riposta da parenti e amici, riusciva a ottenere la disponibilità dei minori anche per diversi giorni.

Truffe online

Nell'ambito delle competenze della Sezione si segnala l'intensificazione dell'attività di prevenzione attraverso il monitoraggio attivo della rete e un'articolata attività di contrasto alle **truffe online (3.441 le persone individuate e segnalate all'Autorità Giudiziaria)**, in particolare nel settore dei siti di *e-commerce* e *market place*, in considerazione del sempre maggiore utilizzo di Internet.

Nell'ambito delle truffe sul web si è rilevato un incremento degli illeciti legati al fenomeno **del trading online (1.652 casi trattati, di cui 33 casi in danno di minori e 79 sono state le persone denunciate),** con l'aumento del numero di portali presenti sul web che propongono programmi speculativi, apparentemente redditizi, evidenziando costi di accesso irrisori, ma rendimenti elevati sia nel breve che nel medio termine.

L'attività investigativa, qualora la denuncia sia tempestiva, prevede l'immediata attivazione dei canali di Cooperazione Internazionale di Polizia, con la richiesta del blocco urgente delle somme versate e l'effettuazione di accertamenti sui flussi finanziari che normalmente sono destinati all'estero.

La Sezione Operativa è impegnata anche nell'individuazione di proposte di vendita online di prodotti contraffatti o all'utilizzo illecito di segni distintivi dei marchi registrati, per la tutela dell'*italian sounding*.

Proprio in tema di contraffazione on line si evidenzia che il Servizio Polizia Postale e delle Comunicazioni è membro della Commissione Consultiva Permanente Interforze del Consiglio Nazionale Anticontraffazione, istituito presso il Ministero dello Sviluppo Economico, e ha aderito nel mese di dicembre 2018 al Protocollo di intesa, realizzato per le iniziative di formazione contro la contraffazione e l'italian sounding rivolte ai giovani.

Giochi e scommesse online

Il monitoraggio di siti e spazi web (blog, gruppi social e siti dedicati) dediti a giochi e scommesse clandestine è un'altra attività operativa particolarmente messa in atto dalla Polizia Postale e delle Comunicazioni, sia per contrastarne la diffusione irregolare o illegale, che per tutelare gli interessi dei consumatori, specie se minori d'età: numerosi sono i siti con sedi legali presso paesi esteri, che operano in Italia anche se privi della prevista autorizzazione per poter esercitare legalmente la raccolta di scommesse.
A tal fine, considerata l'esigenza di rafforzare l'attività di contrasto al fenomeno suindicato, sono stati coinvolti nell'attuazione di una scrupolosa strategia di controllo, tutti gli uffici della Specialità, favorendo la cooperazione info-investigativa con le competenti articolazioni delle locali Questure.

Reati contro la persona

In relazione ai reati afferenti quest'area di interesse, particolare attenzione è rivolta ai fenomeni del **revenge porn (265 casi trattati, di cui 30 casi in danno di minori, 120 le persone individuate e segnalate all'Autorità Giudiziaria) nell'ambito del quale si evidenzia che nel 79% dei casi la vittima è una donna, e delle truffe romantiche (335 casi trattati, di cui 7 casi in danno di minori e 75 sono state le persone denunciate).**

Riguardo quest'ultimo fenomeno si specifica che, purtroppo, le persone coinvolte spesso aspettano molto tempo prima di denunciare, perché devono ammettere, prima a se stesse, di essere state ingannate ovvero, che quello che pensavano fosse un vero interesse nei loro confronti era, in realtà, solo un mezzo per ottenere dei soldi.

Rilievo particolare assume il reato delle "sextortion" con 1.122 casi trattati (di cui 101 casi in danno di minori), 64 persone individuate e segnalate all'Autorità Giudiziaria, dove quasi l'83% delle vittime è rappresentato da soggetti di genere maschile.

Le indagini svolte dalla Specialità in tali ambiti sono finalizzate non soltanto a identificare e perseguire il responsabile del reato, ma anche a intervenire tempestivamente per far rimuovere i contenuti dal web o, quantomeno, limitarne la divulgazione massiva.

Una fetta importante dei reati contro la persona commessi o perfezionati attraverso l'utilizzo dei sistemi informatici è rappresentata dalle fattispecie delittuose riportate nella tabella che segue, evidenziando che alcuni di queste hanno fatto registrare nel 2021 preoccupanti incrementi rispetto all'anno precedente (Diffamazione /molestie/minacce +14%; stalking +34%; sextortion +69%; revenge porn +110%).

		VITTIME MAGGIORENNI		VITTIME MINORENNI			
	CASI TRATTATI	M	F	M	F	ARRESTATI	DENUNCIATI
STALKING	203	43	137	8	15	5	71
DIFFAMAZIONE ON LINE	2455	1415	957	34	49	0	1026
MINACCE	806	415	308	37	46	0	152
REVENGE PORN	265	50	185	5	25	4	116
MOLESTIE	706	216	415	31	44	2	110
SEXTORTION	1122	852	169	76	25	1	63
ILLECITO TRATTAMENTO DATI	539	505		34		0	26
SOSTITUZIONE DI PERSONA	4159	4048		111		0	124

Specifiche iniziative di prevenzione e contrasto sono indirizzate sia al fenomeno degli atti intimidatori nei confronti della categoria dei giornalisti e che alla diffusione del linguaggio d'odio in rete (hate speech) grazie a servizi di monitoraggio dei siti web, piattaforme digitali, profili e pagine presenti sui social network più noti (Facebook, Twitter, Instagram, Telegram, Pinterest e Youtube).

Complessivamente, nel corso dell'anno 2021, sono stati trattati nell'ambito dei reati contro la persona 10.412 casi, individuate e segnale all'Autorità Giudiziaria 1.712 persone.

Soccorso pubblico

Sono stati 51 gli interventi da parte della Specialità finalizzati alla prevenzione di intenti suicidari da parte di utenti dei vari social network, anche grazie alle segnalazioni pervenute direttamente sul sito del Commissariato di P.S. online.

Principali operazioni della Sezione Operativa nel 2021

"Pangea XIV": La Polizia Postale e delle Comunicazioni ha aderito per la prima volta all'Operazione denominata "Pangea XVI" che il Segretariato Generale Interpol di Lione ha organizzato nell'ambito dell'"Illicit Goods and Global health Programme", il cui obiettivo strategico è il contrasto al commercio online di farmaci contraffatti ed illegali, con particolare riferimento a quelli utilizzati per la cura del virus Sars Co2 – Covid 19. Il Servizio Polizia Postale e delle Comunicazioni ha coordinato le attività condotte dal Compartimento Polizia Postale e delle Comunicazioni per la "Sicilia Occidentale" di Palermo che, unitamente ai Compartimenti di Ancona e Bologna, ha predisposto una significativa azione di monitoraggio della rete grazie alla quale sono stati individuati numerosi siti dediti all'attività illecita oggetto di indagine. Le risultanze investigative hanno consentito di ottenere dalla Procura della Repubblica presso il Tribunale di Palermo un decreto di sequestro preventivo in relazione al reato di cui all'art 445 c.p. (Somministrazione di medicinali in modo pericoloso per la salute pubblica), notificato a 171 Internet Service Provider, che ha permesso di oscurare 34 siti, rendendoli irraggiungibili dall'Italia, così da interrompere la vendita, sul territorio nazionale, di farmaci non autorizzati;

"Nassa 3.0": La Polizia Postale e delle Comunicazioni di Reggio Calabria, a seguito di una complessa e delicata attività di indagine, ha eseguito 18 ordinanze di custodie cautelari, 10 delle quali in carcere e 8 domiciliari, emesse dal G.I.P. presso il Tribunale di Palmi (RC), a carico di altrettanti soggetti gravitanti nel territorio reggino. Associazione per delinquere finalizzata alla truffa, riciclaggio, sostituzione di persona e trattamento illecito dei dati personali i principali reati attribuiti alla compagine criminale. Secondo la ricostruzione della Polizia di Stato e della locale Procura della Repubblica, avallata dal GIP presso il Tribunale di Palmi, si contesta agli indagati di aver reiteratamente offerto in vendita, attraverso una serie di ingegnosi stratagemmi finalizzati a "coprire" le proprie effettive identità e un modus operandi organizzato e complesso, autovetture, trattori, scavatori, scooter e quant'altro, in realtà inesistenti, su note piattaforme di e-commerce;

Il Servizio Polizia Postale e delle Comunicazioni, per contrastare le possibili infiltrazioni della criminalità nel mondo sportivo, ha ravvisato l'esigenza di potenziare il monitoraggio della rete internet, coinvolgendo tutti gli uffici della Specialità dislocati sul territorio nazionale, anche riguardo al fenomeno delle scommesse illecite on line e a tutela della correttezza dello svolgimento delle manifestazioni sportive. A seguito del quotidiano monitoraggio attivo degli spazi web, la Sezione Operativa social network del Servizio Polizia Postale e delle Comunicazioni ha individuato 30 siti di raccolta di scommesse on line, sprovvisti della necessaria concessione di A.D.M., tutti riconducibili a società registrate in Paesi esteri, che sono stati oscurati.

"Falso ginecologo": Il Servizio Polizia Postale e delle Comunicazioni e il Compartimento Polizia Postale e delle Comunicazioni di Bari hanno eseguito, su delega della Procura della

Repubblica di Taranto, una perquisizione domiciliare nei confronti di un quarantenne per il reato di violenza sessuale, sequestrando diversi smartphone, supporti di memoria e schede telefoniche. Lo stesso è gravemente indiziato di essere l'autore delle condotte che dal settembre 2021 hanno portato numerose donne a sporgere denuncia presso gli Uffici della Polizia Postale a seguito della ricezione di telefonate da un individuo che si presentava come ginecologo. Il falso medico, rappresentando alle vittime la presenza di pericolose patologie all'apparato riproduttore, le induceva ad effettuare una visita ginecologica online. La vicenda parrebbe aver colpito oltre 400 donne in tutta Italia, i cui dati, dai primi riscontri, sembrerebbero stati ottenuti dalla consultazione di portali di annunci di compravendite online.

C.N.A.I.P.I.C.
Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche

Nell'ambito della protezione delle Infrastrutture Critiche, con particolare riferimento alle attività di prevenzione e contrasto ad attacchi e minacce aventi per obiettivo le infrastrutture sensibili di interesse nazionale (pubbliche e private), il C.N.A.I.P.I.C. - nell'ambito del complessivo Sistema Informativo Nazionale per il Contrasto al Cyber Crime[2], ha gestito:

- **5.509** attacchi informatici significativi nei confronti di servizi informatici relativi a sistemi istituzionali, infrastrutture critiche informatizzate di interesse nazionale, infrastrutture sensibili di interesse regionale, grandi imprese;
- ha diramato **110.880** alert di sicurezza riferibili a minacce per sistemi informatici/telematici oggetto di tutela del Centro;
- ha ricevuto **60** richieste di cooperazione, gestite dall'Ufficio del punto di contatto HTC Emergency presente all'interno del C.N.A.I.P.I.C. nell'ambito della Rete 24-7 "High Tech Crime" del G7.

Le attività investigative avviate dal Centro e dai Compartimenti, hanno portato al deferimento di complessive **201** persone per accesso abusivo e danneggiamento di sistemi informatici afferenti sistemi critici ovvero servizi essenziali, diffusione di mallware, trattamento illecito di dati su larga scala.

Il C.N.A.I.P.I.C., ha rilevato anche per il 2021 che tra tutte le fattispecie delittuose ricomprese nella categoria cybercrime, il ransomware si è dimostrato un fenomeno costantemente in crescita per numero di attacchi perpetrati nonché in continua metamorfosi

[2] Si tratta del più ampio progetto SINC3, che prevede collegati in rete il CNAIPIC, a tutela delle infrastrutture critiche nazionali, ed i Nuclei operativi sicurezza cibernetica – NOSC dei Compartimenti, di prossima istituzione con la riorganizzazione dei presidi territoriali della Specialità, quest'ultimi a tutela dei rispettivi asset cibernetici regionali. Il progetto prevede tra l'altro la formazione degli operatori NOSC e la creazione di una piattaforma informatica per la gestione degli eventi e per la condivisione delle informazioni di sicurezza finanziata con fondi ISF, che, oramai avviata la fase sperimentale, potrà essere inaugurata il prossimo anno.

nelle modalità di offesa alle vittime, caratteristiche queste che lo rendono maggiormente insidioso, sia per il primato statistico del numero di azioni malevoli sferrate che per il livello di minaccia, capace di colpire non solo le grande infrastrutture informatiche ma anche, in modo diffuso, i singoli utenti.
I cyber-criminali hanno continuato la tendenza introdotta lo scorso anno rendendo sempre più frequenti i loro attacchi ransomware, sempre più sofisticati e mirati. Il numero di casi di ransomware mirati sono aumentati lo scorso anno rispetto a quello precedente, registrando un aumento significativo di capacità dell'attore della minaccia e un maggiore impatto sulle vittime.
Significativa è l'evoluzione che ha subito in brevissimo tempo la tecnica utilizzata per sferrare l'attacco, passando da una tipologia con tre passaggi ad una più complessa che si articola in cinque fasi oramai nota come il "ransomware con la doppia estorsione".

Tipo Base: Accesso – Cryptolocker - Estorsione

L'attacco ransomware base viene condotto utilizzando un «trojan horse» che avvia una sequenza di fasi che apre la strada ad un «cryptolocker» in grado di rendere inservibile il sistema colpito. Successivamente gli attaccanti richiedono di essere contattati attraverso «Tor» su una pagina «.onion» (nel dark web) e seguire le istruzioni per riottenerne l'accesso, spesso dopo aver effettuato un pagamento in «cryptovaluta» su di un loro «wallet».

Tipo Evoluto: Accesso – Persistenza – Esfiltrazione - Cryptolocker – Doppia Estorsione

Alla tipologia base dell'attacco vengono aggiunte due fasi intermedie: la persistenza e l'esfiltrazione.
Persistenza: Gli attacchi vengono in molti casi condotti dai cosiddetti APT (Advance Persistent Threat), gruppi di hacker che possono essere liberi o state-sponsored (finanziati da Stati). L'APT utilizza tecniche di hacking continue, clandestine e sofisticate per ottenere l'accesso a un sistema e rimanere all'interno per un periodo di tempo prolungato, con conseguenze potenzialmente distruttive. La minaccia colpisce principalmente stati nazionali e grandi società, con l'obiettivo finale di rubare informazioni per un lungo periodo di tempo. Gli aggressori APT utilizzano sempre più piccole aziende che costituiscono la catena di approvvigionamento del loro obiettivo finale come un modo per ottenere l'accesso a grandi organizzazioni. Usano tali società, che sono tipicamente meno difese, come trampolini di lancio. L'attacco ransomware per questi attaccanti è solo la fase finale dell'attacco, utile ad ottenere un ulteriore finanziamento alle loro attività.
L'esfiltrazione è presente nella quasi totalità dei casi e viene utilizzata per effettuare la cosiddetta **"doppia estorsione"**: si richiede un pagamento in BitCoin (o comunque in cryptomoneta) per ottenere la chiave di decodifica e per scongiurare la pubblicazione dei dati, che, in caso si possegga un valido backup, può comunque creare un danno d'immagine all'ente/azienda/privato, che ha l'onere di comunicare al Garante della Privacy e ai suoi clienti (etc…) l'avvenuto "data-breach" (incidente informatico che la violazione di dati).

Nel 2021 il C.N.A.I.P.I.C. ha gestito 256 eventi ransomware (contro i 220 del 2020), di cui 61 contro Infrastrutture Critiche (IC), Operatori di Servizi Essenziali (OSE) e Piccole Amministrazioni Locali (PAL) e 195 attacchi ad aziende.

L'azione del C.N.A.I.P.I.C. come è noto è diretta alla prevenzione e contrasto alle violazioni dei sistemi informatici critici significando che gli ultimi mesi del 2021 sono stati caratterizzati da una attività di contrasto massivo alle falsificazioni e commercializzazioni di certificati Green Pass illegali, sia sul clear che sul dark web.
L'azione della Polizia Postale e delle Comunicazioni si è diretta, ad ampio spettro:
a) al contrasto ai fenomeni di sottrazione illecita, dai sistemi critici, di interi archivi contenenti centinaia di green pass appartenenti a cittadini italiani, certificati che venivano rivenduti o addirittura posti a disposizione del pubblico su piattaforme di file-sharing per lo scaricamento gratuito, al fine di un successivo utilizzo illecito da parte degli acquirenti;
b) al contrasto ai fenomeni di truffa, basati sulla pubblicazione, su darkweb e canali social, di annunci fraudolenti in cui sedicenti falsari, al solo scopo di adescare le proprie vittime convincendole a rivelare i propri dati personali e a disporre pagamenti anticipati, si dichiarano in grado di fabbricare falsi green pass.
Lo scorso mese di agosto, nell'ambito di una complessa indagine denominata **"Fake pass"**, condotta dal Servizio centrale di Roma e dalle polizie postali di Milano e Bari, ha così individuato e perquisito 4 persone, tra cui 2 minorenni, che gestivano canali social specializzati nell'offerta illegale di certificati green pass Covid-19 falsi, sequestrando i 32 canali Telegram sui quali veniva veicolata la frode.
Grazie al monitoraggio dei pagamenti in cryptovalute effettuati dai clienti per ottenere gli inesistenti green pass, la Polizia Postale e delle Comunicazioni ha ricostruito la rete di vendita, giungendo a disarticolare quelle che, in alcuni casi, si trasformavano in vere e proprie estorsioni: non di rado, infatti, dopo aver millantando di poter fabbricare i falsi green pass, ed essere così entrato in possesso dei dati personali e dei documenti di riconoscimento delle vittime, il truffatore passava a ricattare queste ultime, minacciando denunce alla polizia o ulteriori attacchi informatici nei loro confronti, se non avessero proceduto al pagamento di ulteriori somme di denaro.
c) al contrasto ai fenomeni di intrusione informatica nei sistemi sanitari regionali, allo scopo di poter inserire dati relativi a vaccinazioni e tamponi mai eseguiti, finalizzati ad ottenere il rilascio di certificati green pass.
Risale infatti a pochi giorni fa la messa a segno da parte della polizia postale di una vasta operazione – la più avanzata sinora realizzata nel settore - relativa alla messa in commercio di certificazioni **green pass** radicalmente false, ma in grado di resistere anche ai controlli possibili mediante l'apposita app di verifica, generate mediante furto delle credenziali dei farmacisti e successivo accesso illegale ai sistemi sanitari regionali di **Campania, Lazio, Puglia, Lombardia, Calabria e Veneto.**
Le credenziali di accesso erano carpite alle farmacie mediante sofisticate tecniche di phishing, attraverso email che simulavano la provenienza dal sistema sanitario, e che induce-

vano le vittime a collegarsi ad un sito web, anch'esso falso, perfettamente identico a quello della sanità regionale, in grado di sottrarre le preziose credenziali.
In altri casi, i falsi green pass risultavano prodotti ricorrendo a servizi di chiamata VoIP internazionali, capaci di camuffare il vero numero di telefono del chiamante e simulare quello del sistema sanitario regionale, attraverso cui gli hacker si spacciavano per agenti del supporto tecnico della Regione interessata ed inducevano il farmacista ad installare nel proprio sistema un insidioso software che consentiva di assumere il controllo da remoto del computer e rubare così le credenziali di accesso ai sistemi informativi regionali.
Le indagini - consistite nell'analisi dei dati di connessione, di tabulati telefonici, delle caselle email e delle altre tracce lasciate dai traffici illeciti - hanno consentito di verificare che le tecniche criminose appena indicate sono state messe in campo anche per produrre i cd. Super green pass, a fronte di vaccini mai effettuati.
120 falsi green pass sono stati sinora localizzati nelle province di Napoli, Avellino, Benevento, Caserta, Salerno, Bolzano, Como, Grosseto, Messina, Milano, Monza-Brianza, Reggio Calabria, Roma e Trento, ma sono in corso accertamenti finalizzati a definire il numero reale, che si stima essere assai più ampio, di coloro che si sono rivolti nel tempo all'organizzazione criminale oggetto delle indagini per sfruttarne gli illeciti servizi.
Le perquisizioni, operate dai vari Reparti della Polizia Postale e delle Comunicazioni interessati sul territorio nazionale hanno riguardato le 15 persone già sottoposte ad indagini quali ipotetici appartenenti all'associazione criminosa che risulta aver assicurato la regia degli accessi abusivi ai sistemi informatici e delle conseguenti falsificazioni, nonché 67 dei loro clienti. Con la collaborazione del Ministero della Salute, i falsi green pass individuati sono stati disabilitati, in modo da impedirne ogni ulteriore utilizzo.

Financial Cybercrime

Nel 2021 si è riconfermata una la tendenza, già evidenziata nell'anno precedente, in base alla quale il financial cybercrime si afferma sempre più come una delle forme più predominanti e preminenti del crimine informatico, sia a livello nazionale che globale.
Questa tipologia di reati pone il vantaggio per la criminalità di fornire un immediato riscontro economico alle attività delittuose.
Sono molteplici ed in continua evoluzione le tecniche utilizzate da organizzazioni criminali, che colpiscono il tessuto economico italiano. La minaccia, spesso rappresentata da organizzazioni a carattere transnazionale, è fronteggiata puntualmente attraverso la specializzazione di unità della Polizia Postale che si occupano della materia. Il monitoraggio costante della rete è stato esteso anche al darkweb, e l'obiettivo di prevenire i rischi per i cittadini è stato perseguito anche attraverso campagne d'informazione condivise con il sistema bancario italiano e diffuse sui socialnetwork e sulle piattaforme bancarie.
Il coordinamento delle attività investigative e l'azione di contrasto hanno consentito di individuare e fermare organizzazioni criminali specializzate, attraverso l'applicazione di misure precautelari personali e reali, fino al blocco/congelamento e al sequestro delle somme distratte, consentendone la restituzione alle vittime.

In tale scenario, è proprio il dato, l'informazione relativa all'identità, a costituire l'elemento più pregiato e ambito, che si ottiene grazie alle massive campagne di phishing, di social engineering rivolte soprattutto contro aziende piccole, medie e grandi, che costituiscono l'ossatura del sistema Paese.
Nel settore del contrasto al financial cybercrime, il fenomeno dei "money mules" rappresenta senz'altro una delle modalità più frequenti e consolidate per realizzare frodi online: con la funzione di "teste di legno" cibernetiche, personalità di dubbia moralità si prestano ad essere l'ultimo anello della catena attraverso il quale i criminali monetizzano i proventi del reato. La diffusione di questa modalità e il numero dei soggetti che si prestano a svolgere tale funzione criminale sono in costante crescita e rappresentano ormai una realtà criminale quasi endemica in tutto il mondo. Per tale ragione già da diversi anni EUROPOL ha dedicato al contrasto del fenomeno una specifica Azione (EMMA) ad alto impatto che vede il coinvolgimento di oltre 20 nazioni.
Il 2021, inoltre è stato caratterizzato dalla crescita dell'interesse per le Cryptovalute: i cittadini italiani, anche con bassa scolarizzazione informatica, sono sempre più frequentemente attratti dagli investimenti in Cryptovalute, con la speranza di realizzare i facili e veloci guadagni pubblicizzati.
Quello delle Cryptovalute costituisce un mondo eterogeneo e virtuale, peraltro, non dissimile da quello reale. All'interno di questo mondo è possibile effettivamente fare lauti guadagni, ma anche essere truffati da finte piattaforme di trading online o essere oggetto di furti e frodi attraverso attacchi di phishing.
In tale contesto sono realizzate attività investigative finalizzate a fermare i tentativi di phishing verso i Wallet che le contengono: i truffatori informatici agganciano le vittime attraverso richieste di natura tecnica, su chat ufficiali o semi ufficiali, con la promessa di risolvere i loro problemi gestionali previa cessione delle chiavi private, che permettono la movimentazione delle Crypto (cd. SEED), in realtà queste consentono ai malfattori di prendere il pieno possesso del Wallet e di impadronirsi del contenuto.
Forte anche l'impegno per contrastare il fenomeno del riciclaggio perpetrato attraverso la conversione delle somme frodate in Cryptovalute, sono state infatti coordinate diverse attività investigative dal Servizio Polizia Postale e delle Comunicazioni che hanno visto truffe informatiche ad alto contenuto tecnico conosciute come le BEC, CEO, Vishing, phinshing tentare di realizzare i proventi criminali inviando le somme sottratte tramite bonifico bancario ad exchange di cryptovalute non collaborativi con la Polizia, convertendo la valuta ufficiale in Bitcoin o Ethereum. Tale procedimento gli consente facilmente lo spostamento e spacchettamento delle somme, in attesa di fare cashout.
Per tale ragione è stata intensificata la collaborazione con le grandi società di Exchange di Crypto per i report operativi e per il congelamento delle somme sottratte, così come è stata intensificata anche l'analisi delle transazioni Crypto con la collaborazione degli specialisti di settore di Europol.
La mancanza di confini geografici in Internet consente sempre più frequentemente la formazione di gruppi criminali con nazionalità eterogenee ed è questo che caratterizza ormai

quasi l'intero panorama dei reati commessi attraverso le nuove tecnologie.
Con riferimento al financial cybercrime, in relazione ai fenomeni di phishing, smishing e vishing, tecniche utilizzate per carpire illecitamente dati inerenti le credenziali di accesso ai sistemi di home banking, codici dispositivi, numeri di carte di credito, chiavi private di wallet di cryptovalute, **la Polizia Postale e delle comunicazioni ha registrato 15.068 casi nazionali per i quali sono state indagate 791 persone.** Nonostante la difficoltà operativa di bloccare e recuperare le somme frodate, dirottate soprattutto verso Paesi extra-europei (Cina, Taiwan, Hong Kong), grazie alla versatilità della piattaforma OF2CEN (On line fraud cyber centre and expert network) per l'analisi e il contrasto avanzato delle frodi del settore, **la Specialità ha potuto bloccare e recuperare alla fonte circa 8 milioni di Euro, su una movimentazione di circa 20 milioni di euro, frutto di B.E.C. (Business Email Compromise) e C.E.O. fraud (Chief Executive Officer fraud) in danno di 131 grandi e medie imprese nazionali.** Sono in corso attività di cooperazione internazionale finalizzate al recupero delle restanti somme. A seguito dell'adesione a campagne internazionali ad alto impatto come EMMA 7 (European Money Mule Action), coordinata a livello nazionale dal Servizio Polizia Postale e delle Comunicazioni con la collaborazione di 21 Paesi europei e di Europol, sono state identificate 356 persone in Europa e indagati 205 soggetti nel territorio nazionale. Le transazioni fraudolente sono state 411, per un totale di circa 19 milioni di euro, di cui quasi 12 bloccati e/o recuperati.

Attività di rilievo dell'anno 2021

- **Operazione "Black out"** - Il Servizio Polizia Postale e delle Comunicazioni ha coordinato l'esecuzione, su tutto il territorio nazionale di 45 provvedimenti di perquisizione locale personale ed informatica a carico di partecipi ad un'associazione criminale dedita alla vendita di abbonamenti per lo streaming di canali ad accesso condizionato in violazione della normativa penale sul diritto d'autore.
  Nel corso dell'investigazione, il Compartimento Polizia Postale e delle Comunicazioni per la Sicilia Orientale di Catania, coordinato dalla locale Procura della Repubblica, è riuscito ad individuare una serie di centrali di distribuzione del segnale pirata dislocate in particolare in Sicilia, Puglia e nelle Marche.
  I soggetti coinvolti riuscivano a dirottare il segnale digitale proveniente da una serie di abbonamenti legittimi ad una struttura informatica che assicurava la successiva distribuzione dello stesso a diverse migliaia di utenti, creando così una immensa rete illegale di "abbonati pirata".
  Preme segnalare che fra i soggetti nei confronti dei quali sono stati eseguiti i provvedimenti di perquisizione, vi erano un dipendente della Marina Militare, un dipendente del Ministero della Difesa ed un Consigliere Comunale di un comune della provincia di Agrigento.
- Nel febbraio 2021 il Servizio Polizia Postale e delle Comunicazioni, coinvolto dal Servizio di Cooperazione Internazionale di Polizia, in seguito ad una segnalazione del collaterale tedesco che informava di aver rilevato conversazioni relative alla richiesta di **consumazione di lesioni gravissime ai danni di un'ignara vittima.**

In particolare, all'interno del dark web, nel sito "Internet Assassins", un cliente sconosciuto chiedeva che una persona residente in Italia venisse gravemente ferita, provvedendo al pagamento in moneta elettronica per la prestazione richiesta. Nelle conversazioni con l'intermediario, l'uomo richiedeva esplicitamente la lesione della schiena della vittima con il fine di lasciarla paralizzata e sfigurata con dell'acido. Le transazioni effettuate verso diversi wallet btc avevano un valore di circa 11.700 USD. Nelle conversazioni venivano comunicati i dati della potenziale vittima, una cittadina romana, di 27 anni, della quale veniva fornito anche il profilo personale sulla piattaforma Facebook.

La donna, rintracciata presso la propria abitazione da parte del personale della Squadra Mobile della Questura di Roma, riferiva in un primo momento di non avere sospetti su alcuno. Gli approfondimenti compiuti hanno permesso di riscontrare atteggiamenti molesti ed ossessivi posti in essere da un uomo con il quale la donna aveva intrattenuto una relazione sentimentale fino al luglio 2020. L'uomo è risultato essere impiegato nella stessa azienda della ragazza, in una posizione gerarchicamente sovraordinata.

A fronte della situazione ricostruita, il personale del Servizio Polizia Postale procedeva all'analisi del traffico della moneta elettronica, individuando il wallet di origine, radicato presso una società italiana di Exchange. L'intestatario è, in effetti, risultato essere l'ex fidanzato della potenziale vittima, un uomo di anni 38, residente a Roma. Approfonditi accertamenti OSINT, consentivano di confermare la collocazione lavorativa del soggetto attenzionato e i legami con la potenziale vittima, presenti sulle piattaforme social, ove i due erano in contatto.

A fronte degli importati riscontri emersi, l'A.G. emetteva in urgenza un ordine di custodia cautelare in carcere a carico dell'uomo, al fine di scongiurare il pericolo nel quel versava la vittima. I wallet destinatari dei pagamenti sono stati localizzati in Romania e in Cina. Sono attualmente in corso le attività finalizzate ad individuare i destinatari del denaro inviato per commissionare il delitto.

- **Operazione "Numero Verde"** - Gli operatori del Servizio Polizia Postale e delle Comunicazioni e del Compartimento di Napoli hanno condotto una complessa e articolata attività investigativa, coordinata dalla Procura della Repubblica presso il Tribunale di Torre Annunziata, finalizzata al contrasto dei crimini finanziari in danno di ignari correntisti bancari, che ha visto coinvolti anche il locale Commissariato di PS e la Sezione di PG presso la citata Procura.

  I responsabili delle condotte criminose, risultati appartenere ad un sodalizio criminale sedente sul territorio di Torre del Greco operante su tutto il territorio nazionale, si dedicavano al phishing bancario di ultima generazione i cui proventi venivano monetizzati presso sportelli ATM della città metropolitana di Napoli.

  L'indagine è stata avviata a seguito di un controllo operato su strada nei confronti di un indagato trovato in possesso di un gioiello di valore, acquistato online con i proventi di una frode: quella che apparentemente poteva sembrare una semplice truffa, fin dai primi accertamenti effettuati, ha permesso di documentare complessi risvolti delittuosi.

  Riscostruito il modus operandi degli indagati, all'esito anche di approfonditi accertamenti

tecnici svolti dagli investigatori, si è delineato uno scenario estremamente esteso del fenomeno, che ha consentito, tra l'altro, di individuare diverse vittime sull'intero territorio nazionale. I truffatori, attraverso una stabile organizzazione, riuscivano a procurarsi liste di numeri telefonici di ignari destinatari della frode online-phishing, per poi inviare agli stessi sms fraudolenti (cd. smishing), ai quali facevano seguito telefonate effettuate da falsi operatori bancari, con chiamate provenienti apparentemente dal numero verde/servizi bancari. I criminali riuscivano così ad ottenere le credenziali di accesso ai conti correnti che subito dopo provvedevano a svuotare.

La frode veniva completata attraverso i complici che procedevano agli incassi fraudolenti con ingenti prelievi di somme di denaro presso ATM abilitati con modalità cardless.

Al termine delle attività investigative, l'A.G. procedente ha emesso una ordinanza di custodia cautelare in carcere nei confronti dei sette appartenenti all'associazione criminale, tutti residenti a Torre del Greco, gravemente indiziati dei reati di frode informatica e di associazione per delinquere finalizzata alla commissione di tali frodi. Le frodi accertate sono state 92 frodi per un importo del danno complessivo cagionato alle vittime identificate pari ad euro 94.700,00, tutti sottoposti a sequestro preventivo in attesa degli esiti dibattimentali.

- **"Fake Pass"-** Operazione di contrasto al **commercio online di green pass covid-19 falsi** - Nell'ambito di una complessa attività d'indagine effettuata dal Servizio Polizia Postale e delle Comunicazioni, di concerto con i Compartimenti di Milano e Bari, con il coordinamento delle Procure della Repubblica presso i Tribunali di Roma, Milano e dei minorenni di Bari, sono stati identificati e denunciati a piede libero tre soggetti, tra i quali un minore, gestori di diversi canali Telegram specializzati nell'offerta illegale di Certificati Green Pass Covid-19 falsi, per i reati di truffa e falso.

  Le indagini sono scaturite da un capillare monitoraggio della rete internet, attraverso il quale, gli specialisti della Polizia Postale e delle Comunicazioni, tramite complesse analisi finanziarie della blockchain, la tecnologia alla base delle criptovalute, sono riusciti ad individuare i canali e ad identificarne gli amministratori.

  Erano migliaia gli utenti iscritti ai canali Telegram dove veniva proposta, con garanzia assoluta di anonimato, la vendita dei green pass, da pagare in criptovaluta o buoni acquisto di piattaforme per lo shopping on-line, ad un prezzo compreso tra i 150 ed i 500 euro.

  Sono in totale trentadue i canali Telegram sequestrati dagli agenti della Polizia Postale e delle Comunicazioni nel corso dell'indagine e resi successivamente irraggiungibili in Italia, in esecuzione del decreto di sequestro preventivo emesso dal Giudice per le Indagini Preliminari del Tribunale di Roma, consentendo, così, l'interruzione dell'attività delittuosa.
- **Operazione "EMMA"** - Si è conclusa a fine novembre 2021, l'Operazione di polizia ad alto impatto denominata EMMA, giunta alla sua settima edizione, messa in campo anche quest'anno dalla Polizia Postale e delle Comunicazioni e dalle Forze di polizia cyber di altre 27 Nazioni e coordinata da Europol ed Interpol.

  I numeri complessivi dell'Operazione nei diversi Paesi europei, frutto del lavoro di tutte le Forze di polizia estere impegnate insieme alla Polizia italiana, sono ragguardevoli: anche

grazie al supporto di oltre 400 istituti bancari e altre istituzioni finanziarie, sono state individuate 7000 transazioni bancarie fraudolente, sono state avviate oltre 2500 autonome indagini, riuscendo a prevenire frodi per una danno stimato in 67,5 milioni di euro. Più di 18000 i muli individuati, 324 organizzatori e coordinatori di muli identificati.
L'iniziativa è stata resa possibile anche grazie alla fattiva collaborazione delle banche e degli istituti di credito italiani, che, attraverso CERTFin e ABI, hanno assicurato un supporto in tempo reale agli investigatori, grazie alla piattaforma per la condivisione delle informazioni denominata "OF2CEN", realizzata appositamente dall'Italia al fine di prevenire e contrastare le aggressioni criminali ai servizi di home banking e monetica.

- **Carding Action 2021** - Per il 2021, l'Italia è stata il paese leader in Europa del contrasto al carding nel Dark Web, nell'ambito dell'azione europea ad alto impatto, denominata Carding Action, supportata da Regno Unito, AP TERMINAL e JCAT-EC3 di Europol ed Eurojust.

La Sezione Financial Cybercrime del Servizio Polizia Postale e delle Comunicazioni al termine di una lunga attività di monitoraggio, prevenzione e repressione, durata circa tre mesi, ha determinato il recupero di 16 milioni di euro, il blocco di 49.761 codici di carte di credito trafugate. Tale risultato è stato raggiunto attraverso l'analisi puntuale delle tracce informatiche che hanno consentito di approfondire il fenomeno del carding sul dark web ovvero la circolazione dei codici relativi a carte di credito rubate.
Nel corso dell'azione, grazie all'analisi delle transazioni in criptovaluta utilizzata come mezzo di pagamento dai venditori, sono stati identificati 12 profili, di diverse nazionalità, considerati tra i maggiori venditori di codici di carte di credito compromesse sul dark web, segnalati alle rispettive Autorità dei Paesi in cui essi operavano.

Cyberterrorismo

La costante 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 da cui emergeva la volontà di reagire alle decisioni governative attraverso vere e proprie azioni di piazza, anche violente.
Ed invero, tra le fattispecie illecite che hanno fatto registrare un considerevole incremento c'è sicuramente la diffusione di fake news (notizie destituite di fondamento relative a fatti o argomenti di pubblico interesse, elaborate al solo fine di condizionare l'opinione pubblica, orientandone tendenziosamente il pensiero e le scelte) legate alla propaganda NO VAX/ NO GREEN PASS, nonché di vere e proprie "teorie del complotto" volte a destabilizzare l'ordine democratico ed indirizzare i sentimenti di rabbia nei confronti di determinate "categorie sociali".
Appare evidente, inoltre, come i problemi economici e sanitari causati dall'emergenza coronavirus siano stati strumentalizzati da numerosi esponenti dei movimenti della c.d. ultrade-

stra, per alimentare la disinformazione ed organizzare l'imminente "chiamata alle armi per reagire al caos globale" attraverso azioni di violenza eversiva.
Ed invero, nell'ambito dei fenomeni specificatamente neofascisti e neonazisti e non solo riconducibili al mondo virtuale, il web rappresenta uno strumento strategico per la diffusione della propaganda delle ideologie estremiste e violente, per la strumentalizzazione del malcontento attraverso la propagazione consapevole di notizie "fake", nonché per il reclutamento di nuovi adepti, il finanziamento, lo scambio di comunicazioni riservate nella pianificazione degli attentati e/o azioni di protesta di natura violenta
In tale contesto, tra le varie attività di contrasto poste in essere dalla Specialità si segnala, ad esempio, l'attività investigativa avviata condotte dal Compartimento Polizia Postale e delle Comunicazioni di Milano e dalla locale D.I.G.O.S. e coordinata dalla Sezione Distrettuale Antiterrorismo della Procura di Milano, che ha portato, lo scorso 9 settembre 2021, all'esecuzione di 8 decreti di perquisizione delegata nei confronti di altrettanti soggetti indagati per istigazione a delinquere aggravata.
Oltre al Capoluogo lombardo, le perquisizioni sono state effettuate con la collaborazione degli omologhi Uffici territorialmente competenti – hanno interessato le Province di Roma, Venezia, Padova, Bergamo e Reggio Emilia.
Gli indagati figuravano tra i membri attivi di un gruppo Telegram denominato "I guerrieri" nel quale venivano progettate azioni violente da realizzare – anche con l'uso di armi ed esplosivi fai da te – in occasione delle manifestazioni "no green pass" organizzate su tutto il territorio nazionale.
L'indagine ha tratto origine dalla costante attività di monitoraggio condotta dai due Uffici investigativi milanesi – su input della Direzione Centrale della Polizia di Prevenzione – Servizio per il Contrasto dell'Estremismo e del Terrorismo Interno e del Servizio Polizia Postale e delle Comunicazioni – nei confronti dei numerosi gruppi di protesta attivi sul web contro le misure di contenimento adottate dall'Esecutivo per fronteggiare l'emergenza sanitaria da COVID-19.

Dall'analisi dei messaggi pubblicati sulla chat dei "Guerrieri" è emerso che gli indagati – uno dei quali titolare di porto d'arma e già noto alle Forze dell'Ordine per la sua vicinanza al separatismo veneto – oltre all'intenzione di partecipare in massa alla manifestazione di protesta in programma nella Capitale il prossimo sabato, incitano gli altri membri del gruppo a realizzare azioni violente nelle rispettive Province di residenza, contro non meglio precisati "obiettivi istituzionali" o approfittando della visita di esponenti dell'Esecutivo, come quella – poi annullata – prevista a Padova lo scorso 2 settembre da parte dell'On. Speranza.
A titolo esemplificativo, si segnala l'ulteriore attività avviata dal Compartimento Polizia Postale e delle Comunicazioni di Torino nei confronti degli attivisti NO Vax/NO GreenPass che ha portato all'esecuzione nella mattinata del 15 novembre 2021 di 17 decreti di perquisizione a carico dei soggetti più radicali affiliati al noto canale Telegram "Basta Dittatura", uno degli spazi web di maggiore riferimento nella galassia dei negazionisti del COVID 19.
Il canale era già stato oggetto di un provvedimento giudiziario di sequestro nonché della

decisione di chiusura da parte della stessa società in considerazione della gravità dei contenuti pubblicati.
L'operazione è stata realizzata a seguito delle indagini svolte sotto la direzione dei magistrati specializzati della Procura della Repubblica di Torino, gruppo terrorismo ed eversione.
Le complesse attività che ne sono conseguite, svolte congiuntamente dalla Polizia Postale e dalla DIGOS di Torino, sono state condotte per diverse settimane monitorando h 24 il canale divenuto polo principale nell'organizzazione di proteste violente su tutto il territorio nazionale.
In particolare, "Basta Dittatura" aveva raccolto decine di migliaia di iscritti, risultando il nodo di collegamento con tutti i principali spazi web di protesta, degradata via via in un persistente incitamento all'odio ed alla commissione di gravi delitti; la propagazione virale dei messaggi ha determinato inoltre consistenti disagi nella gestione dell'ordine e sicurezza pubblica delle piazze.
Gli indagati avevano partecipato alla chat istigando sistematicamente all'utilizzo delle armi ed a compiere gravi atti illeciti contro le più alte cariche istituzionali, tra cui il presidente del Consiglio Draghi; obbiettivi ricorrenti sono stati inoltre le forze dell'ordine, medici, scienziati, giornalisti e altri personaggi pubblici accusati di "asservimento" e "collaborazionismo" con la "dittatura" in atto. Presa costantemente di mira con pesanti insulti anche tutta quella parte di popolazione che, vaccinandosi e osservando le regole di protezione personale, ha accettato di rendersi "schiava" dello Stato.

Molti dei perquisiti risultavano già noti alle FF.OO sia per aver aderito a posizioni estremiste sia per precedenti reati quali resistenza a p.u, furto, rapina, estorsione ed in materia di stupefacenti. Tra gli indagati figurano però anche soggetti incensurati caduti nella spirale dell'odio online.
I contenuti e i toni sono risultati esasperati, con riferimenti espliciti a "impiccagioni", "fucilazioni", "gambizzazioni", oltre ad allusioni dirette a "nuove marce su Roma" ed al terrorismo; tra gli identificati anche soggetti che avevano promosso blocchi autostradali e ferroviari nonché attivisti resisi protagonisti di aggressioni di piazza alle forze dell'ordine impiegate per i servizi di ordine pubblico.
Ed ancora, tra le molteplici attività investigative in tale contesto, appare opportuno segnalare quella avviata dal Compartimento Polizia Postale e delle Comunicazioni della Liguria, con il coordinamento del Servizio di Polizia Postale e delle Comunicazioni, e con la partecipazione diretta dei Compartimenti di Milano, Torino, Bari, Roma, Firenze, Venezia, Trieste, Palermo e Catania, nonché delle DIGOS delle citate città, su input della Direzione Centrale della Polizia di Prevenzione, che ha portato all'esecuzione, nelle prime ore del 18 novembre 2021, di ventiquattro perquisizioni nell'ambito di una vasta operazione, coordinata dalla DDA della Procura della Repubblica di Genova, tesa ad individuare i vertici e le figure intermedie di un'associazione segreta NO VAX/NO GREEN PASS i cui appartenenti operavano compiendo attività illecite pianificate da un numero ristretto di individui.
L'indagine è stata avviata nel più ampio contesto degli accertamenti volti a identificare gli

autori di minacce rivolte a esponenti delle istituzioni regionali e a un medico infettivologo, criticati per le loro posizioni a favore della vaccinazione.
I reati contestati agli indagati riguardano la costituzione e partecipazione ad associazione segreta e istigazione all'interruzione di pubblico servizio.
La propaganda tesa ad avvicinare proseliti avveniva su Facebook, con il reclutamento degli affiliati che prendevano il nome di Guerrieri V_V ed ai quali veniva assegnato un numero di matricola; il coordinamento delle azioni illecite avveniva invece su canali Telegram segreti.
Il simbolo dell'organizzazione è formato da una doppia V racchiusa da un cerchio, di colore rosso, probabilmente ispirato al film V per Vendetta.
Una volta entrati nelle chat di reclutamento, gli aspiranti guerrieri dovevano ascoltare una serie di audio, registrati da una voce contraffatta, nei quali si parlava dell'instaurazione di un nuovo ordine mondiale, governato da intelligenze artificiali e si ipotizzavano parallelismi tra il regime nazista e l'attuale situazione di emergenza. Finito il percorso di formazione l'aspirante guerriero doveva superare un esame e veniva guidato da un tutor per la realizzazione delle prime operazioni.
Gli appartenenti alla suddetta associazione erano indotti a compiere azioni di vandalismo ai danni di centri vaccinali, ad intralciare e sabotare la campagna di vaccinazione, e a pubblicare in maniera coordinata e ad orari prestabiliti, tramite account falsi, post denigratori che prendevano di mira in particolare politici, infettivologi e giornalisti.
Specifici programmi di reclutamento erano stati previsti per i no vax appartenenti alle categorie dei sanitari, degli insegnanti e degli appartenenti alle forze dell'ordine.
Sono in corso le indagini volte a identificare altri affiliati e i responsabili degli atti vandalici e degli altri reati commessi dagli aderenti all'associazione.
Si precisa, inoltre, che le previsioni normative circa gli interventi di contenimento e contrasto alla situazione epidemiologica in atto, con particolare riferimento all'obbligo del cd. Green Pass per l'accesso ai luoghi di lavoro a decorrere dal 15 ottobre 2021, hanno dato luogo a crescenti manifestazioni di dissenso, alcune delle quali sfociate in episodi violenti.
In particolare, a seguito dei fatti avvenuti nella Capitale il 9 ottobre 2021, con l'attacco alla sede della CGIL in Roma nel corso di una manifestazione, le contestazioni alla obbligatorietà della "certificazione verde" hanno investito oltre alle persone anche luoghi sensibili e dalla forte valenza simbolica come alcuni Siti istituzionali e delle organizzazioni sindacali maggiormente rappresentative.
In tale contesto, la Specialità ha dato ulteriore impulso all'attività di monitoraggio info-investigativo sulla rete Internet e specificatamente sulle piattaforme di comunicazione online, al fine di intercettare in anticipo ogni evento o manifestazione, in fase preparatoria o organizzatoria, che avrebbe potuto acquisire rilevanza per l'ordine e la sicurezza pubblica, nonché su ogni account che poteva contenere manifestazioni di volontà dirette ad aderire alla protesta con modalità non consentite.
Proprio grazie al monitoraggio effettuato dal Servizio polizia Postale e delle Comunicazioni e dalla DIGOS di Roma a seguito degli scontri occorsi nella Capitale il 9 ottobre 2021, è stato accertato che attraverso il sito ufficiale di Forza Nuova, venivano diffusi, da parte dei

componenti dello Staff e della Redazione del movimento, numerosi comunicati e dichiarazioni volte ad incitare alla violenza contro le Istituzioni e, pertanto, si è proceduto ad informare la competente A.G., che ha ritenuto di emettere un decreto di sequestro preventivo del sito www.forzanuova.eu.
Tale provvedimento è stato eseguito in data 11 ottobre 2021 dal personale della Specialità, tramite la sostituzione della homepage con un'apposita "stop page".
Per concludere, appare opportuno evidenziare come la Sezione Cyberterrorismo sia stata interessa dal Servizio per la Cooperazione Internazionale di Polizia, per la prosecuzione degli accertamenti investigativi finalizzati al rintraccio in Italia di un cittadino nigeriano ventitreenne, destinatario di mandato d'arresto europeo, emesso dalla Germania, in quanto responsabile del reato di stupro, compiuto in un alloggio per richiedenti asilo sito in Germania, nei confronti di una ospite del centro stesso.
Acquisiti i primi utili riscontri investigativi, sotto il Coordinamento della Procura Generale della Repubblica presso la Corte di Appello di Roma, il personale del Servizio Polizia Postale e delle Comunicazioni si è recato tempestivamente a Faenza, dove, grazie all'utilizzo di tecniche di investigazione telematica, e con la collaborazione del personale della Questura di Ravenna e del Commissariato di Faenza, il ricercato è stato tratto in arresto, nonostante la difficoltà determinata dal nascondiglio all'interno in un bunker sotterraneo.
In materia di **cyberterrorismo** (estremismo religioso e politico, area antagonista), nel 2021, la Polizia Postale e delle Comunicazioni ha segnalato all'Autorità giudiziaria **140 persone**. Nel monitoraggio della rete sono stati visionati **130.000 spazi web** ed in **1.200 casi** sono stati rilevati contenuti illeciti.

Commissariato di P.S. Online

L'azione di contrasto attuata, rispetto alle varie fenomenologie delittuose che hanno caratterizzato l'anno 2021, anche in correlazione con l'emergenza Covid-19, è stata realizzata non soltanto sotto il profilo della repressione dei reati tentati o consumati, ma anche nell'ottica di interventi di tipo preventivo.
In tale direzione, il potenziamento dell'operatività del Commissariato di PS online ha permesso di innalzare i livelli di interazione con i cittadini, che hanno mostrato, nella situazione di emergenza sanitaria, 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.

Sintomatico in tal senso il notevole incremento delle segnalazioni pervenute dai cittadini allo "sportello virtuale" della Polizia Postale e delle Comunicazioni, più del doppio dell'anno precedente (per un incremento percentuale pari al + 103%), come pure il numero delle visite e degli accessi[3] che, dopo l'aumento esponenziale registrato nell'anno 2020, si è con-

[3] Riferibile al numero di pagine visionate in occasione di una "visita" al sito.

fermato anche per l'anno 2021 su livelli di assoluto rilievo, facendo registrare un alto indice di popolarità del sito (circa 52.000 accessi).

PERIODO	SEGNALAZIONI	INFORMAZIONI
2019	23.311	22.853
2020	56.532	25.952
2021	114.989	29.229

PERIODO	VISITE	ACCESSI
2019	1.027.726	28.672.115
2020	3.216.779	65.630.427
2021	2.962.332	51.891.661

Grazie alle segnalazioni pervenute al Commissariato di P.S. online, sono stati realizzati 70 interventi per casi di suicidio annunciati in rete da utenti tempestivamente individuati in emergenza dal personale specializzato, a seguito dello sviluppo di attività di indagine informatica.
Istituito nell'anno 2006 per consentire agli utenti del web di avere delle risposte in tempo reale su ciò che accade nella rete ed evitare loro di cadere nelle tante insidie della navigazione in internet, il "Commissariato di P.S. on line" è stato concepito come un portale (raggiungibile attraverso la URL www.commissariatodips.it) gestito da investigatori, tecnici ed esperti del settore, volto a garantire un servizio attivo in materie giuridiche e sociali.
Nel corso degli anni, il portale è stato rinnovato, sia nella grafica che nella tipologia delle richieste che il cittadino può inoltrare, rimodulando la piattaforma con nuove funzionalità orientate a profili di maggiore efficienza e finalizzate non solo all'informazione, ma anche alla divulgazione di una cultura orientata alla sicurezza informatica in ogni sua declinazione.

Il nuovo sito web si caratterizza, infatti, per le modalità di offerta di notizie e consigli utili per un uso sicuro, consapevole e responsabile della rete, con specifici riferimenti ai social network grazie anche all'innovativa pagina Facebook del Commissariato online.
Questa nuova veste e finalità si inserisce nella più ampia attività di comunicazione che la Specialità svolge, anche in collaborazione con altre articolazioni dipartimentali ed altri Ministeri, 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 ed una consapevolezza sempre crescente dei rischi e pericoli del web.
Uno strumento agevole che permette al cittadino, da casa, dal posto di lavoro o da qualsiasi luogo si desideri, di accedere al sito web dedicato ed usufruire dei medesimi servizi di segnalazione, informazione e collaborazione che la Polizia Postale e delle Comunicazioni quotidianamente offre agli utenti e che ha mostrato in maniera ancora più evidente la sua

efficacia nel periodo connesso all'emergenza pandemica da Covid-19.
Nell'ambito del diversificato contesto operativo della 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.
In tale direzione è proseguita anche nel 2021 l'attività costante di contrasto a tale fenomeno - che aveva visto un crescente proliferare nel 2020 -, attraverso la predisposizione e diffusione di specifici alert, funzionali alla veicolazione delle corrette informazioni.
All'interno del sito, inoltre, è presente una sezione dedicata alle "news" attraverso cui gli utenti vengono informati circa i fenomeni del momento presenti in rete e per il cui tramite vengono divulgati "alert" riguardanti situazioni di pericolo nelle quali si può incorrere durante la navigazione. Nella medesima sezione vengono, inoltre, veicolati i comunicati stampa sulle più importanti operazioni della Polizia di Stato.

Campagne preventive di sensibilizzazione

Oltre al monitoraggio continuo della rete, la Polizia Postale e delle Comunicazioni è impegnata costantemente nella progettazione e realizzazione di campagne di sensibilizzazione e di educazione al corretto uso delle tecnologie, nel tentativo di far comprendere agli adolescenti, che talora non ne percepiscono a pieno il disvalore, le conseguenze che possono derivare dall'uso distorto della rete. In relazione alle misure di contenimento dell'emergenza epidemiologica da COVID-19, le predette iniziative sono state portate avanti anche con incontri in videoconferenza, riscuotendo consensi e partecipazione da parte di alunni, genitori e insegnanti.

Tale ulteriore opportunità di incontro ha consentito di arricchire l'azione preventiva realizzata rispetto a determinate fenomenologie delittuose atteso, peraltro, che proprio in queste occasioni vengono spesso segnalati episodi o situazioni che permettono quel tempestivo intervento utile ad impedire la consumazione di un reato o l'aggravarsi delle conseguenze di determinate condotte che sovente vedono protagonisti i giovani.

Tra le iniziative più significative si inserisce "Una vita da Social", la campagna itinerante attraverso la quale la Polizia di Stato incontra, in collaborazione con gli istituti scolastici, studenti, docenti e genitori che, nell'anno scolastico 2020-2021, si è svolta prevalentemente in modalità videoconferenza. Per la 9^ edizione, relativa all'anno scolastico in corso, in relazione al ritorno in presenza dei ragazzi in aula, è stato possibile ricominciare ad organizzare diversi incontri de visu con la platea scolastica, ripristinando anche la caratteristica di campagna itinerante del progetto.

L'impegno profuso dagli specialisti della Polizia Postale e delle Comunicazioni nell'azione di sensibilizzazione e informazione ha consentito, **nel corso dell'anno 2021 di realizzare incontri con 2.200 istituti scolastici e di veicolare contenuti educativi a oltre 93.000 studenti, più di 6.000 docenti e circa 4.700 genitori.**

L'azione preventiva è proseguita con costanza e dedizione anche nei confronti del cyberbullismo, un fenomeno che desta grande allarme sociale. Una coinvolgente campagna realizzata periodicamente in questa prospettiva dalla Polizia Postale e delle Comunicazioni è il format teatrale #cuoriconnessi dedicato agli studenti delle scuole, con il quale, attraverso uno spettacolo in cui il conduttore concentra l'attenzione del pubblico sull'importanza delle parole in tutte le sue sfumature, con filmati, letture, musiche e testimonianze dirette, vengono forniti agli spettatori informazioni utili alla corretta navigazione in rete, volte anche a stimolare nei ragazzi una sempre maggiore consapevolezza della gravità delle azioni prodotte on line, in relazione all'impatto prodotto nella vita dei loro coetanei.

Per l'anno 2021, la 5^ edizione della citata manifestazione è stata realizzata in data 9 febbraio, in occasione del Safer Internet Day, giornata mondiale per la sicurezza in Rete, con un grande evento on line, durante il quale la Polizia di Stato si è collegata, attraverso una piattaforma dedicata, con oltre 200 mila studenti di 3 mila scuole italiane.

Email security in Italia

[A cura di Rodolfo Saccani, Libraesva]

Avrete notato come si stia diffondendo una modalità di descrivere lo stato della security non attraverso i dati reali ma attraverso il tentativo di quantificare i rischi percepiti. Mi riferisco alle affermazioni del tipo *"L'X% dei responsabili IT è preoccupato da Y"* che leggiamo sempre più spesso nei report sullo stato della security.
È una tendenza per certi versi curiosa ma indicativa del problema di cui stiamo per parlare.

Descrivere lo stato della email security basandosi su numeri e statistiche sta diventando meno efficace e, volendo sintetizzare al massimo, il motivo è sostanzialmente il naturale processo di evoluzione e selezione.
Gli attacchi massivi, quelli tradizionali che spesso sono poco sofisticati e condotti su ampia scala, pongono sempre meno problemi grazie all'evoluzione dei sistemi posti a protezione della posta elettronica.
Al contempo emergono in modo sempre più capillare campagne sofisticate, mirate o comunque con componenti di personalizzazione, condotte con messaggi confezionati in modo spesso curato e competente.
Questi messaggi, proprio in quanto personalizzati, vengono consegnati in quantità tali da confondersi col rumore di fondo e rendere meno efficaci i metodi di contrasto che funzionano con le campagne più tradizionali.

Quando parliamo di attacchi mirati e sofisticati naturalmente parliamo di phishing. Il phishing è lo strumento attraverso il quale si ottiene l'indispensabile collaborazione da parte della vittima, la quale deve in un modo o nell'altro fare la sua parte.
L'obiettivo può essere il furto di credenziali, la consegna di malware, la truffa con fine economico, il furto di informazioni confidenziali. Gli obiettivi cambiano ma la collaborazione della vittima è sempre necessaria. Le tecniche utilizzate e le leve psicologiche in fondo sono le medesime, indipendentemente dal fine ultimo.

Sebbene un attacco mirato non lasci tracce evidenti dal punto di vista statistico, quando colpisce ha una efficacia di ordini di grandezza superiore rispetto agli attacchi massivi e di bassa qualità, quelli su cui si concentra la gran parte delle analisi statistiche e dei report di fine anno.

L'estrazione di statistiche più o meno accurate dai flussi di posta diventa quindi sempre meno utile, mentre la cosiddetta "expert analysis" diventa sempre più rilevante.
Non fraintendiamoci: avere una ampia visibilità sui flussi è ancora estremamente importante ma quando ci si trova a fare il punto sui rischi concreti a cui la posta elettronica ad oggi ci espone, la qualità conta molto più della quantità.
Adesso probabilmente ci è più chiaro anche il trend di cui parlavamo in apertura.

Per capirci meglio partiamo direttamente da un esempio pratico:

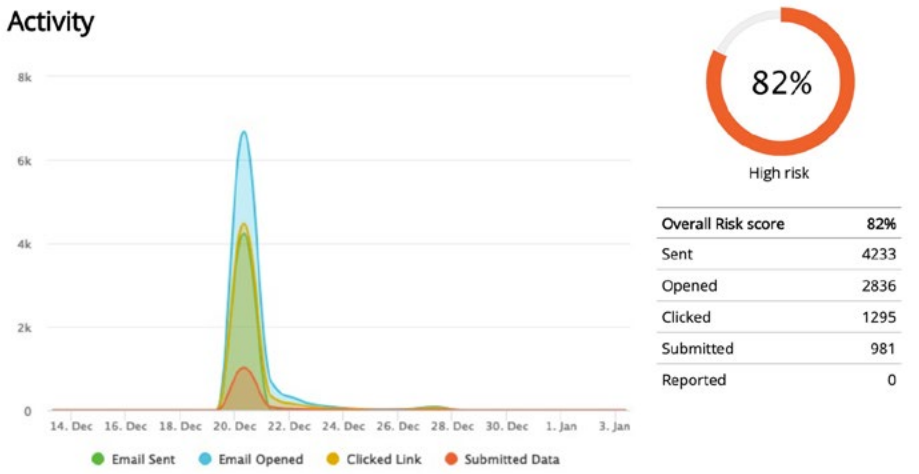


Figura 1 - *Campagna di phishing simulato (Fonte: servizio PhishBrain di Libraesva)*

La figura precedente mostra gli esiti di una campagna di phishing simulata: una finta email di auguri natalizi inviata ai dipendenti di un'azienda italiana.

Le campagne di phishing simulato sono lo strumento ideale per andare a misurare in modo rigoroso la permeabilità di una organizzazione al phishing. Rappresentano uno strumento di misura ancora più efficace dell'analisi delle campagne di phishing reali e non solo perché, come abbiamo già detto, una parte di queste attività illecite resta inosservata falsandone la percezione, ma anche perché nelle campagne simulate si elimina gran parte della variabilità e dell'aleatorietà.

In una campagna simulata si può stabilire in anticipo il livello di "difficoltà" della campagna stessa attraverso la modulazione della qualità e la quantità degli "indizi" contenuti nel messaggio e poi si va a misurare in modo preciso la quantità di azioni eseguite sul totale delle mail consegnate. È anche possibile misurare la progressione, nel tempo, del livello di rischio sullo stesso bacino di utenti. Il tutto attraverso una metodologia uniforme e riproducibile. È più o meno la stessa differenza che passa tra una analisi epidemiologica, con tante variabili difficili da controllare, e un trial clinico in doppio-cieco. Entrambi gli approcci sono utili e necessari ma nel periodo storico che stiamo vivendo l'analisi epidemiologica a cui siamo abituati diviene sempre meno utile a comprendere uno scenario che muta velocemente in una direzione più insidiosa.

Cerchiamo quindi di utilizzare questo approccio metodologico che abbiamo paragonato ad un tiral clinico per rispondere alla domanda oggi più interessante: quanto sono "permeabili" le aziende italiane alle campagne di phishing mirato, ovvero agli attacchi via posta elettronica che più ci preoccupano?

Nell'esempio che abbiamo appena visto, che è un caso rappresentativo, c'è un numero che salta immediatamente all'occhio: quasi un quarto dei destinatari ha fornito le proprie credenziali all'attaccante. Una condizione che può rivelarsi fatale per una qualunque organizzazione.

Eppure in questo caso la campagna di phishing simulato era classificata come "moderatamente difficile" in quanto erano stati lasciati all'interno del messaggio alcuni indizi di maliziosità. Quali sono gli elementi che rendono una campagna di questo tipo così efficace nonostante tutto?

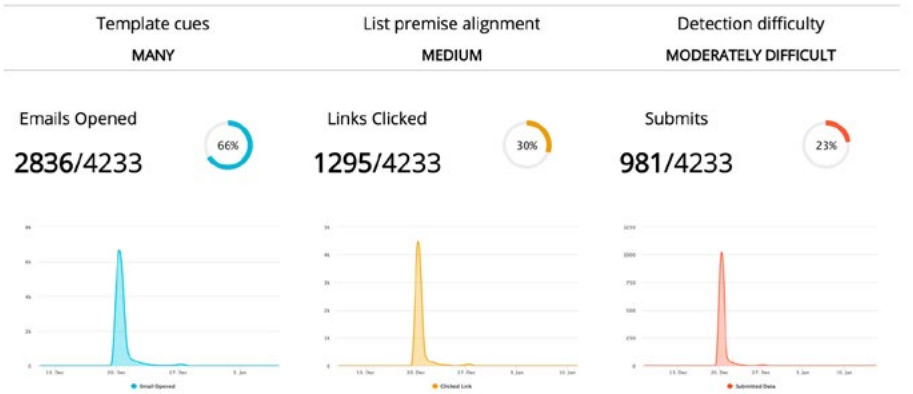


Figura 2 - *Metriche di una campagna di phishing simulato (Fonte: piattaforma PhishBrain di Libraesva)*

L'efficacia di un messaggio "mirato" rispetto ad uno più generico e massivo è evidente. È sufficiente un minimo di personalizzazione per superare la gran parte delle difese. Il messaggio personalizzato viene di per sé ritenuto molto più sicuro di un messaggio generico.
Se alla personalizzazione aggiungiamo un elemento emotivo che induca sollecitudine o urgenza, magari lasciando intravedere un potenziale beneficio individuale, il tempo che viene dedicato all'analisi del messaggio stesso si riduce e l'efficacia del messaggio stesso aumenta.

Tornando al nostro esempio, gli auguri aziendali ricevuti al momento giusto nel periodo prefestivo e la possibilità di un premio individuale la cui entità può essere rivelata autenticandosi, producono il risultato che vediamo.

Il messaggio di per sé non è particolarmente sofisticato e neppure sono presenti riferimenti specifici all'organizzazione o al destinatario se non un logo, ma spesso è sufficiente la presenza di un semplice logo aziendale per far percepire il messaggio come legittimo e abbassare in modo sensibile le difese.

Analisi come questa ci portano a comprendere in modo sempre più puntuale quali siano le leve più efficaci, quali piccoli dettagli facciano la differenza tra una campagna molto efficace ed una poco efficace. A parità di "effort" da parte dell'attaccante, una migliore conoscenza dei meccanismi legati al social engineering e l'attenzione a determinati piccoli dettagli può essere un grande amplificatore dell'efficacia di una campagna di phishing.

È opportuno che questa conoscenza non venga lasciata nelle mani degli attaccanti ma sia acquisita tempestivamente da chi difende. La rilevanza degli attacchi massivi che abbiamo visto evolvere negli ultimi anni va scemando, anche grazie all'evoluzione dei sistemi di protezione nei confronti di una metodologia ormai nota. È il momento di iniziare a porre l'attenzione sulla pericolosità degli attacchi mirati ed è il caso di farlo prima dei nostri avversari.

Per quanto riguarda gli attacchi con obiettivo estorsivo (principalmente ransomware) gli attacchi sono sempre più "ottimizzati" con bersagli e richieste di riscatto scelti con oculatezza in modo da massimizzare il ritorno economico.
Sempre più spesso l'esfiltrazione di dati precede la crittografia degli stessi e alla richiesta di riscatto per poter decrittare i dati (che è meno efficace se l'azienda ha una efficiente policy di disaster recovery) si affianca la minaccia di rendere pubblici i dati trafugati.
Quello che viene consegnato via email è il cosiddetto "dropper" o "stage 1", un piccolo malware solitamente nella forma di una macro in un documento Office che ha il compito di installare il malware vero e proprio (payload) che viene scaricato da internet o estratto dal dropper stesso ove è conservato in forma cifrata.
Questo tipo di attacco è tanto meno efficace quanto più sono allo stato dell'arte i sistemi di protezione della posta elettronica. L'approccio basato su riconoscimento di signature e pattern, con la sua inevitabile latenza, viene agevolmente superato da una nuova variante o una nuova famiglia di malware. Una protezione di tipo proattivo in grado di rimuovere le istruzioni che abilitano alla realizzazione del dropper stesso resta ad oggi lo strumento più efficace. L'approccio segue una logica simile a quella dei "firewall", il documento viene scomposto e analizzato, le istruzioni che abilitano alla realizzazione di un dropper (recupero, scrittura ed esecuzione del payload) non sono consentite e vengono rimosse. Questo approccio impedisce il passaggio di varianti ancora ignote.
La suscettibilità delle aziende a questo tipo di attacchi dipende quindi in modo diretto dal tipo di protezione che viene adottata ma se la protezione è adeguata il rischio è ragionevolmente basso.

Il livello di rischio diviene più uniforme tra le varie organizzazioni quando passiamo ad analizzare gli attacchi basati su furto di credenziali. Dal punto di vista tecnico è assai più difficile intercettare una mail di phishing ben confezionata rispetto ad una mail contenente un dropper.
Al contempo, lo spostamento sempre più massivo verso servizi cloud, rende più facile per gli attaccanti simulare le richieste di login di servizi cloud che sono sempre più comuni e standardizzate.

Come abbiamo visto la personalizzazione del messaggio è uno strumento altamente efficace in questo tipo di attacco. La personalizzazione non si limita al messaggio di posta elettronica ma sempre più spesso prosegue sulla "landing page", ovvero la pagina web (solitamente ospitata su un sito internet legittimo che è stato compromesso) a cui l'utente arriva dopo aver cliccato sul link di phishing presente nella mail.

Diversi toolkit infatti recuperano in modo automatico il logo aziendale a partire dall'indirizzo email contenuto nel link di phishing e quindi adattano in tempo reale la pagina in base alla vittima che la sta visitando.

L'immagine che segue mostra un esempio di una di queste landing page.

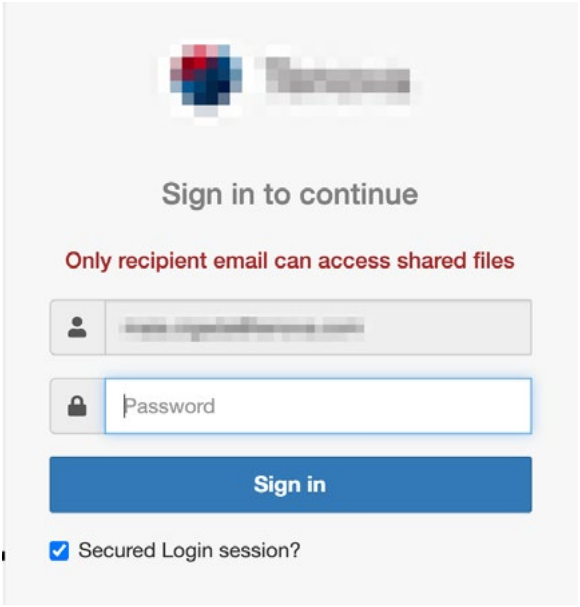


Figura 3 - *Landing page con logo recuperato automaticamente (Fonte: Libraesva)*
Quasi sempre l'indirizzo email della vittima viene inserito nel link, ogni email ha quindi un

link diverso che viene generato in base all'indirizzo destinatario di quella mail. È la stessa tecnica che utilizzano tutte le piattaforme per l'invio di email transazionali o pubblicitarie.

Spesso è sufficiente modificare l'indirizzo all'interno del link per vedere apparire un logo diverso, in questo esempio ho inserito il mio indirizzo personale di lavoro in un link di phishing recuperato da una campagna reale, ed ecco apparire il logo e il nome della mia azienda nello stesso form di phishing che poco fa ne mostrava un altro:

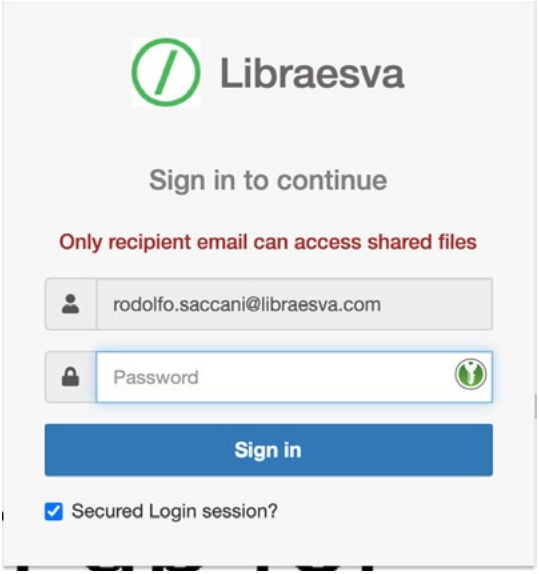


Figura 4 - *Viene automaticamente mostrato il logo aziendale (Fonte: Libraesva)*

Sono diversi i servizi pubblici che consentono di recuperare in modo molto facile il logo di un'azienda a partire da un nome di dominio, gli autori di queste campagne utilizzano questi servizi al fine di massimizzare l'efficacia della campagna di phishing. Si tratta di uno di quei piccoli dettagli che fanno la differenza.

Possiamo fare lo stesso "gioco" modificando il dominio dell'indirizzo email creando un indirizzo inesistente sul dominio clusit.it, ed ecco apparire il logo del CLUSIT.

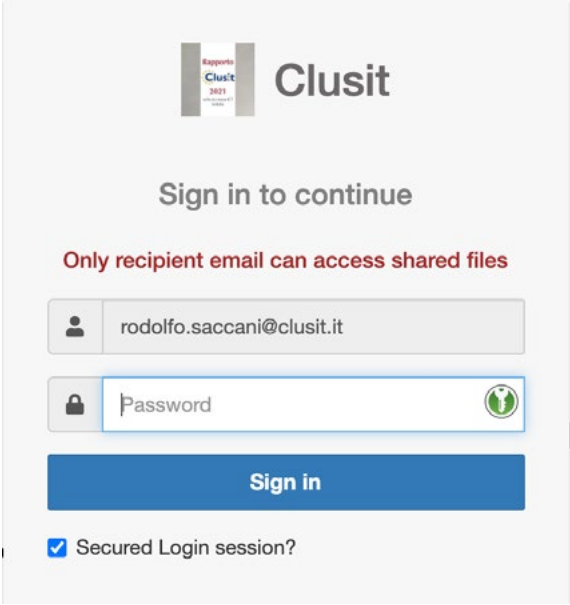


Figura 5 - *Landing page con logo CLUSIT (Fonte: Libraesva)*

Chiudiamo con un ultimo esempio di una di queste landing page relative a una campagna di phishing ancora attiva nel momento in cui scriviamo.

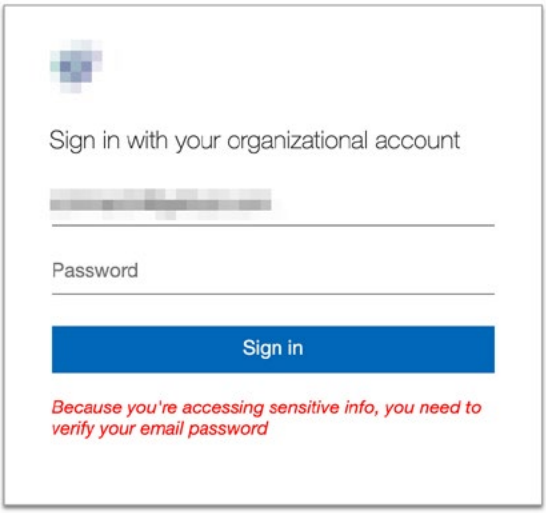


Figura 6 - *Ancora un esempio di landing page personalizzata (Fonte: Libraesva)*

I sistemi di "URL sandboxing", ovvero l'analisi in tempo reale, al momento del click, del contenuto e del comportamento della pagina che sta per essere visitata partendo da un link presente in una email, rappresentano uno strumento molto efficace a patto che l'analisi non si limiti alla consultazione di blacklist ma prenda in considerazione i toolkit di phishing, i tentativi di offuscamento ed evasione e le richieste di inserimento di informazioni confidenziali in qualunque forma.
Anche in questo contesto non è più sufficiente limitarsi a bloccare pagine note come malevole ma è indispensabile entrare nel merito del comportamento delle stesse, sapendo cosa cercare grazie alla conoscenza delle modalità operative degli autori di questo tipo di attacco.

L'email security sta entrando in una nuova fase, una fase in cui la specializzazione è sempre più indispensabile e in cui alle competenze tecniche vanno affiancate competenze di tipo diverso, oltre ad una capacità di analizzare e comprendere i fenomeni con un approccio di tipo scientifico e strumenti in grado di misurare la permeabilità della propria organizzazione nel tempo.

Le piattaforme di simulazione di campagne di phishing rappresentano uno strumento estremamente efficace per valutare, monitorare e migliorare la componente umana al fine di ridurre il rischio rappresentato dalle campagne di phishing mirato che inevitabilmente prima o poi riusciranno a superare la difesa perimetrale magari raggiungendo l'utente sul suo dispositivo personale attraverso un SMS.
È opportuno e necessario estendere questo tipo di lavoro di formazione e prevenzione nei confronti del personale anche a questi canali che tradizionalmente restano al di fuori del perimetro aziendale ma che ad oggi vengono già attivamente utilizzati per veicolare attacchi.

Seguono un paio di esempi di campagne di smishing (SMS phishing) simulate costruite imitando le campagne reali attualmente in circolazione, campagne attraverso le quali gli attaccanti provano a raggiungere i dipendenti attraverso canali non protetti:

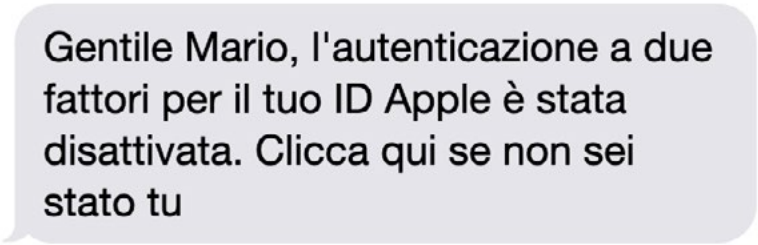


Figura 7 - *Esempio di SMISHING (Fonte: Libraesva)*

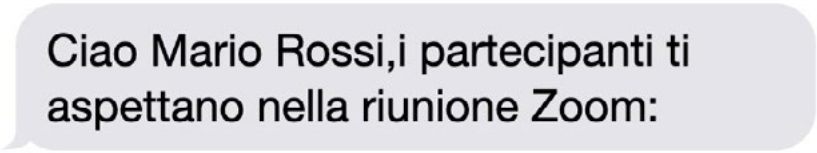


Figura 8 - *Altro esempio di SMISHING (Fonte: Libraesva)*

Gli attacchi di phishing che puntano al furto di credenziali rappresentano un pericolo concreto e in crescita. La compromissione di account aziendali rappresenta il primo passo per una serie di attività illecite quali la distribuzione di malware e ransomware dall'interno dell'azienda stessa (bypassando quindi la protezione perimetrale), il furto di informazioni, l'estorsione, lo spionaggio industriale e l'utilizzo delle infrastrutture aziendali come trampolino per ulteriori attacchi verso altre organizzazioni.
Ogni cosa ha un valore sul mercato del dark web. Le credenziali, i contenuti delle mailbox, gli accessi ad infrastrutture aziendali vengono venduti e acquistati in tempi brevissimi, spesso più volte, portando in breve tempo una varietà ed una molteplicità di attori malevoli all'interno della propria organizzazione.

Preso atto del fatto che le minacce si fanno più subdole e che le tecniche di attacco evolvono in direzioni più difficili da monitorare, da quantificare e anche da intercettare, è opportuno che le organizzazioni restino al passo con l'evoluzione delle tecniche di attacco le quali seguono una naturale evoluzione verso lo sfruttamento dei punti di ingresso più deboli, inclusi gli individui.
Il problema si fa meno tecnico, più metodologico e sempre più specialistico.

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 2021, ed evidenzio alcune tendenze che potremmo osservare nei primi mesi del 2022. 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 settore finanziario, che include le istituzioni bancarie e assicurative, è stato il più attaccato per il quinto anno consecutivo [1] attirando il 23% di tutti gli attacchi registrati.
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 attaccarne i clienti in quanto obiettivo indubbiamente più facile.
L'analisi delle principali campagne del 2021 mostra che la frode avviene prevalentemente attraverso i seguenti vettori di attacco:

- malware per il furto di credenziali o fattori addizionali di autenticazione o manipolazione di una transazione;
- phishing per il furto di credenziali di accesso e dei fattori di autenticazione forte (credential theft), quasi sempre combinata con l'interazione con un finto operatore;
- hacking del dispositivo mobile tramite SIM Swap o emulazione software dello smartphone;
- e infine, attacco diretto all'infrastruttura dell'istituzione finanziaria, sfruttando vulnerabilità spesso note ma non fissate.

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

Il furto delle semplici credenziali di accesso, intese come nome utente e password, da solo non basta a portare a termine un attacco. Domina, nella quasi totalità dei casi e sia per vittime nel mercato retail che corporate, la combinazione di più tecniche per costruire schemi di manipolazione completa dell'utente.

Financial malware

ENISA, Agenzia dell'Unione Europea per la Cybersecurity, pone i malware tra le principali minacce cyber del biennio 2020/2021 [3], secondi solo agli attacchi ransomware.
Nel contesto variegato di tutti i malware, qui analizziamo *solo i financial malware* o malware per frodi finanziarie. Riportiamo dati e valutazioni sul malware per frodi al settore finanziario e alle sue declinazioni (banche, assicurazioni e finanza) limitatamente a osservazioni fatte da IBM Security Trusteer nell'area geografica EMEA (Europa, Medio Oriente e Africa) sull'intero anno 2021.
QakBot, Ursnif/Gozi e Bugat sono stati i principali malware dell'anno, seguiti da una nutrita lista di altri malware con impatto minore.
Non ci sono sostanziali novità tra i malware più diffusi rispetto al 2020, piuttosto un riposizionamento di alcuni di essi e la forte perdita di terreno di TrickBot, legata allo smantellamento della Botnet di TrickBot (ottobre 2020) [5], seguita poi dallo smantellamento delle tre botnet Epoch 1, 2 e 3 di Emotet (gennaio 2021) [10][11], che erano state uno dei principali veicoli di diffusione di TrickBot.
Ci sono state invece novità relativamente alla comparsa di nuovi codici malware, per adesso ancora di impatto limitato, e con loro nuovi attori, a riprova della fase di espansione del settore del cyber crime. Un settore che continua a popolarsi di persone tecnicamente molto preparate e capaci di mettere in difficoltà le soluzioni tecnologiche e i processi messi in campo per limitare il fenomeno.

Figura 1

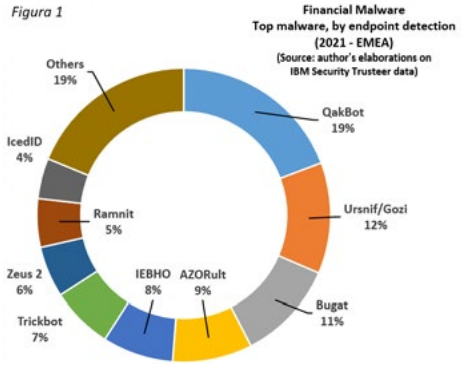
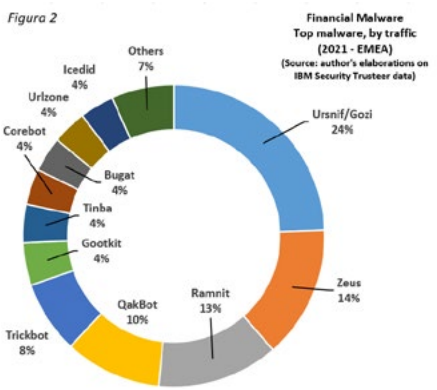


Figura 2



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.
In questo primo diagramma e nel successivo (**Figura 2**) abbiamo scelto di *non* riportare l'incidenza di Emotet, diffuso in Italia e nel resto d'Europa, in quanto il suo ruolo è stato prevalentemente di *loader* (veicolo di distribuzione) per altri malware, in particolare QakBot e TrickBot, attraverso un sodalizio tra i gruppi criminali. In questo connubio, Emotet è il veicolo che elude le misure di protezione della rete e dell'endpoint, infettando la macchina della vittima per poi scaricare il payload, spesso l'eseguibile di QakBot o TrickBot, a cui poi lascia il controllo. Questi ultimi, in molti casi, hanno poi ulteriormente veicolato il ransomware Ryuk o altri malware, con un incapsulamento di malware all'interno di altro malware.

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**) e il traffico verso le rispettive infrastrutture di Command and Control (C2).
In questo caso, i malware che hanno generato maggiore attività sono Ursnif/Gozi, Zeus, Ramnit, QakBot, Trickbot. Anche qui si conferma il riposizionamento di alcuni malware già diffusi negli anni precedenti, assieme alla comparsa di nuovi malware che emergono rapidamente alla conquista di vittime.
Questa seconda tipologia di rilevazione è speculare a quanto già osservato relativamente agli endpoint infetti. 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 endpoint 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 o verso l'infrastruttura di Command-and-Control (tipicamente una botnet) 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 osservare, individuare e rispondere ad entrambi i fenomeni, combinandoli per proteggere l'endpoint durante ciascuna fase della transazione bancaria.

Attività dei principali financial malware nel corso dell'anno

I malware per frodi finanziarie mirano anzitutto ad impossessarsi delle credenziali di accesso o dei fattori aggiuntivi di autorizzazione nei 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 dalla normativa PSD2 [6], al furto dei dati delle carte di pagamento e,

infine, allo "IBAN Swapping", ovvero la sostituzione delle coordinate di pagamento IBAN o del wallet elettronico; questo ultimo caso soprattutto per i malware sui dispositivi mobili.

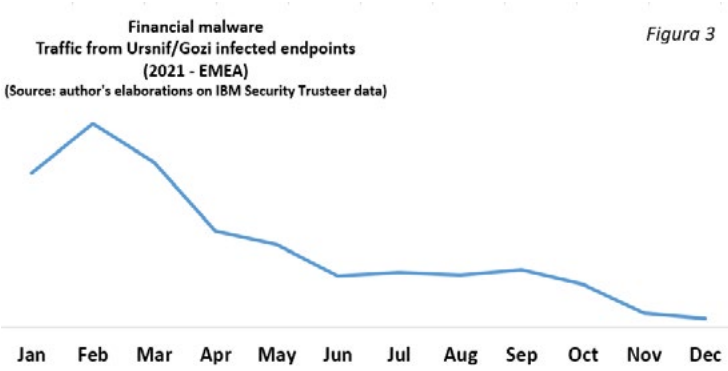
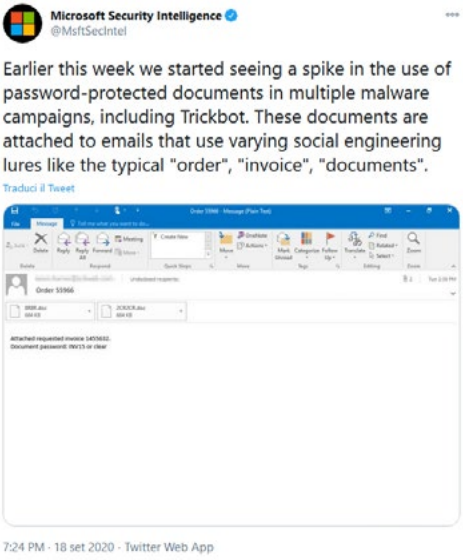


Figura 3

Ursnif, conosciuto anche come Gozi, è uno dei più antichi malware bancari ancora attivi e al centro di numerose campagne verso utenti di online banking anche in Italia. IBM X-Force ha individuato ed analizzato una variante di Ursnif/Gozi [37] costruita per infettare il sistema Windows della vittima e contemporaneamente anche il suo dispositivo Android con il malware Cerberus. La componente Cerberus dell'attacco serve a catturare i codici dispositivi inviati dalla banca attraverso SMS.
Cerberus è un malware per dispositivi Android di tipo overlay. Consente di mostrare sullo schermo del dispositivo mobile schermate disegnate dagli attaccanti appositamente per richiedere l'inserimento di elementi di autenticazione, che vengono catturati e inviati all'esterno. Emerso nel 2019, era inizialmente privo di funzionalità avanzate. Ora si è evoluto fino ad implementare la capacità di catturare gli SMS ricevuti ad esempio con One Time Password, aprire overlay personalizzati sul layout grafico della banca online e rubare codici 2FA da Google Authenticator. Funzionalità aggiuntive includono l'accesso alla carta di credito del cliente, la possibilità di reindirizzare le chiamate, accedere al dispositivo tramite le funzionalità di Remote Access Tool e di concedere le autorizzazioni richieste dalle App.

Il vettore di infezione iniziale di Ursnif/Gozi sono documenti Office con macro malevole allegate a email artefatte, in apparenza contenenti fatture, avvisi di consegna o altra corrispondenza commerciale. Una volta infettate dal malware Ursnif e dopo aver tentato di accedere al proprio conto bancario online, le vittime ricevono un messaggio a schermo che le invita ad installare un'app di sicurezza per continuare a utilizzare i servizi della propria banca. Per questo viene mostrato loro un QR code da scansionare con il proprio telefono. Alla scansione del QR vengono reindirizzati su una pagina Google Play falsa, che usa typo-squatting o URL verosimili, e con il logo dell'app bancaria corrispondente alla banca della vittima. Questa app in realtà installa il malware Cerberus sul dispositivo mobile.

L'opzione di non consentire l'installazione di app da fonti sconosciute, disabilitata di default sui dispositivi Android, ha fortunatamente limitato l'impatto che questo tipo di campagne potrebbe aver avuto.
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, anche apparentemente insignificante, può essere utile per costruire e dare maggiore credito all'attacco, o collezionare informazioni per attacchi futuri.



Come nell'esempio di Ursnif già citato, i malware sono stati veicolati nella maggioranza dei casi attraverso documenti Office allegati a 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 prevalentemente 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.

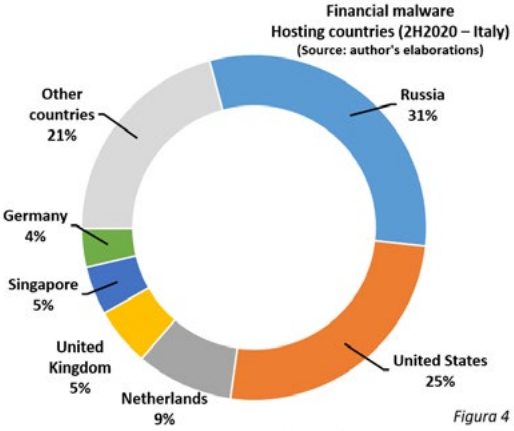
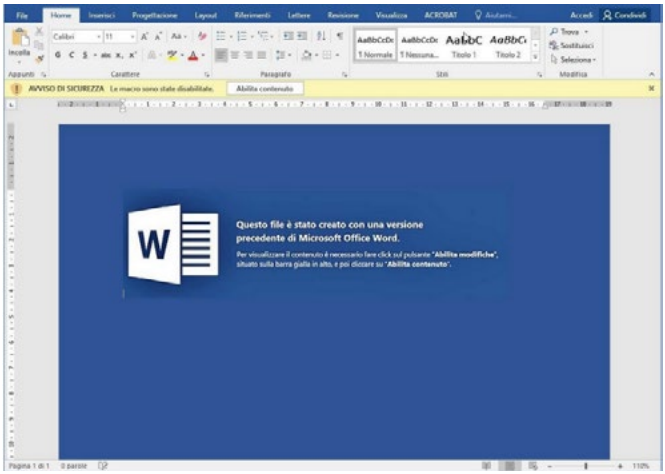


Figura 4

Il malware è ospitato su provider russi nel 31% dei casi, statunitensi del 25% dei casi, ed in percentuali via via descrescenti 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.
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 nel luglio 2020, 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 da molti siti di Threat Intelligence 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 *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.



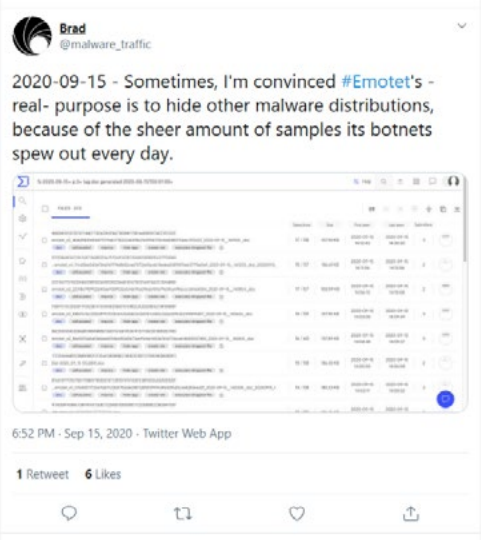
Nel corso del 2019 avevamo osservato molti documenti malevoli sfruttare la CVE-2017-0199 e la CVE-2017-11882, due Remote Execution Vulnerability per Windows molto insidiose. Era sufficiente aprire il documento, e in talune circostanze fare la sola preview, per eseguire la componente malevola che scaricava il codice malware. Il meccanismo, su macchine non aggiornate, era particolarmente potente in quanto richiedeva un'interazione minima da parte della vittima.
Nel corso del 2020 e 2021 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 far 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, dai quali riceve ulteriori elementi di configurazione, watchlist, comandi remoti da eseguire sul sistema infetto, o attraverso i quali esfiltra i dati della macchina infetta, come username, password o URL visitate.
La pandemia COVID-19 ha favorito numerose ondate di spamming costruite 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.

Ottima l'iniziativa "I Navigati – Informati e sicuri", campagna di informazione e sensibilizzazione sulla sicurezza informatica, promossa dal CERTFin, per i clienti del settore bancario, finanziario e assicurativo che, con video molto chiari e incisivi, ha mostrato il funzionamento delle più comuni minacce e attacchi e spiegato le semplici regole e contromisure per non caderne vittima. La campagna è stata veicolata sia sui social network che sui canali televisivi e sicuramente avrà ricadute positive sugli utilizzatori dei servizi finanziari e del commercio online.

La caduta e la rinascita 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 rilievo 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 il malware scritto da altri gruppi cyber criminali.

Anche in questo caso, i documenti Office (prevalentemente Word) allegati ad e-mail inviate in automatico dalle botnet di Emotet 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. 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, l'hash è stato cambiato in media ogni 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 (denominate Epoch1, Epoch2 e Epoch3) da parte dei tecnici delle forze di polizia coinvolte.Senza dubbio una delle più imponenti operazioni di polizia contro il cybercrime dell'ultimo decennio.
Un'analisi dei conti bancari usati dal gruppo cyber criminale ha mostrato transazioni per circa 10.5 milioni di dollari nei due anni antecedenti l'operazione di polizia. 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 preparati, 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.
Per molti mesi successivi al takedown non si sono notate attività delle botnet di Emotet e si è pensato quindi ad una definitiva battuta d'arresto. Rimaneva tuttavia molto malware ancora in circolazione, TrickBot e QakBot ad esempio, alla ricerca di nuovo serio veicolo di distribuzione. Subito dopo il takedown di Emotet la botnet di Trickbot ha ricominciato la sua attività di espansione.
Negli ultimi mesi del 2021 si è però assistito anche ad una graduale ricostruzione di due nuove botnet Emotet (denominate Epoch4 e Epoch5) in un tentativo di riconquistare una fetta importante del panorama malware mondiale. Fenomeno interessante è che in questa fase è il malware TrickBot che distribuisce sulle macchine infette il malware Emotet, in una sorta di mutuo soccorso tra i due sodalizi criminali.

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 1573 campagne di furto di credenziali per l'accesso a banche e altre istituzioni finanziarie italiane, attive e monitorate nel periodo 1° gennaio – 31 dicembre 2021. Questa analisi non prende in considerazione i domini registrati con nomi verosimili di banche o prodotti finanziari (domain squatting) e mai attivati, presu-

mibilmente bloccati durante l'attivazione oppure abbandonati dagli stessi creatori, oppure ancora pronti per usi futuri.

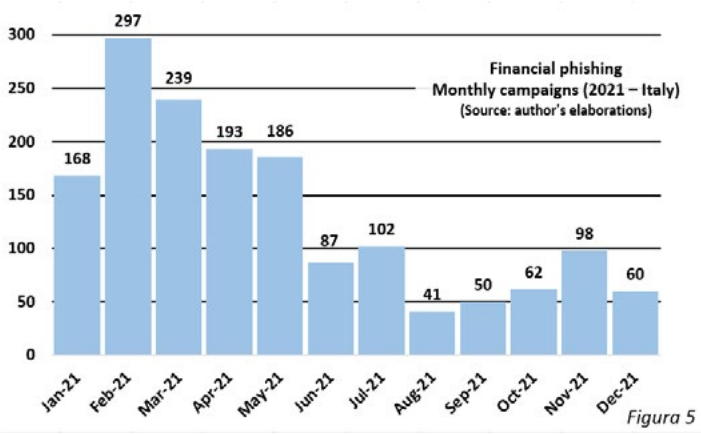


Figura 5

Limitandosi al settore finanziario italiano, in tutto il 2021 è stata osservata una media di 4,3 nuove pagine di phishing al giorno attivate e perfettamente funzionanti, con attività particolarmente intensa nei primi 5 mesi dell'anno (**Figura 5**).
La massima attività si è raggiunta nel mese di febbraio 2021, con una media di 11 nuove pagine attivate al giorno.

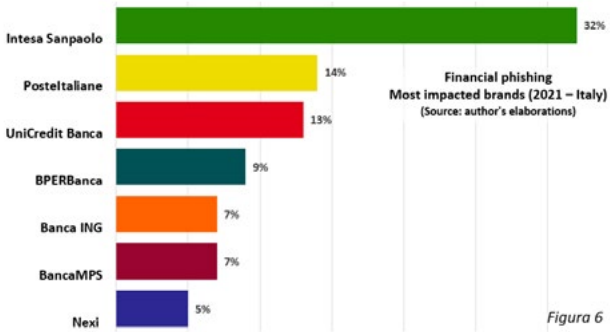


Figura 6

I brand più frequentemente obiettivo di phishing sono stati Intesa Sanpaolo (32% delle campagne di phishing analizzate), Poste Italiane (14% delle campagne), Unicredit (13% delle campagne), BPER (9%), Banca ING e Banca MPS (entrambi al 7%), Nexi (5%) e a seguire altri 23 brand italiani per un totale complessivo del 13% delle campagne di phishing.
In totale nel corso del 2021 il fenomeno del phishing ha colpito 30 istituzioni finanziarie

italiane. La distribuzione delle campagne è evidentemente legata alla dimensione della banca e al numero dei suoi clienti, in un attacco di tipo opportunistico.

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 alcuni mesi.

Nel corso del 2021 il 57% dei siti di phishing verso il settore finanziario italiano è stato ospitato negli Stati Uniti, 10% in Olanda, 6% Germania e 5% in Italia (**Figura 7**).
C'è da notare che il 36%, quindi oltre un terzo, 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 operati dal provider.

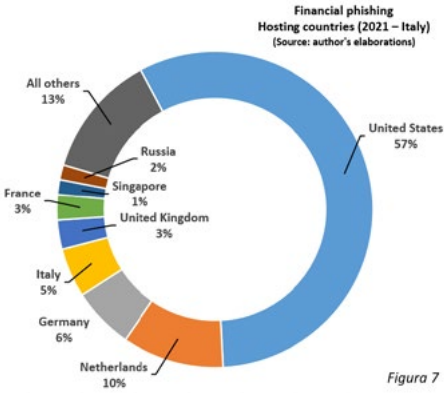


Figura 7

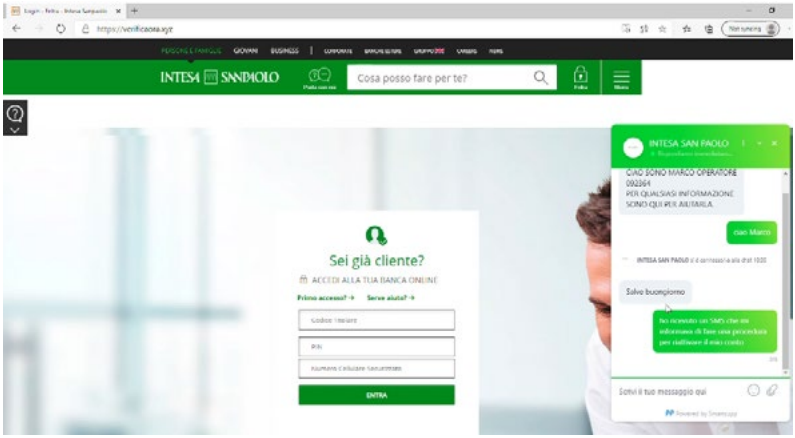
Il dato che più di ogni altro deve farci riflettere è che ormai il 97,5% delle URL di phishing usa il protocollo HTTPs, il cosidetto HTTP "sicuro" che quindi non è più un'indicazione sull'affidabilità o meno del sito.
Tecnologie come HTTPS e l'SSL/TLS sono progettate per proteggere le comunicazioni tra client e server, tuttavia l'icona del lucchetto nella barra indirizzi del browser può creare la falsa illusione che un sito web possa essere considerato attendibile. Questo interferisce molto con il giudizio che i visitatori danno del sito internet, e 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*, parimenti 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 Do-

main 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 sul reale titolare del sito web. Per evitare il phishing, il controllo non dovrebbe essere sull'utilizzo del protocollo HTTPS, ma 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).
Molti 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. Purtroppo, l'indicazione è di difficile comprensione per un utente non attento.

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 registrano e attivano 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.

Già dal 2020 abbiamo osservato campagne che usano 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 su 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.

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 in passato.

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 deliberata 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 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.
Guardando ai data breach, nel 2021 i più frequenti vettori di attacco iniziale sono stati compromissione di credenziali, nel 20% delle violazioni, e phishing con il 17% [16]. Ancora nei data breach il phishing è stato il secondo più costoso vettore d'attacco, con un impatto medio di $4.65M per data breach, superiore ad altri vettori d'attacco come cloud misconfiguration ($3.86M). Combattere il phishing è quindi un imperativo per proteggerci da una vasta gamma di attacchi.

Emulazione dello smartphone e SIM swap

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. Tutti elementi usati per il device fingerprinting spesso usato dai siti bancari per individuare connessioni potenzialmente fraudolente. Infine, il dispositivo emulato viene usato per tentare un attacco all'account della vittima, 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, aggiustando dinamicamente il

tiro in base alle contromisure predisposte dalla banca, e lanciando attacchi automatizzati multipli in contemporanea.
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. [2]
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.
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.

Conclusioni

Il *cloud computing* e l'*intelligenza artificiale* sono due fenomeni inarrestabili che caratterizzano il panorama informatico di questi anni.

Verso il cloud le aziende stanno spostando le applicazioni, i workload e i dati. Il lungo dilemma della scelta tra cloud e on-premises, che ha caratterizzato il dibattito negli anni passati, ha trovato una naturale soluzione nel cloud ibrido (hybrid cloud) attraverso il quale le organizzazioni posso integrare i dati e le applicazioni dei propri data center con dati e applicazioni in cloud privati, oppure nei cloud pubblici dei provider di mercato, senza vincolarsi a nessuno di questi (vendor lock-in) e a nessuna scelta architetturale di lungo termine. Il cloud ibrido lascia la più ampia scelta e flessibilità all'organizzazione in quanto questa può decidere di far risiedere i dati e le applicazioni dove ritiene più appropriato, o dove le è economicamente più conveniente, integrando perfettamente ambienti eterogenei. Una soluzione di sicurezza deve essere in grado di poter gestire tale livello di complessità,

adattandosi alle scelte architetturali dell'organizzazione e gestendo le minacce e i rischi a cui sono costantemente esposte tutte le componenti IT, indipendente da dove queste siano collocate.
Pervasiva anche l'Intelligenza Artificiale, non come soluzione ultima a tutti i problemi, ma con componenti mirate in grado di gestire determinate classi di fenomeni.
Il Machine Learning, ad esempio, può rivelarsi davvero utile per catturare anomalie rispetto al comportamento "caratteristico" di ciascun utente o del traffico di rete, facendosi carico dell'onere di capire cosa è caratteristico utente per utente. Collegarsi da una località geografica insolita, oppure collegarsi a un orario insolito, e sappiamo quando lo smart working abbia rivoluzionato il concetto di orario di lavoro e luogo di lavoro, e lo abbia diversificato persona per persona. Oppure fare sequenze di operazioni insolite. Navigare all'interno di un sito web seguendo pattern anomali. Oppure fare improvvisamente file transfer insoliti o verso reti o servizi considerate a rischio. O accedere ad una quantità insolita di documenti office, come fanno molti ransomware. Ora siamo in grado di seguire questi andamenti utente per utente, proprio perché ciascun utente nell'organizzazione ha un modo di lavorare unico che il Machine Learning è in grado di catturare.
Il tema è quantomai attuale. Il Ponemon Institute, nel *Cost of a Data Breach Report* [16] pone proprio l'intelligenza artificiale, assieme all'automazione nella risposta agli incidenti, tra i fattori che possono maggiormente contribuire alla riduzione del danno, e quindi dei costi associati, nel caso in cui una azienda sia vittima di un data breach.
La *User Behaviour Analytics*, o UBA, sfrutta modelli di Machine Learning che tengono costantemente sotto controllo le attività di autenticazione e accesso di ciascun utente, i download, gli upload, i data transfer, i movimenti laterali e molti altri parametri. I modelli apprendono da soli sulla base dell'attività di ciascun utente. *Più passa il tempo, e più l'algoritmo diventa preciso*. Un comportamento anomalo, sulla base di quanto ciascun utente normalmente fa, ad esempio un file transfer via http in uscita di dimensioni particolarmente grandi o verso destinazioni inusuali, oppure un percorso di navigazione inconsueta all'interno di un'applicazione, viene immediatamente evidenziato come attività anomala e può scatenare azioni automatiche, più o meno importanti, in base alla effettiva rischiosità dell'operazione.
Ci sono poi altre applicazioni dell'Intelligenza Artificiale applicabili alla cyber security. Watson for CyberSecurity è alla base di molte soluzioni di cyber security. Analizza da alcuni anni blog, siti web, discussioni dell'underground, mailing list, report, security advisory, estraendo contenuti rilevanti per la cyber security da un insieme di contenuti non strutturati e scritti in linguaggio naturale, che quindi sarebbero difficilmente fruibili da una soluzione informatica. lo fa combinando la traduzione automatica con il Natural Language Understanding e la Content Analytics per estrarre da informazioni non strutturate e scritte in linguaggio naturale e in molte lingue nazionali diverse, contenuti, pattern, tendenze e indicatori che possono essere riusati da un'applicazione. Dalla enorme mole di informazioni sulla cyber security generate ogni ora, su una moltitudine di canali diversi e in molte lingue diverse, vengono estratte informazioni fruibili da una macchina e che supportano il lavoro

di decisione e azione delle varie figure coinvolte nella cyber security, a tutti i livelli. Inoltre, permettono di individuare automaticamente condizioni sulle quali scatenare azioni di Incident Response automatiche o supportate dall'operatore.

Molto promettenti sono anche i progressi del paradigma Zero Trust.Le organizzazioni lo stanno usando per modernizzare i propri programmi di cyber security e adattarsi al mutato rischio derivato da un modo di lavorare che sta cambiando. Tra i principi fondanti ci sono:

- accessi di tipo "least privilege", con i privilegi minimi per effettuare l'operazione, rilevando e valutando i rischi su dati, identità, endpoint, app e infrastruttura;
- non fidarsi mai, ma verificare sempre con il controllo dell'accesso sensibile al contesto a tutte le app, dati, API, endpoint e risorse cloud ibride;
- assumere che una violazione possa prima o poi realmente accadere. Identificare le minacce e predisporre risposte automatiche (Incident Response) che non solo fermano l'attacco nell'immediato, ma adattano dinamicamente i controlli di accesso.

Questo approccio diventa critico con l'aumentare del numero dei sistemi connessi e con il mutare del modello di computazione, basato su una combinazione fortemente interdipendente di risorse e applicazioni on-premises e in cloud, e con gli endpoint (computer e smartphone dei dipendenti) ormai quasi sempre fuori il tradizionale perimetro aziendale, a causa dello smart working e delle nuove forme di lavoro.

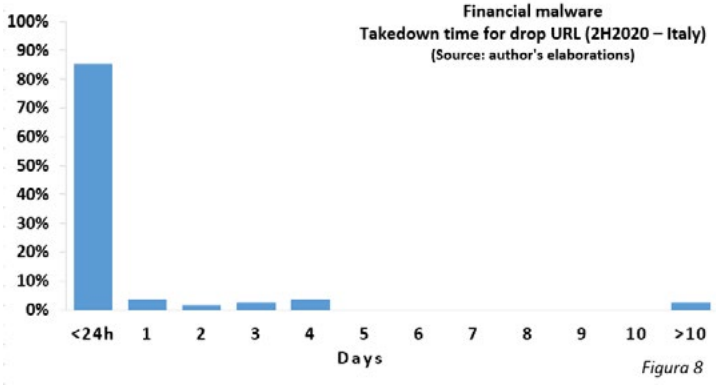


Figura 8

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.

Gli attacchi diventano sempre più veloci, soprattutto a causa dei meccanismi di automazione usati dagli attaccanti.

L'Endpoint Detection and Response, ma soprattutto la sua naturale *evoluzione Extended Detection and Response (XDR)*, integra tutte le componenti della soluzione di sicurezza

in un'unica piattaforma di individuazione (detection) e risposta agli incidenti, portando l'intelligenza di protezione fino al terminale del dipendente, sia esso un computer o uno smartphone. Questo consente di proteggere i dati aziendali, spesso custoditi o acceduti dal terminale del dipendente, anche quando si lavora al di fuori dell'ufficio tradizionale e quindi dalla protezione offerta dalla rete aziendale. Capacità autonome di detection e risposta agli attacchi vengono abilitate già sull'endpoint, e sono sempre attive, anche quando il computer non è disconnesso dal resto dell'infrastruttura IT aziendale.

Bibliografia

[1] *X-Force Threat Intelligence Index 2021* IBM Security, February 2021
[2] *Sicurezza e frodi informatiche in banca – Come prevenire e contrastare attacchi informatici e frodi su Internet e Mobile Banking* CERTFin ABI Lab, luglio 2020
[3] ENISA Threat Landscape 2021 ENISA European Union Agency for Cybersecurity, October 2021
[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] Ponemon Institute,IBM Security*Cost of a Data Breach Report 2021*July 2021
[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 https://ibm.biz/attacchibec
[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 https://ibm.biz/ibmblackfriday
[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
[35] Pier Luigi Rotondo*Soluzioni di sicurezza più efficaci con la threat intelligence di IBM X-Force Exchange* IBM thinkMagazine, aprile 2021 https://ibm.biz/xforcethreatintelligence
[36] S. Weeden*What makes FIDO and WebAuthn phishing resistant?*IBM Security Community, December 2021
[37] I. Chimino*Ursnif Leverages Cerberus to Automate Fraudulent Bank Transfers in Italy*SecurityIntelligence, June 2021
[38] J. Gregory*Cybersecurity Trends: IBM's Predictions for 2022*SecurityIntelligence, January 2022
[39] Pier Luigi Rotondo*Sarà un anno sicuro, a patto che …* IBM thinkMagazine, marzo 2021 https://ibm.biz/2021sicuro

L'evoluzione delle tecniche di ingegneria sociale e il loro utilizzo negli attacchi contro gli utenti di servizi di pagamento online

[A cura di Walter Arrighetti, Francesco De Francesca, Simone Ciccarone e Pasquale Digregorio – CERT Banca d'Italia] [1]

Introduzione e scenario di riferimento

La recente pandemia ha catalizzato il già rapido processo di trasformazione digitale che da tempo coinvolge tanto la sfera privata quanto quella lavorativa dei cittadini dei principali Paesi industrializzati. Se da un lato la digitalizzazione ha rappresentato una enorme opportunità di sviluppo, in alcuni casi la rapidità di questo fenomeno ha reso evidenti nuove vulnerabilità di tipo tecnologico, procedurale, psicologico e sociale.

Lo scenario della minaccia cyber è evoluto conseguentemente: i *threat actor* hanno colto le nuove opportunità affinando le tecniche, tattiche e procedure d'attacco (TTP), rendendole più efficaci per il perseguimento dei propri interessi.

In questo frangente si osserva, in particolare contro il settore finanziario, un'ampia diffusione di tecniche avanzate di ingegneria sociale (dall'inglese *social engineering*), in sinergia con l'uso malevolo di piattaforme e artefatti digitali.

La diffusione di un'adeguata consapevolezza sull'evoluzione di questa minaccia a livello individuale, professionale e collettivo rappresenta il principale fattore di contrasto. A tal fine è fondamentale sviluppare un'adeguata conoscenza (*situational awareness*) della minaccia cyber, attraverso attività continuative di *cyber threat intelligence* (CTI) e *information sharing*, e la conduzione di campagne di *security awareness*, finalizzate a trasformare l'elemento umano da vulnerabilità a sensore in grado di rilevare la componente degli attacchi cyber non individuabili attraverso i presidi di sicurezza tecnologici.

Le fasi di un attacco di ingegneria sociale

L'ingegneria sociale è l'arte di manipolare psicologicamente le persone, allo scopo di indurle a commettere – o non commettere – azioni funzionali ad un piano criminale, come ad esempio rivelare informazioni confidenziali o eseguire operazioni per conto dell'attaccante. Nel contesto della *cybersecurity*, l'ingegneria sociale è un attacco in cui i *threat actor*, mediante l'interazione sociale con le vittime, sfruttano le vulnerabilità del "fattore umano" per violare sistemi informatici[2]. In questo scenario sono particolarmente efficaci le tecniche di ingegneria sociale che utilizzando mezzi di comunicazione digitale quali email (c.d. *phishing*), telefonate (c.d. *vishing*), SMS (c.d. *smishing*) o QR-code malevoli (c.d. *qrishing*)[3].

---

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

[2] Wang Z., Sun L., Zhu H., 'Defining social engineering in Cybersecurity', in IEEE Access, Vol. 8, pp.85094–85115, 2020, doi: 1109/ACCESS.2020.29928072807.

[3] Phishing, vishing, smishing e qrishing si riferiscono ai diversi canali di comunicazioni digitali utilizzati per la conduzione di attacchi

I criminali possono prendere di mira specifici individui o categorie ristrette di persone (in quel caso si parla di *spear-phishing*, intesa come variante mirata del *phishing*), come i dipendenti di una organizzazione, o di una sua unità costitutiva. I criminali talvolta si spacciano per un interlocutore che possa avere un ascendente sulla vittima, come ad esempio un superiore della propria organizzazione (la cosiddetta "*CEO Fraud*") o un operatore del supporto tecnico di servizi informatici[4]. Nell'ultimo biennio sono inoltre aumentate le truffe di ingegneria sociale a tema pandemico, che sfruttano la paura del contagio[5], per indurre il cittadino a compiere azioni che inconsapevolmente favoriscono l'attaccante, invogliandolo ad esempio a installare app di *contact tracing* (spesso varianti malevole di app realmente esistenti), o a collegarsi ad un sito di *phishing*. In alcuni casi l'utente viene ingannato con messaggi che gli comunicano un possibile contagio, creando così un pretesto ancora più forte.

Di seguito si propone un modello strutturato che permette di descrivere lo sviluppo di un attacco di ingegneria sociale attraverso un ciclo composto da diverse fasi che si susseguono iterativamente fino al raggiungimento degli obiettivi dell'attaccante o al mutamento del piano criminale in seguito a nuovi elementi scaturenti dall'interazione con la persona colpita (cfr. **Figura 1**).

di ingegneria sociale; in ciascuno di questi l'attaccante utilizza rispettivamente l'email, il telefono, gli SMS, o il QR code come vettore d'attacco per far "abboccare" la vittima del piano criminale. Infatti il termine phishing deriva dal verbo inglese fishing (letteralmente "pescare).

[4] FBI Internet Crime Compliance Center (IC3), Internet Crime Report 2020.

[5] https://www.us-cert.gov/ncas/current-activity/2020/03/06/defending-against-covid-19-cyber-scams.

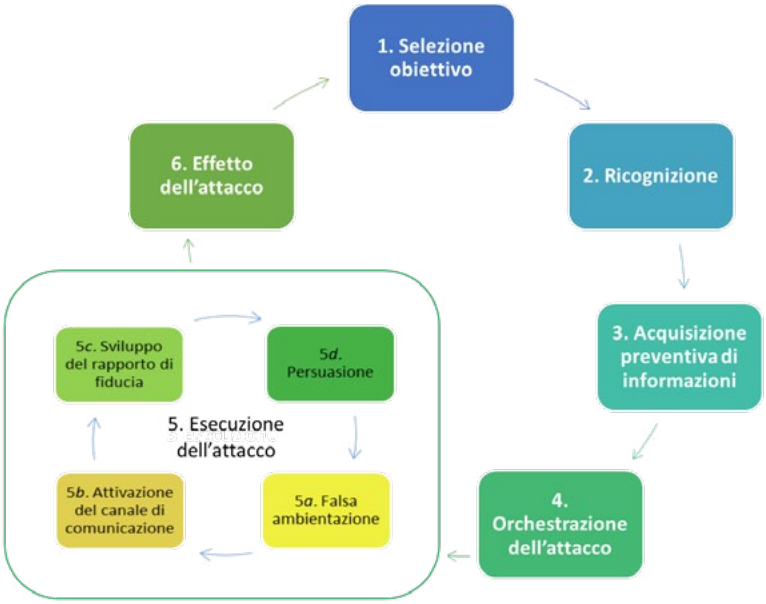


Figura 1 - *Il ciclo di vita di un attacco di ingegneria sociale.*

1. **Selezione obiettivo**
   Processo di selezione degli obiettivi rilevanti per il perseguimento degli scopi dell'attaccante, che consiste nell'individuare i soggetti la cui manipolazione permette di attuare il piano criminale.

2. **Ricognizione**
   Attività posta in essere dall'attaccante per individuare le modalità da poter utilizzare per acquisire le informazioni necessarie a organizzare e condurre l'attacco, come ad esempio individuando gli aspetti rilevanti del *digital footprint*[6] della persona da colpire.

3. **Acquisizione preventiva di informazioni**
   In base agli elementi raccolti durante la ricognizione, si acquisiscono le informazioni rilevanti sulla persona da colpire, funzionali a definire le modalità per contattarla e le leve psicologiche da utilizzare, senza tuttavia entrare in contatto diretto con quest'ultima.

[6] Il *digital footprint* (impronta digitale) si riferisce all'insieme dei dati, delle informazioni e delle attività tracciabili in internet o attraverso servizi digitali. In particolare sempre più informazioni vengono inconsapevolmente diffuse dagli utilizzatori di tali servizi e possono essere sfruttate contro di loro.

4. **Orchestrazione dell'attacco**
   Le informazioni raccolte sono elaborate e valorizzate per la definizione di un piano offensivo che massimizzi le probabilità di riuscita al minor costo e minor rischio per l'attaccante. In particolare si scelgono gli strumenti, i vettori d'attacco, i canali di comunicazioni e le prove verosimili a sostegno delle tesi utilizzate dall'attaccante per ingannare la persona colpita.

5. **Esecuzione dell'attacco**
   Questa fase prevede un'ulteriore attività ciclica che parte con l'applicazione del piano d'attacco precedentemente definito e che può proseguire in modo iterativo in base a come le azioni ingannevoli evolvono in relazione alle interazioni con la vittima. In particolare l'attaccante nella fase 5*a* predispone gli elementi funzionali alla falsa ambientazione da sfruttare per ingannare la persona oggetto dell'attacco, come ad esempio finti portali web e identità virtuali[7] fasulle o rubate.
   Successivamente nella fase 5*b* si stabilisce il contatto con la persona oggetto dell'attacco e, nella fase 5c, si sfrutta la finta ambientazione per instaurare un rapporto di fiducia con la vittima.
   La fase 5*d* prevede che la persona oggetto dell'attacco fornisca le informazioni richieste o ponga in essere le azioni desiderate dall'attaccante, che a tal fine può utilizzare diverse tecniche di comunicazione efficace e manipolazione psicologica con finalità persuasive. Ciò si realizza anche facendo leva su caratteristiche socialmente rilevanti della personalità umana e spesso presenti naturalmente nella psiche degli individui, quali: gratitudine, ansia e paura, frustrazione, vendetta, odio, vergogna e senso di colpa o inadeguatezza, pulsioni della sfera sentimentale e sessuale, compassione, subordinamento (nella sfera lavorativa, sociale, religiosa, familiare).

6. **Effetto dell'attacco**
   In questa fase si valuta se l'attacco è andato a buon fine e se è stato ottenuto quanto previsto. In tal caso l'attaccante terminerà le sue azioni, cercando di destare il minor sospetto nella vittima e/o rimuovendo eventuali tracce. Nel caso in cui gli effetti non fossero quelli sperati o emergessero nuove opportunità per far evolvere l'attacco, il ciclo procede iterativamente.

[7] Indirizzi email, *nickname*, numeri di telefono, *account* sui *social network* e i loro fattori di autenticazione.

Attacchi rivolti contro utenti di servizi di pagamento online attraverso tecniche miste di ingegneria sociale

Il settore finanziario, in particolare gli operatori di servizi di pagamento online, è particolarmente esposto alla minaccia cyber poiché permette la monetizzazione diretta delle azioni fraudolente. In questo scenario, reso ancora più profittevole dagli impatti legati alla digitalizzazione e dagli effetti della pandemia, i cyber criminali hanno affinato le loro tecniche per renderle ancora più efficaci, anche attraverso l'utilizzo di tecniche miste di ingegneria sociale. Lo schema d'attacco prevede che i truffatori stabiliscano un rapporto di fiducia con clienti o operatori di servizi di pagamento e li manipolino psicologicamente per acquisire le informazioni e i mezzi necessari a realizzare le truffe, nell'intento di sottrarre illecitamente alcune somme di denaro.

In particolare è possibile individuare due distinti scenari che prevedono l'utilizzo di tecniche evolute di ingegneria sociale per attuare il piano criminale ai danni di utenti di servizi di pagamento online. Per ogni scenario vengono descritte le fasi dell'attacco e le principali tattiche e tecniche adottate, illustrate utilizzando il *framework* MITRE ATT&CK[8] per i domini tecnologici *Enterprise* e *Mobile*.
I due scenari individuati si contraddistinguono per specifiche modalità di orchestrazione ed esecuzione dell'attacco. Per questo motivo si descrivono di seguito le fasi di selezione obiettivo, ricognizione e acquisizione preventiva di informazioni (prime tre fasi del ciclo rappresentato in Figura 1), comuni ai due scenari, e si rimanda invece ai paragrafi seguenti per gli aspetti peculiari di ciascuno scenario.
Individuata la persona da colpire, gli attaccanti effettuano una ricognizione per acquisire le informazioni necessarie a organizzare e condurre l'attacco. In particolare, anche esplorando il *footprint* digitale, si acquisiscono tutte le informazioni rilevanti sulla persona da colpire, funzionali a individuare la modalità per contattarla e le leve psicologiche da utilizzare.

Tra le principali discipline utilizzabili in questa fase ci sono l'OSInt, WebInt, SocMInt. Sono spesso utilizzate le informazioni presenti in *data breach* precedenti e potenzialmente relativi alle email in uso alla persona da colpire. In questo caso gli attaccanti, avendo accesso alla casella email della vittima, possono sfruttare a proprio vantaggio le informazioni ivi presenti, come ad esempio le email inviate alla vittima dall'operatore di servizi finanziari online. La **Figura 2** illustra le TTP adottate dagli attaccanti nelle fasi preliminari di selezione obiettivo, ricognizione e acquisizione preventiva di informazioni.

[8] MITRE ATT&CK (*Adversarial Tactics, Techniques, and Common Knowledge*) è un *framework* per la condivisione di una base di conoscenza di TTP usate dai threat actor per eseguire attacchi cyber. Il *framework* prevede la possibilità di specializzare alcune tecniche in sub-tecniche. Alcune tecniche di ingegneria sociale, quali *smishing, vishing*, non sono al momento rappresentate nell'ultima versione del *framework* (v. 10). La selezione delle TTP è stata elaborata mediante lo strumento *ATT&CK Navigator* (https://mitre-attack.github.io/attack-navigator).

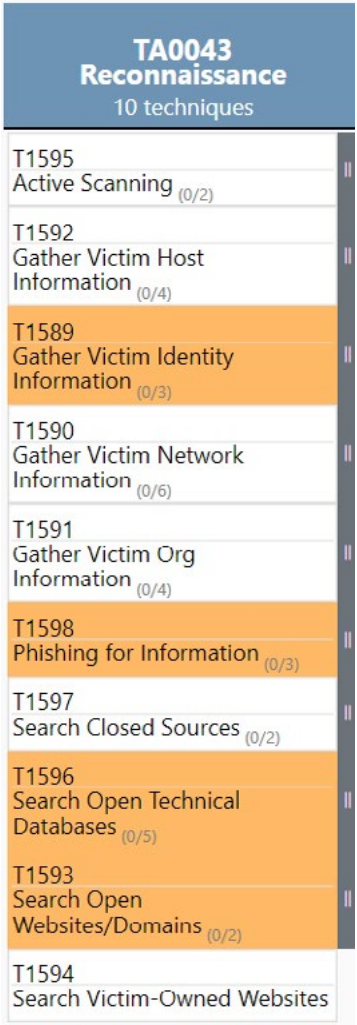


Figura 2 - *TTP adottate dagli attaccanti nelle fasi di selezione obiettivo, ricognizione e acquisizione preventiva di informazioni. TTP selezionate dal framework MITRE ATT&CK sul dominio Enterprise.*

Si descrivono di seguito per ciascuno scenario la modalità di esecuzione dell'attacco (*fase 5 del ciclo rappresentato in Figura 1*).

Scenario 1

In questo scenario un utente di servizi finanziari online subisce un attacco realizzato con tecniche di ingegneria sociale che ha la finalità di convincerlo a comunicare le informazioni necessarie per consentire all'attaccante di effettuare transazioni finanziarie in proprio favore.

Per la creazione della falsa ambientazione funzionale all'attacco di ingegneria sociale (*fase 5a di Figura 1*), l'attaccante predispone e registra siti web di *phishing* che emulano nell'aspetto le pagine di autenticazione del portale di *internet banking* utilizzato dalla vittima. Il cyber criminale per la registrazione del portale *fake* utilizza un nome simile a quello del portale reale, impiegando tecniche di *typosquatting*.

In questa fase l'attaccante acquisisce o sviluppa tutti gli altri strumenti necessari a perpetrare l'attacco: dai *phishing kit*, alle piattaforme per lo *spoofing* dei numeri di telefono.

Le fasi successive dell'attacco sono riportate in **Figura 3** e di seguito descritte.

L'attaccante, fingendo di essere un operatore dell'istituto finanziario, contatta telefonicamente (*vishing*) la vittima convincendola a collegarsi al sito web di *phishing* che emula la pagina di accesso al portale di *internet banking*. Il truffatore in alcuni casi si avvale di tecniche di *spoofing* del numero di telefono[9] chiamante per far credere alla vittima che la chiamata provenga dal *contact center* dell'istituto finanziario o da servizi di emergenza (*fasi 5b e 5c di Figura 1*).

[9] La tecnica dello *spoofing* del numero di telefono chiamante non è rappresentata nell'ultima versione del *framework* MITRE ATT&CK sul dominio *Mobile* (v. 10).

La vittima inserisce sul sito web di *phishing* le proprie credenziali di accesso al sito dell'istituto finanziario rivelandole così al truffatore. L'attaccante utilizza le credenziali impropriamente acquisite dalla vittima per accedere al portale e inserire le transazioni finanziarie in proprio favore. L'attaccante induce infine la vittima a fornirgli i codici dispositivi (es. *One Time Password*) necessari ad autorizzare le transazioni finanziarie illegittime. In alcuni casi l'attaccante adotta anche la tecnica nota come *SIM Card Swap*[10] per acquisire il pieno controllo del numero di telefono della vittima e ricevere così SMS o chiamate necessarie ad autorizzare le transazioni finanziarie (*fase 5d di Figura 1*).

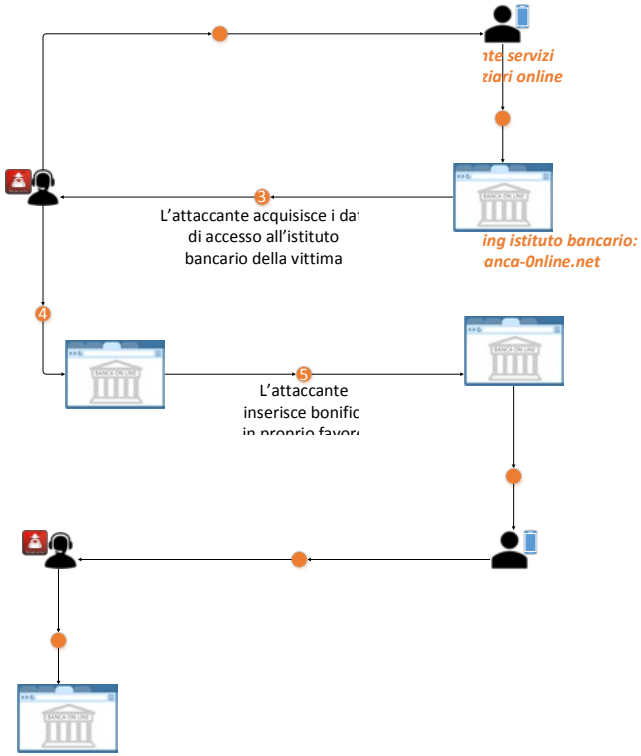


Figura 3 - *L'ingegneria sociale è adottato dall'attaccante lungo tutta la catena d'attacco.*

[10] Il *SIM Card Swap* è una tecnica di attacco che consente di acquisire il controllo della numerazione *mobile* associata a un utente, allo scopo di violare servizi *online* che usano il numero di telefono come sistema di autenticazione (es: reset password, OTP inviata via SMS in qualità di secondo fattore di autenticazione, *secure call*, etc.). I truffatori convincono il gestore di telefonia mobile a spostare il numero di telefono della vittima su una nuova scheda SIM controllata dal *cybercriminale*. I truffatori intercettano così le telefonate e gli sms inviati dalla banca della vittima e li utilizzano per operare sul suo conto bancario.

In **Figura 4** sono presentate le tattiche e le tecniche adottate dagli attaccanti, riprese dal *framework* MITRE ATT&CK.

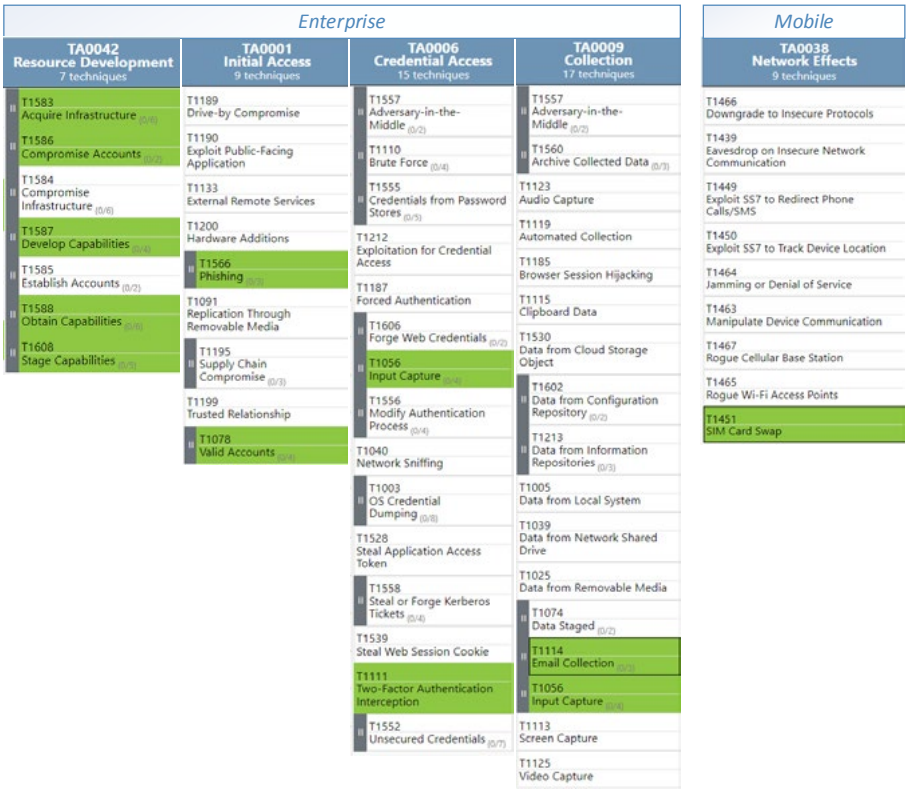


Figura 4 - *Principali TTP adottate negli attacchi di ingegneria sociale agli utenti di servizi finanziari online. TTP selezionate dal framework MITRE ATT&CK sui domini Enterprise e Mobile.*

Scenario 2

Questo scenario riguarda, come il precedente, un attacco contro utenti di servizi finanziari online e si contraddistingue rispetto al precedente per l'utilizzo combinato di tecniche di ingegneria sociale e attacchi cyber.

In aggiunta a quanto descritto nella fase di creazione della falsa ambientazione (*fase 5a di Figura 1*) dello scenario 1, l'attaccante predispone un'app malevola[11] verosimile per la vittima.

[11] Il download dell'app malevola può avvenire da *store* ufficiali, *store fake* o tramite link a siti web.

L'attaccante invia un link al sito di *phishing* che emula quello dell'istituto finanziario attraverso una email o un SMS (*smishing*) affinché la vittima inserisca inconsapevolmente le proprie credenziali (**Figura 5**).

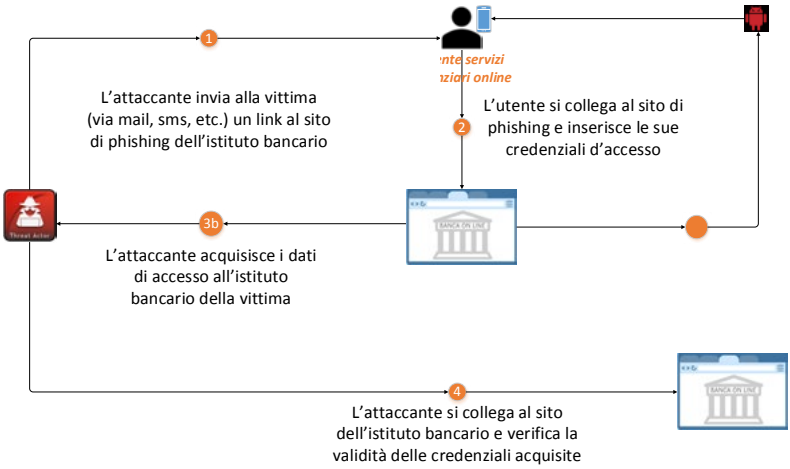


Figura 5 - *L'ingegneria sociale utilizzata nell'adescamento dell'utente e per l'installazione del malware.*

L'attaccante contatta telefonicamente (*vishing*) la vittima e la convince con l'inganno a installare sul proprio dispositivo mobile l'app malevola precedentemente predisposta. In alcuni casi il pretesto è quello di aggiornare l'applicazione reale utilizzata dall'utente per accedere al proprio servizio di *home banking* o di installare un'app di sicurezza per proteggere il dispositivo della vittima. L'app è in realtà un *dropper* che scarica e installa un *malware* di tipo RAT (*Remote Access Trojan*) sullo *smartphone* che consente all'attaccante di prenderne il controllo. Per ingannare ulteriormente la vittima, il contatto telefonico può avvenire dal numero telefonico del *contact center* dell'istituto finanziario o da numerazione di emergenza (*spoofing* del numero di telefono).
L'attaccante acquisisce così il pieno controllo del dispositivo, potendone eseguire la registrazione dello schermo e intercettare SMS o notifiche necessari per eseguire l'accesso al portale di *mobile* o *internet banking* del servizio finanziario online e autorizzare le transazioni finanziarie. Il *cyber criminale* infine cancella la *app* dal dispositivo o esegue il reset dello *smartphone* alle impostazioni di fabbrica, al fine di rimuovere ogni traccia.
La **Figura 6** rappresenta graficamente gli *step* adottati per l'attuazione dell'attacco combinato.

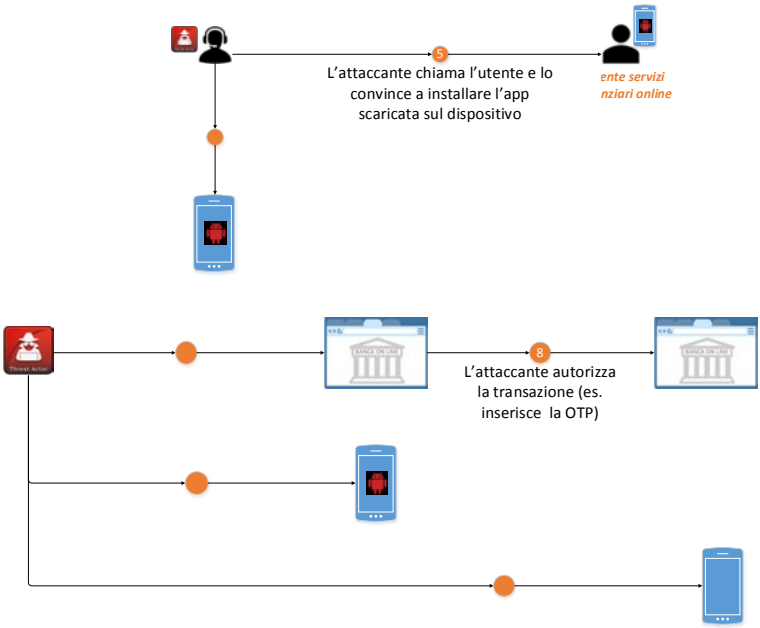


Figura 6 - *Malware (RAT) utilizzato per finalizzare la frode informatica e autorizzare le transazioni finanziarie indebite.*

In **Figura 7** e in **Figura 8** sono presentate le tattiche e le tecniche adottate dagli attaccanti, riprese dal framework MITRE ATT&CK.

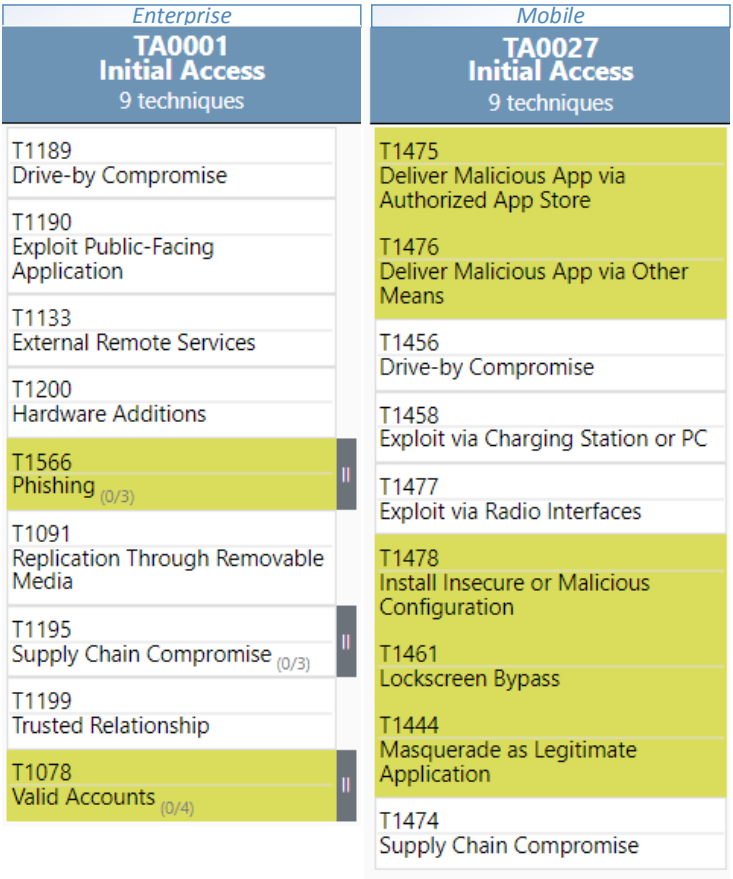


Figura 7 - *Principali TTP dell'attacco agli utenti di servizi finanziari online, eseguito con tecniche di ingegneria sociale combinate a malware. TTP selezionate dal framework MITRE ATT&CK sui domini Enterprise e Mobile.*

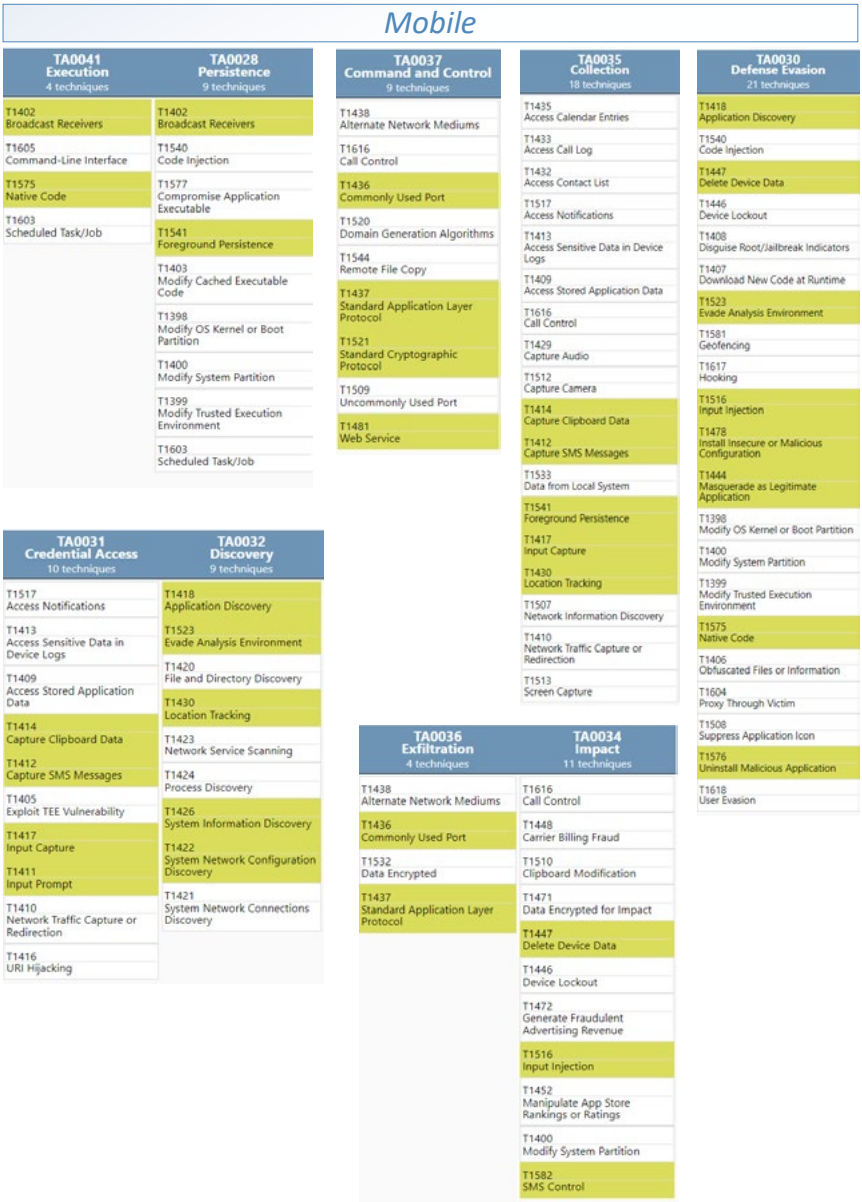


Figura 8 - *Principali TTP di uno degli attacchi malware effettuati sugli smartphone degli utenti di servizi finanziari online. Le TTP sono selezionate dal framework MITRE ATT&CK sul dominio Mobile.*

La *security awareness* come misura preventiva contro attacchi che impiegano tecniche di ingegneria sociale

La difesa più efficace contro gli attacchi cyber basati sull'ingegneria sociale consiste nel sensibilizzare e rendere consapevoli delle minacce – da cui il termine *security awareness* – i potenziali destinatari di tali attacchi. Essa è tanto più efficace quanto più è:[12]

- frequente e continua;
- interattiva per coinvolgere i destinatari in un percorso di auto-apprendimento;
- mirata ai casi specifici di truffe e rispetto a bacini di utenti esposti a specifiche vulnerabilità;
- costruita a partire dalla conoscenza elaborata delle TTP usate dagli attaccanti.

I tentativi di formazione tradizionale si rivelano spesso inefficaci, proprio perché effettuati sporadicamente e con scarse opportunità di coinvolgimento diretto degli interessati[13]. La *security awareness* indirizzata dai processi di CTI, in particolare, riesce ad essere più efficace proprio perché calata nel contesto evolutivo delle minacce specifiche del settore di riferimento.
Un aspetto fondamentale della *security awareness* è la capacità di abilitare il meccanismo "*human as a security sensor*", in cui è l'utente consapevole a individuare tentativi di truffe basate sull'ingegneria sociale, che avrebbero altrimenti una possibilità scarsa, se non nulla, di essere intercettate con contromisure tecniche di sicurezza.
Le organizzazioni del settore bancario e finanziario sono da sempre molto sensibili alle tematiche della *cybersecurity*. Di recente il CERTFin[14], con la partecipazione di Banca d'Italia, IVASS, ABI e insieme ad altri 13 banche e gruppi assicurativi[15], ha organizzato una campagna informativa, dedicata al pubblico degli utenti dei servizi bancari e finanziari nazionali. Successivamente l'iniziativa è stata riproposta anche con una veste istituzionale grazie al patrocinio della Presidenza del Consiglio dei Ministri e dell'Agenzia per la Cybersicurezza Nazionale.

---

[12] Si veda: Heartfield R., Loukas G., Gan D., 'You are probably not the weakest link: towards practical prediction of susceptibility to semantic social engineering attacks,' in *IEEE Access*, Vol. 4, pp.6910–6928, 2016, doi: 10.1109/ACCESS.2016.2616285. Si veda anche: Aldawood H., Skinner G., 'Analysis and finding of social engineering industry experts explorative interviews: perspectives on measures, tools, and solutions,' in *IEEE Access*, Vol. 8, pp.67321–67329, 2020, doi: 10.1109/ACCESS.2020.29832180.

[13] Secondo lo standard SP 800-50 del NIST la *security awarenss* non è formazione, in quanto spinge l'utente a riconoscere i problemi di sicurezza ed agire di conseguenza. Secondo ENISA (*The new users' guide: how to raise information security awarness*) essa è, tra le altre cose, la componente "cosa" della strategia di educazione di un'organizzazione, che punta a cambiare gli schemi comportamentali nell'uso delle tecnologie e di internet.

[14] Il CERTFin, il CERT del settore finanziario italiano, è un'iniziativa cooperativa pubblico-privata finalizzata a innalzare la capacità di gestione dei rischi *cyber* degli operatori del settore bancario/finanziario e la *cyber resilience* del sistema finanziario italiano.

[15] BPER Banca, CREDEM, La Cassa di Ravenna, Generali Italia, Gruppo Cassa Centrale, ICCREA Banca, ING, Intesa Sanpaolo, Banca Mediolanum, Banca popolare del Lazio, Banca Sella, UniCredit.

La campagna, denominata "*I Navigati, informati e sicuri*", nasce con l'obiettivo di sensibilizzare l'opinione pubblica sui temi della sicurezza cibernetica e delle frodi, divenuti ancor più rilevanti in seguito alla recente pandemia che ha amplificato il ricorso a strumenti digitali per eseguire acquisti e operazioni bancarie e che ha generato nuove opportunità per i criminali rendendo più efficaci le tecniche di ingegneria sociale utilizzate per la conduzione di truffe online.
La campagna ha come protagonisti i membri della famiglia Navigati che, consapevoli dei comportamenti virtuosi da adottare nel spazio cibernetico, si cimentano nelle attività giornaliere dimostrando di saper gestire adeguatamente le insidie connesse con l'utilizzo di strumenti digitali.
Si tratta della prima iniziativa di *security awareness* a livello nazionale, realizzata usando uno stile attuale e il linguaggio dei cosiddetti *commercials*[16], con un'ampia diffusione pubblica. La campagna è andata in onda, a partire da novembre 2021, sulle principali emittenti radiotelevisive, testate giornalistiche (quotidiane e periodiche), sui principali *social media* e sul sito dedicato[17] dove è presente una web-serie composta da 8 episodi[18]. Alcuni dei partecipanti all'iniziativa, stanno rilanciando l'intera campagna a beneficio della propria clientela. Inoltre gli esperti di alcune organizzazioni aderenti all'iniziativa hanno realizzato delle video pillole su alcune tematiche di particolare interesse[19].

Conclusioni

La pandemia ha ulteriormente rafforzato la centralità della digitalizzazione nella vita di istituzioni, organizzazioni e cittadini, imponendo l'intermediazione della maggior parte delle interazioni sociali attraverso mezzi di comunicazione digitale. In questo scenario i cyber criminali hanno affinato le proprie tecniche d'attacco per persuadere le vittime a porre in essere i comportamenti funzionali al piano criminale, sfruttando le opportunità offerte dai canali di comunicazione digitale e le vulnerabilità psicologiche esaltate dal contesto pandemico.
Un ulteriore fattore amplificare della pericolosità di questo scenario è rappresentato dall'utilizzo combinato di tecniche di ingegneria sociale e attacchi cyber in grado di sfruttare sinergicamente vulnerabilità umane e tecnologiche.
I cittadini, utenti di servizi di pagamento online, sono particolarmente esposti a questa minaccia perché rappresentano un mezzo facilmente accessibile che permette agli attaccanti la monetizzazione diretta delle azioni fraudolente.

---

[16] Cioè la pubblicità commerciale condotta attraverso canali video (televisione, internet, social network, cinema).

[17] https://www.inavigati.it

[18] ciascuno dedicato ad un particolare tema: smishing, social network, ingegneria sociale, *sim swap*, acquisti online, *money muling*, download pericolosi, *ghost broking*.

[19] In particolare la Banca d'Italia ha realizzato un approfondimento sull'ingegneria sociale, disponibile al seguente indirizzo: https://inavigati.certfin.it/#section-gli-esperti.

La diffusione di un'adeguata consapevolezza sull'evoluzione di questa minaccia a livello individuale, professionale e collettivo rappresenta il principale fattore di contrasto. A tal fine è fondamentale seguire l'evoluzione della minaccia cyber (*situational awareness*) per sviluppare e condurre campagne di *security awareness* efficaci. Ciò permette di sensibilizzare le persone sui profili evolutivi dello scenario della minaccia cyber per stimolare l'adozione di comportamenti virtuosi, al fine di prevenirne gli impatti.
A tal proposito è determinante la collaborazione tra le organizzazioni private e le istituzioni, che sono costantemente impegnante per garantire la sicurezza dell'ecosistema digitale e per proteggere dipendenti e cittadini.

2022 Sysadmin Report
Quando il gioco si fa duro, i duri iniziano a giocare

[A cura di Netwrix]

Il 2021 è stato un anno caratterizzato da diversi avvenimenti importanti che hanno portato il mondo della sicurezza informatica a doversi adattare a questi nuovi scenari. Gli amministratori di sistema, in particolare, sono stati quelli la cui realtà ne è stata maggiormente influenzata. Per celebrare la giornata a loro dedicata, il Sysadmin Day 2021, abbiamo intervistato 732 amministratori di sistema di diverse aziende e di tutto il mondo, per capire appunto in che modo questo anno eccezionalmente particolare ne abbia influenzato il loro lavoro. Questo Report è il frutto di tale ricerca e descrive in dettaglio ciò che abbiamo scoperto e celebra il potere e la resilienza degli amministratori di sistema, che rappresentano il cuore stesso della forza dell'IT!

I risultati significativi includono:

- **Aumento del rischio associato agli attacchi alla sicurezza informatica nonché l'aumento del carico di lavoro** sono le principali sfide che gli amministratori di sistema devono affrontare a causa del lavoro in remoto; entrambi sono stati nominati **da oltre il 60%** degli intervistati.
- Il **59%** dichiara che **la quantità di tempo che dedica al lavoro è aumentata rispetto allo scorso anno** e il 62% lavora più di 40 ore a settimana.
- Il **29%** afferma di essere **più concentrato sulla sicurezza informatica rispetto a quanto lo fosse prima della pandemia**.
- Il **40%** degli amministratori di sistema dichiara di essere preoccupato per la rapida evoluzione delle minacce informatiche ed ammette che **il lavoro a distanza ha distolto l'attenzione dalle attività di sicurezza**.
- Il 51% afferma che **lo stipendio medio** per gli amministratori di sistema in Italia e nel Regno Unito è inferiore al previsto.
- Il 73% afferma che la propria vita sarebbe più semplice se gli utenti smettessero di **cliccare su collegamenti** o allegati sospetti ed il 42% dichiara inoltre che sarebbe per loro un sogno se gli utenti smettessero **scrivere le proprie password su post-it** attaccati ai loro computer.
- Il 37% degli amministratori IT afferma **il miglior regalo di sempre** sarebbe del tempo da trascorrere con la propria famiglia, mentre il 14% insiste sul fatto che il regalo ideale sarebbe una vacanza senza internet, dove nessuno possa raggiungerli.

Tempi duri, tempi domestici: gli effetti del lavoro da remoto sugli amministratori di sistema

Le principali sfide del lavoro a distanza

Quando abbiamo chiesto agli amministratori di sistema di elencare le tre principali sfide che hanno dovuto affrontare a causa del passaggio del lavoro da remoto, si sono concentrati principalmente sull'aumento del rischio di attacchi alla sicurezza informatica (68%) e sull'aumento del carico di lavoro (66%). Un altro punto della lista, anche se distante dalla vetta, è stato la mancanza di strumenti per supportare il lavoro a distanza (38%).

Le principali sfide che gli amministratori di sistema hanno dovuto affrontare a causa del lavoro da remoto

Aumento del rischio di attacchi cyber	68%
Aumento del carico di lavoro	66%
Mancanza di strumenti adeguati per supportare il lavoro a distanza	38%
Riduzione del budget	33%
Riduzione del personale IT	30%
Mancanza di competenze informatiche per supportare il lavoro a distanza	22%
Altro	5%

Le sfide principali, infatti, sono state sostanzialmente le stesse, indipendentemente dalla dimensione dell'azienda. Tuttavia, l'85% degli amministratori di sistema di aziende di grandi dimensioni, che al proprio interno conta almeno cinque amministratori di sistema, ha scelto come sfida principale l'aumento del carico di lavoro e non la sicurezza; sorprendentemente è stato l'unico gruppo intervistato a fare tale scelta. Molto probabilmente, questa differenza è dovuta al fatto che la maggior parte degli amministratori di sistema intervistati lavora in aziende di medie dimensioni (101–1.000 dipendenti) e large (1.001–5.000): più sono i dipendenti che lavorano da remoto e più difficile diventa poterli supportare tutti.

Il 42% degli amministratori di sistema nel settore dell'istruzione ha subito tagli al budget a causa della pandemia, rappresentando così il numero più alto tra gli oltre 25 settori intervistati.

Si lavora sempre di più

Un'altra sfida per gli amministratori di sistema, scatenata dall'improvviso e repentino passaggio del lavoro da remoto, è stata quella relativa al tempo dedicato al lavoro: il 59%, infatti, ha confermato un aumento di quest'ultimo ed il 62%, invece, ha dichiarato di lavorare più di 40 ore a settimana.

Ore settimanali lavorate dagli amministratori di sistema

40 o meno	38%
41–50 ore	40%
51–60 ore	14%
Più di 61 ore	5%
Lavoro 24 ore su 24, 7 giorni su 7, senza dormire	3%

I settori finanziario, retail e sanitario sono quelli che hanno riportato una maggiore pressione: il 79% degli amministratori di sistema di questi settori, infatti, dichiara di lavorare più di 40 ore a settimana. Inoltre, il 94% degli amministratori di sistema nel settore della vendita al dettaglio afferma che il proprio orario di lavoro è aumentato dall'inizio della pandemia.

Implicazioni sulla sicurezza del lavoro da casa

Volevamo capire se il passaggio al lavoro da casa avesse in qualche modo distolto l'attenzione degli amministratori di sistema dalla sicurezza informatica verso attività più operative e di supporto, come la risoluzione dei problemi di connessione per gli utenti. Gli amministratori di sistema intervistati si sono suddivisi in tre gruppi abbastanza uniformi: il 38% ha ammesso che la sicurezza è diventata meno prioritaria ora, il 29%, invece, ha affermato di essere più concentrato sulla sicurezza informatica rispetto a quanto lo fosse prima della pandemia ed, infine, il 33% ha affermato che il rapporto tra operativo e sicurezza non sono cambiati rispetto all'era pre-pandemia.

Il 72% degli amministratori di sistema che lavora nel settore della vendita al dettaglio è meno concentrato sulla sicurezza informatica rispetto a quanto lo fosse prima della pandemia - è il numero più alto rispetto agli oltre 25 settori intervistati.

Solo il 17% degli intervistati ha ammesso che la propria azienda non sta affrontando i problemi relativi alla sicurezza causati dal passaggio al lavoro a distanza. Per gli altri, invece, la principale preoccupazione sono le minacce alla sicurezza informatica che sono in rapida evoluzione e che spesso prendono di mira i dipendenti che lavorano da remoto (66%), seguito dalla mancanza di personale (42%), competenze IT (39%) e budget (36%). Inoltre, un altro punto degno di nota è il fatto che il 40% degli intervistati ha ammesso di essere preoccupato per l'aumento delle minacce informatiche in continua evoluzione e soprattutto il lavoro a distanza ha distolto la loro attenzione dalle attività di sicurezza.

Le principali sfide rappresentate per le aziende nel definire la propria strategia sulla sicurezza informatica per i lavoratori remoti, secondo gli amministratori di Sistema

La continua evoluzione delle minacce alla sicurezza	66%
Il nostro team IT non dispone di personale sufficiente	42%
Il nostro team IT non dispone delle competenze necessarie in materia di sicurezza	39%
Non riusciamo ad ottenere abbastanza budget per gli strumenti necessari	36%
Non stiamo riscontrando delle sfide significative in merito alla nostra strategia di sicurezza informatica per i lavoratori da remoto	17%

Questi riscontri risultano abbastanza omogenei tra tutte le aziende intervistate, indipendentemente dalla dimensione o del settore. Tuttavia, analizzando i dati, abbiamo trovato interessante il fatto che il settore dell'istruzione sia quello maggiormente preoccupato per la mancanza di personale IT dedicato: il 54%, infatti, ha affermato che questa mancanza sia per loro la principale sfida alla sicurezza.

I sogni di un amministratore di sistema "Are made of this"

In che modo gli utenti possono supportare gli amministratori di sistema?

Quando abbiamo chiesto agli amministratori di sistema di indicare in che modo gli utenti potrebbero aiutarli ed alleggerire in questo modo il loro carico di lavoro, quasi tutti hanno affermato che l'aiuto principale sarebbe quello di seguire le regole basi della sicurezza informatica, come non cadere nelle tecniche di phishing e non utilizzare i dispositivi aziendali per gli acquisti personali.

Cosa vorrebbero gli amministratori di sistema che gli utenti imparassero

A non cliccare su link o allegati sospetti	73%
A non scrivere le password su post-it e di attaccarle al computer	42%
A non rispondere alle email di fantomatici principi o altro che offrono un milione di dollari	29%
A non effettuare shopping on line con i dispositivi aziendali	27%
Come resettare le proprie password	26%
A non cancellare o spostare file importanti	25%
Come mutarsi o smutarsi durante le riunioni	13%
Come trovare il pulsante di accensione	9%

Aspettative salariali degli amministratori di sistema

Lo stipendio medio di un amministratore di sistema negli Stati Uniti è di circa 62.979 $ (circa 55.048 €) (Payscale); nel Regno Unito, invece, è di £ 47.500 (circa 64.391 €) (CW Jobs). Quando abbiamo presentato queste cifre nel nostro sondaggio, oltre la metà (51%) degli amministratori di sistema ha affermato che il proprio stipendio medio è inferiore al previsto, il 35%, invece, ha dichiarato che è in linea e solo il 13% ritiene che sia superiore al previsto.

Alla domanda su quale secondo loro dovrebbe essere lo stipendio medio di un amministratore di sistema, poco più della metà lo ha fissato intorno ai 61-85.000 €.

Come dovrebbe essere lo stipendio medio ideale secondo gli amministratori di sistema

Sotto i € 60K	4%
€ 61–75K	27%
€ 76–85K	26%
€ 86–100K	20%
Sopra € 100K	13%
Non puoi dargli un valore, non ha prezzo!	10%

La maggior parte degli intervistati nel settore manifatturiero ha affermato che secondo loro lo stipendio medio dovrebbe essere intorno ai € 86-100.000 (43%) o superiore a € 100.000 (29%), segnando così l'aspettativa salariale più alta tra tutti i settori analizzati.

La Vacanza Ideale

Si sa l'estate è il periodo delle vacanze, un periodo che tutti noi aspettiamo con trepidazione soprattutto negli ultimi anni. Con questo in mente abbiamo cercato di capire quale secondo gli amministratori di sistema potesse essere la loro vacanza ideale. La maggior parte di loro ha dichiarato che il tempo passato con la propria famiglia, a prescindere dal luogo, fosse la miglior vacanza di sempre! Un'altra parte invece ha dichiarato che sceglierebbe un'isola paradisiaca (come biasimarli, chi non lo vorrebbe). Al tempo stesso, comunque, 1 amministratore di sistema su 5 ha dichiarato che una vacanza ideale sarebbe anche quella in cui nessun utente li contatti per avere supporto.

Il modo ideale di trascorrere le vacanze, secondo gli amministratori di sistema

Trascorrere del tempo con la famiglia, indipendentemente dal luogo	37%
Isola paradisiaca	29%
Ovunque gli utenti non possano raggiungermi	14%
Una settimana senza dover rispondere alle chiamate dell'helpdesk sarebbe perfetto	9%
Escursione in montagna con gli sci	5%
Altro	6%

Abbiamo, inoltre, dato agli amministratori di sistema l'opportunità di indicarci la loro vacanza ideale. Sentiti libero di usare queste risposte come spunto per la tua prossima vacanza!

"Un viaggio di 2 settimane in Giappone; è il mio sogno da prima della pandemia".
"Una vacanza in una baita nel bosco con un ottima TV ed un accesso a internet."

"In crociera in giro per il mondo."
"Qualsiasi cosa all'aperto (escursionismo, caccia, pesca)."
"Un mese a Bordeaux nei migliori castelli."
"Campeggio, cani inclusi."
"Passare del tempo con gli amici."
"Ovunque senza servizio cellulare ma con molte attività all'aperto."
"Da solo. Siediti, rilassati, scrivi, ricerca e studia."
"Videogiochi e relax."
"Viaggiare in giro per il mondo per conoscere altre culture e persone."
"Equitazione".

"Ho un sacco di pazienza": ciò che gli amministratori di sistema vorrebbero che gli utenti sapessero sul loro lavoro

Siamo convinti che gli amministratori di sistema siano dei veri e propri eroi dell'IT, ma gli utenti generalmente ne sono ignari. In effetti, gli utenti raramente (leggi: mai) inviano loro un'email per dire che tutto funziona alla grande. Abbiamo chiesto ai nostri intervistati di indicare una cosa che vorrebbero che gli utenti sapessero del loro lavoro. Abbiamo raggruppato quindi le cose principali.

- **"Segui le FAQ e le policy!!1!111!!"**
  Beh che dire, l'affermazione si commenta da sola. Anche se inconsapevolmente gli utenti possono rendere il lavoro di un amministratore di sistema un vero e proprio incubo. Questo accade ogni qualvolta un utente ignora le regole di base della sicurezza e non segue delle semplici FAQ. Come ha osservato un amministratore di sistema, "*Se gli utenti ci ascoltassero di più, avrebbero meno bisogno di noi*".

- **"La mia pazienza non conosce confini."**
  Essere un amministratore di sistema è un lavoro stressante. Alcuni intervistati hanno dichiarato che a volte si sentono come se avessero conseguito una laurea in psicologia in quanto hanno dovuto imparare a gestire ed a relazionarsi con diversi stakeholder nel mentre cercano di eliminare i tempi di inattività.

- **"Gli amministratori di sistema adorano aiutare le persone.**
  Nonostante tutti i grattacapi del mestiere, molti amministratori di sistema ammettono di amare il proprio lavoro e ritengono che il loro super potere sia quello di aiutare gli utenti. Un intervistato ha persino detto: ""*Il lavoro di amministratore di sistema è un lavoro d'amore*". Una vera e propria dichiarazione d'amore quindi.

- **"Questo lavoro richiede una ricerca costante; quello che si vede è solo la punta dell'iceberg."**
  Una buona amministrazione del sistema è spesso invisibile. Quando i sistemi sono operativi, significa che gli amministratori di sistema hanno svolto molto bene il proprio lavoro: dietro le quinte, hanno gestito correttamente server, rete, switch, router, firewall, punti di accesso, dispositivi biometrici, telefoni IP, gateway di posta elettronica, backup su cloud , strumenti antivirus e molto altro ancora. Inoltre, devono registrare ed indagare sugli incidenti, nonché apprendere e testare costantemente nuove tecnologie. Gli amministratori di sistema vogliono che gli utenti sappiano che lavorano duramente tutto il giorno.

- **"Il lavoro di amministratore di sistema è importante quanto il core business dell'azienda."**
  L'amministratore di sistema rimane un ruolo fondamentale per ogni azienda che si affida ad un software - quindi questo vale praticamente per ogni singola azienda presente sul pianeta! Gli amministratori di sistema aiutano le proprie aziende a rimanere resilienti e sicure, quindi il loro impegno e lavoro deve essere apprezzato e riconosciuti da tutta l'azienda.

Pillole di saggezza dall'amministratore di sistema!

Siamo convinti che i nostri lettori meritino di avere qualche indicazione dagli amministratori di sistema. Abbiamo chiesto quindi ai nostri intervistati di indicarci una "regola d'oro" che secondo loro tutti dovrebbero seguire per essere al sicuro. Infine, abbiamo stilato questa breve guida gratuita per essere tutti più protetti e sicuri.

- **Non pubblicare nulla online che non indosseresti su una maglietta quando il CEO è in visita in ufficio.**
- **Mantieni aggiornato il tuo antivirus e usa la VPN quando lavori sulla rete aziendale.**
- **Non visitare siti Web ingannevoli quando sei al lavoro!**
- **Proteggi il tuo equilibrio tra lavoro e vita privata e prenditi il tempo necessario per quest'ultima.**
- **Conta fino a 10 prima di premere "Invia".**
- **Non cadere vittima di email sospette: se sembra troppo bello per essere vero, è sicuramente una truffa.**
- **Non rispondere a tutti nelle email di gruppo.**
- **Nessuno chiederà mai i dati della tua carta di credito per mostrarti le foto del gatto.**
- **Leggi attentamente cosa dice la finestra di dialogo, non dare mai nulla per scontato.**
- **Usa una password diversa per ogni cosa.**
- **Diffondi amore e meme!**

Risultati regionali

Regno Unito

- Le tre principali preoccupazioni per gli amministratori di sistema nel Regno Unito sono l'aumento del carico di lavoro (82%), l'aumento del rischio di attacchi alla sicurezza informatica (61%) e la mancanza di strumenti adeguati per supportare il lavoro a distanza (42%).
- Il 56% degli amministratori di sistema nel Regno Unito lavora più a lungo rispetto a prima della pandemia. Più della metà (55%) lavora più di 40 ore settimanali e il 15% lavora per più di 60 ore settimanali.
- Il 52% ammette di essere meno concentrato sulla sicurezza rispetto a prima della pandemia.
- Il 39% afferma che la mancanza di personale IT e competenze di sicurezza dedicate espone la propria azienda ad un rischio maggiore per la sicurezza.
- Il 63% pensa che lo stipendio medio annuo di un amministratore di sistema nel Regno Unito dovrebbe essere intorno ai £ 44.000–61.000, che è in linea con lo stipendio medio effettivo di £ 47.500 all'anno.

Italia

- L'86% degli amministratori di sistema italiani afferma la loro sfida principale sia il rapido aumento del rischio di attacchi alla sicurezza informatica e il 57% dichiara un aumento del carico di lavoro.
- Il 43% afferma che il tempo dedicato al lavoro è aumentato rispetto a prima della pandemia. Il 63% lavora dalle 41-50 ore settimanali e il 13% lavora per più di 60 ore.
- Solo il 14% degli amministratori di sistema nelle aziende italiane afferma che il lavoro a distanza ha distolto la loro attenzione dai progetti di sicurezza informatica. In effetti, il 43% nota di concentrarsi maggiormente sulla sicurezza rispetto a prima.
- Il 61% afferma che le minacce informatiche in rapida evoluzione sono un problema serio per la propria strategia di sicurezza informatica per i lavoratori da remoto. Altre preoccupazioni includono la mancanza di budget (38%) e la mancanza delle competenze di sicurezza necessarie (37%).

Informazioni su questo rapporto

Area geografica degli intervistati	
EMEA	24%
APAC	17%
Nord America	53%
Sud America	6%

Dimensione delle Aziende intervistate	
1–100 dipendenti	32%
101–1,000 dipendenti	38%
1,001–5,000 dipendenti	16%
5,001–50,000 dipendenti	10%
50,001+ dipendenti	4%

SETTORI PRINCIPALI	
Technology/Managed Services	10%
Istruzione	10%
Governo	9%
Banking & Finance	8%
Technology/Software	8%
Sanità	7%
Consulenza	5%
Manufacturing	5%
Telecomunicazioni	5%
Retail & Wholesale	4%
Technology/Hardware	4%
Construction & Engineering	3%
Servizi	3%
Non-Profit	3%
Energy	2%
Assicurazioni	2%

Il report è stato redatto da Netwrix Research Lab, che conduce sondaggi di settore tra i professionisti IT di tutto il mondo per scoprire i cambiamenti e le tendenze.

Per ulteriori rapporti, visitare: www.netwrix.com/go/research.

GDPR e Cloud Provider: la compliance e la sicurezza dei dati – Uno studio dell'Osservatorio Cybersecurity & Data Protection della School of Management del Politecnico di Milano

[A cura di Alessandro Piva, Giorgia Dragoni, Ivan Antozzi]

Nel 2021, dopo un anno complesso in cui l'avvento della pandemia aveva letteralmente stravolto la quotidianità delle persone, condizionando fortemente la vita lavorativa e privata con enormi implicazioni anche dal punto di vista della cybersicurezza, si è lentamente instaurato un inedito equilibrio di convivenza con il protrarsi della situazione di emergenza sanitaria.
La risposta delle organizzazioni, dapprima indirizzata verso una massiccia adozione di strumenti in Cloud per garantire continuità al proprio business – aggiuntasi al già in atto utilizzo di più tecnologie della nuvola a supporto dei diversi processi aziendali, si è focalizzata sul consolidamento degli aspetti di sicurezza centrali nel proteggere il patrimonio informativo e prevenire gli attacchi informatici: dagli strumenti di protezione della rete alle soluzioni di Endpoint Protection, necessarie per un'efficace gestione dei dispositivi anche in regime di smart e remote working.

In questo contesto l'Osservatorio Cybersecurity & Data Protection, al suo settimo 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.
All'interno della Ricerca 2021, l'Osservatorio ha affiancato ad alcune indagini trasversali, volte a monitorare il mercato della cybersecurity e l'impatto dei principali trend dell'innovazione digitale sul modello della gestione della sicurezza informatica all'interno di grandi imprese e PMI, anche una Survey con focus più verticale. Tale rilevazione si è posta l'obiettivo di monitorare e valutare in termini di impegno il rapporto con i provider di servizi Cloud e le attività di valutazione di requisiti di sicurezza e di compliance alle normative in materia di protezione dei dati. L'attività, di cui verranno illustrati i risultati nel presente capitolo, ha coinvolto 90 CISO, CSO, CIO, Compliance Manager, Risk Manager, Chief Risk Officer e DPO appartenenti a imprese operanti in Italia.

L'attività di valutazione della compliance alla normativa sui dati personali

Con la corposa adozione di strumenti in Cloud nel periodo pandemico, il numero di organizzazioni che ha adottato tecnologie della nuvola, stipulando contratti con uno o più provider di soluzioni erogate come servizio, corrisponde a un'importante e sempre crescente fetta delle realtà del Paese.

Secondo la fotografia emersa dalla Survey dell'Osservatorio, il 78% delle organizzazioni ha stipulato almeno un contratto di Public Cloud negli ultimi due anni.
La porzione di aziende che hanno all'attivo da 1 a 5 contratti, pari al 63% del totale, non è costituita solo da grandi realtà, ma anche da un 23% di imprese di dimensioni piccole o medie. Sebbene risultino più contenute le quote di organizzazioni che hanno sottoscritto un numero di contratti maggiore, rispettivamente pari all'8% per la fascia tra 6 a 10 contratti e al 7% per la categoria "oltre 10", si evidenzia un trend di crescente complessità, attribuibile in parte anche a un sempre maggiore ricorso a logiche multi-Cloud (**Figura 1**).

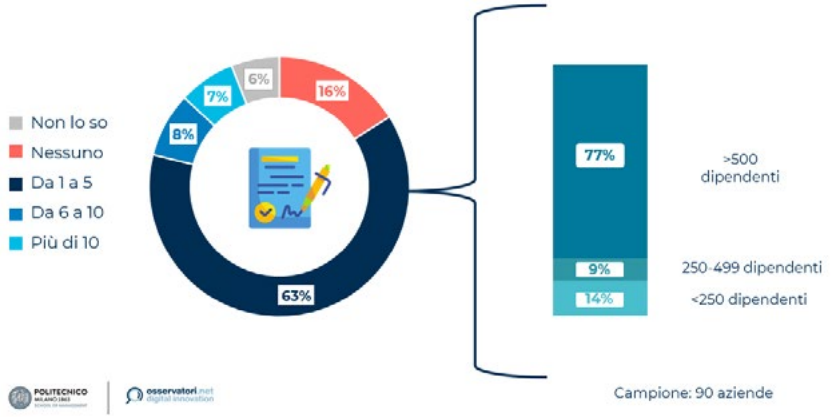


Figura 1 - *I contratti di Public Cloud stipulati negli ultimi due anni dalle organizzazioni italiane – Fonte: Osservatorio Cybersecurity & Data Protection, School of Management – Politecnico di Milano*

La componente contrattuale gioca un ruolo centrale nell'adozione di un servizio Cloud, in cui sono fondamentali le attività preliminari di valutazione della compliance del fornitore alla normativa sui dati personali. Considerando le aziende che hanno stipulato contratti negli ultimi due anni, si attesta all'80% la quota di chi effettua attività di valutazione della compliance alla normativa sui propri fornitori in maniera costante e continuativa, con percentuali minori che vedono valutazioni sporadiche (17%).
Estendendo poi l'analisi ai subfornitori, la regolarità delle attività di valutazione della compliance effettuate scende vistosamente, a favore di un controllo più sporadico (**Figura 2**).

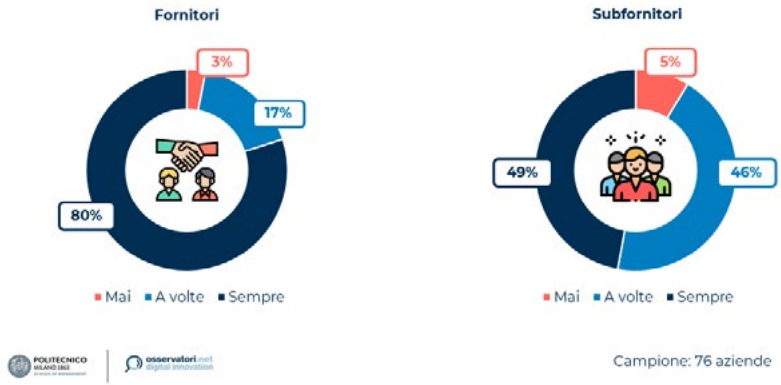


Figura 2 - *L'attività di valutazione della compliance alla normativa sui dati personali – Fonte: Osservatorio Cybersecurity & Data Protection, School of Management – Politecnico di Milano*

L'Osservatorio ha quindi analizzato più nel dettaglio aspetti riguardanti le modalità di svolgimento delle attività di valutazione della compliance dei fornitori. Dal quadro emerge come più della metà delle organizzazioni intervistate basi il proprio esame sia sulla documentazione messa a disposizione direttamente dal fornitore sia su documenti e checklist predisposti dall'azienda stessa. A livello dimensionale, le imprese sotto i 500 addetti appaiono più improntate verso l'accettazione "passiva" della documentazione messa a disposizione dal fornitore, mentre un approccio più proattivo viene adottato dalle grandissime imprese, che tendono a guidare la valutazione secondo i propri criteri.
Focalizzando l'attenzione sulla durata delle attività, emerge come la fetta più corposa del campione impieghi tra 1 e 3 giornate uomo per ciascun contratto, con la dimensione dell'azienda che influisce anche nella durata della valutazione. Le piccole e medie imprese, infatti, impiegano un massimo di 3 giornate uomo, mentre nelle grandi realtà, in cui sono presenti servizi più complessi e contratti più articolati, la durata media cresce oltre le 3 giornate uomo, nonostante i processi di valutazione standardizzati e la presenza di personale dedicato. A livello settoriale, sono gli ambiti Telco & Media e Finance in testa per la maggiore durata delle attività di valutazione della compliance, a causa degli stringenti vincoli normativi che li caratterizzano.

L'attività di valutazione del livello di sicurezza

Un secondo aspetto chiave nell'analisi dei fornitori riguarda le attività di valutazione del livello di sicurezza. Questo tipo di attività viene praticata in maniera minore rispetto alla valutazione della compliance alla normativa sui dati personali, sia sui fornitori, che sui subfornitori. Considerando ancora una volta le aziende che hanno stipulato contratti Cloud

negli ultimi due anni, infatti, solo nel 60% viene sempre effettuata la valutazione del livello di sicurezza dei fornitori, con un ulteriore 32% che effettua le attività in maniera sporadica. Estendendo poi anche in questo caso l'analisi ai subfornitori, la percentuale di aziende che effettua attività di valutazione regolari cala drasticamente fino al 34%, a favore di un controllo più sporadico o inesistente (**Figura 3**).

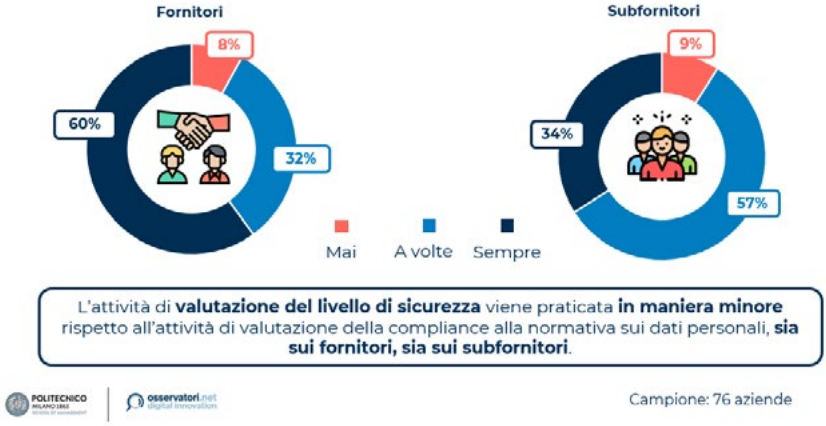


Figura 3 - *L'attività di valutazione del livello di sicurezza – Fonte: Osservatorio Cybersecurity & Data Protection, School of Management – Politecnico di Milano*

L'attenzione dell'Osservatorio si è poi focalizzata sulle modalità di svolgimento delle attività, con il 59% del campione che utilizza sia documentazione messa a disposizione dal fornitore, sia documenti e checklist predisposti internamente e poi condivisi con il fornitore. Anche in questo caso, come rilevato per la valutazione della compliance alla normativa, l'attività è influenzata dalla dimensione aziendale, con le imprese di grandissime dimensioni (> 1.000 addetti) che tendono ad avere una maggiore proattività nella relazione con i fornitori.
Venendo alla durata delle attività di valutazione, emerge come anche in questo caso la componente più estesa del campione impieghi tra 1 e 3 giornate uomo per ciascun contratto, con la dimensione aziendale che incide nuovamente sul tempo dedicato alle attività. In particolare, nelle imprese sopra i 500 addetti, la complessità e l'articolazione dei contratti influiscono negativamente sulla durata media della valutazione, superiore alle 3 giornate uomo, con i settori Telco & Media e Utility che impiegano la porzione di tempo più estesa.

Lo scenario generale italiano: alcuni messaggi dalla Ricerca

Provando a estendere l'analisi allo scenario generale italiano, è possibile trarre alcune considerazioni.

Secondo i dati rilevati dall'Osservatorio Cloud Transformation del Politecnico di Milano, il numero di imprese con più di 250 addetti che ha stipulato almeno un contratto di Public Cloud è pari a 3.318, per un totale di circa 6.600 contratti sottoscritti (il numero medio di contratti stipulati all'anno è pari a 1,5 per aziende tra i 250 e i 500 dipendenti e a 2,4 per aziende oltre i 500 addetti).

Considerando che, come emerso dalla Survey, non tutte le grandi realtà che adottano il Cloud svolgono attività di valutazione della sicurezza e della compliance, emergono due dati riassuntivi che identificano lo scenario generale del Paese:

- Ogni anno vengono destinate tra le 17.000 e le 19.000 giornate uomo ad attività di valutazione della compliance dei fornitori e dei subfornitori alla normativa sui dati personali da parte delle grandi imprese;
- Ulteriori 14.000 - 15.000 giornate uomo vengono poi dedicate annualmente alla valutazione della sicurezza dei fornitori e dei subfornitori.

La stima delle giornate uomo dedicate alle attività di valutazione complessivamente è pari a circa 31.000 - 34.000 giornate uomo, equivalenti a 154 FTE, investite dalle 3.318 grandi imprese che adottano il Public Cloud (**Figura 4**).

Figura 4 - *Lo scenario generale a livello italiano – Fonte: Osservatorio Cybersecurity & Data Protection, School of Management – Politecnico di Milano*

Inoltre, nel caso in cui tutte le 3.318 grandi imprese italiane che adottano il Public Cloud fossero state adempienti alla normativa, effettuando attività di valutazione della compliance alla normativa e della sicurezza dei propri fornitori costantemente, il numero totale di giornate uomo dedicate a tali aumenterebbe ulteriormente, fino a raggiungere 43.000, pari a 195 FTE[1].

La Ricerca evidenzia quindi un basso grado di maturità dell'impianto normativo attuale, in cui le attività di valutazione della compliance alla normativa e della sicurezza dei fornitori a carico delle aziende sono estremamente distribuite e frammentate, richiedendo l'utilizzo di risorse aziendali che potrebbero essere destinate ad altre attività interne alle aziende di maggior valore.
L'approccio attuale è estremamente inefficiente: attività ripetute su uno stesso contratto e che hanno come oggetto della valutazione lo stesso fornitore potrebbero infatti essere gestite con una logica differente ed essere effettuate una tantum per esempio da un ente super-partes.

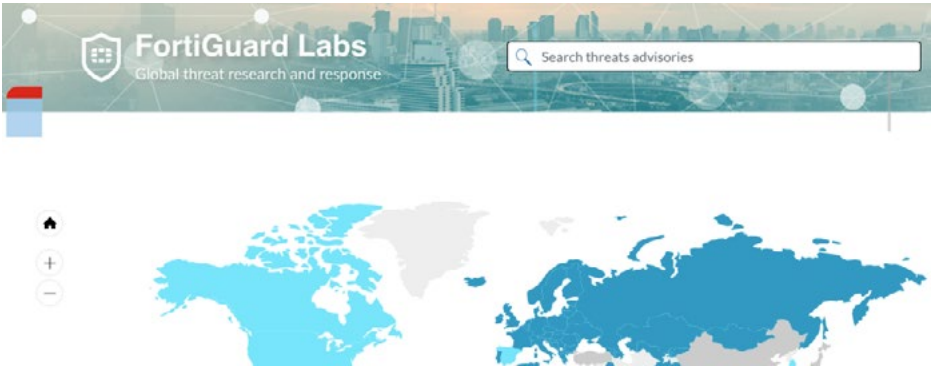
[1] La stima non tiene conto della catena di subfornitura delle aziende.

Pubbliche amministrazioni italiane sotto assedio

(A cura di Aldo Di Mattia, Fortinet)

Nel corso del 2021 le pubbliche amministrazioni italiane (da qui in avanti PA) sono state prese di mira da un numero cospicuo di minacce informatiche e la sanità è stata particolarmente bersagliata. Estraendo i dati dai FortiGuard Labs emerge una situazione allarmante, non tanto per quanto mostrato nei seguenti grafici, i quali sono costituiti dagli attacchi identificati/bloccati dalle PA italiane, ma soprattutto considerando che non ancora tutte le organizzazioni effettuano l'ispezione del traffico cifrato con il protocollo SSL (Secure Sockets Layer). La mancata ispezione dei flussi dati crittografati consente pertanto a una parte crescente di minacce di transitare inosservate fino al loro obiettivo. Oltre agli attacchi contenuti nel traffico cifrato bisogna aggiungere che non tutte le aziende utilizzano le più moderne soluzioni di sicurezza, che includono l'uso automatico di IoC (Indici di compromissione) da fonti esterne e algoritmi di intelligenza artificiale, per lo più basati su machine learning e deep neural network, fondamentali per indentificare e bloccare gli attacchi sconosciuti. I seguenti grafici hanno lo scopo principale di permettere a tutte le organizzazioni di visionare le tipologie di attacchi che hanno colpito i diversi settori della PA (Sanità, Governo, Istruzione e Difesa), permettendo così di verificare se i sistemi di sicurezza attualmente utilizzati sono adeguati e opportunamente configurati.

Nei grafici seguenti è possibile vedere il nome di molte minacce dirette alla PA italiana. Nel sito web https://www.fortiguard.com, nel campo di ricerca in alto a destra (Search threats advisories), può essere inserito il nome delle firme mostrate così da avere dettagli aggiornati in tempo reale.



Schermata del portale FortiGuard Labs

Le minacce più riscontrate nella pubblica amministrazione italiana

Nei grafici da 1 a 4, le minacce più individuate di tipo Exploit, Botnet e Malware, dirette alla pubblica amministrazione italiana nei settori Governo, Istruzione, Difesa e Sanità, suddivise nei quattro trimestri del 2021. Considerando i picchi delle minacce malware nella Sanità si è reso necessario utilizzare una scala logaritmica nell'asse delle ordinate, che permette di avere dei valori comprensibili anche per le altre minacce, ma nella lettura è fondamentale tenerne conto.

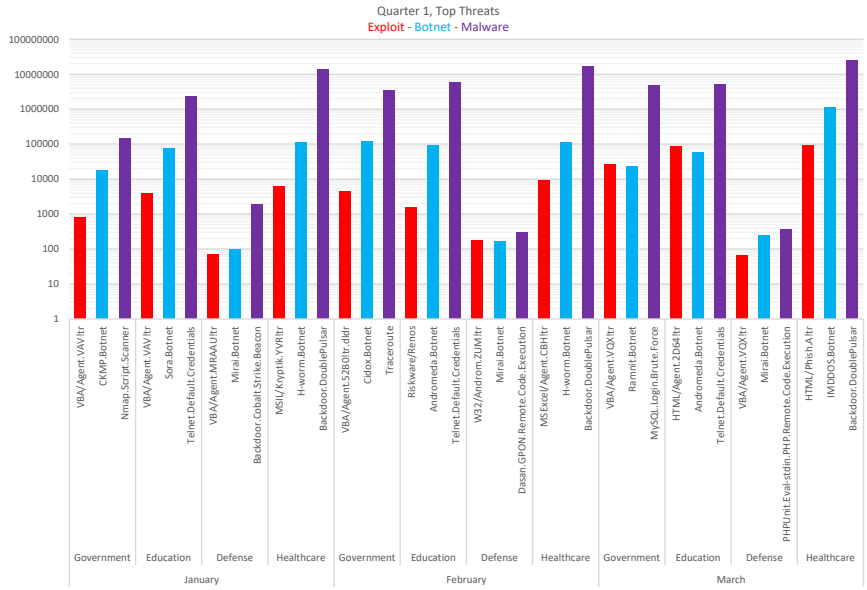


Grafico 1 - *Primo trimestre, top signature IPS, AV, Botnet nei settori della PA*

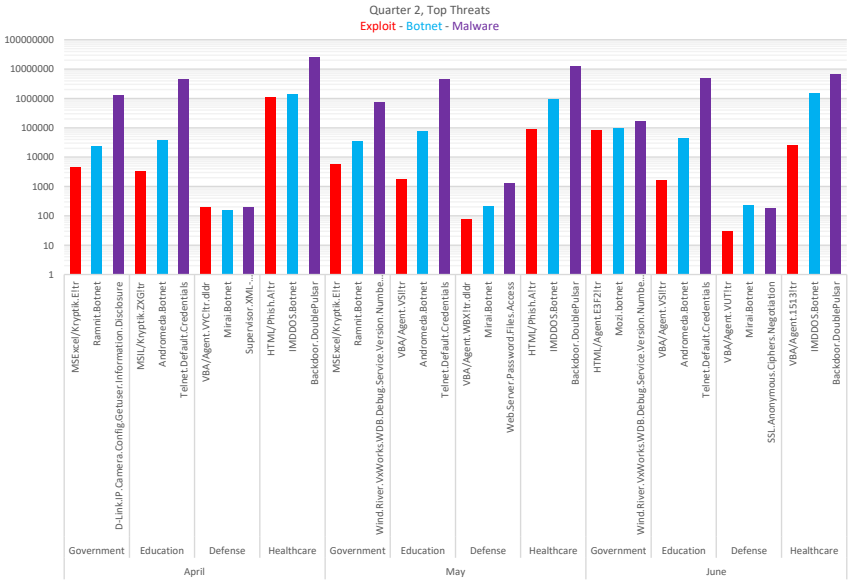


Grafico 2 - *Secondo trimestre, top signature IPS, AV, Botnet nei settori della PA*

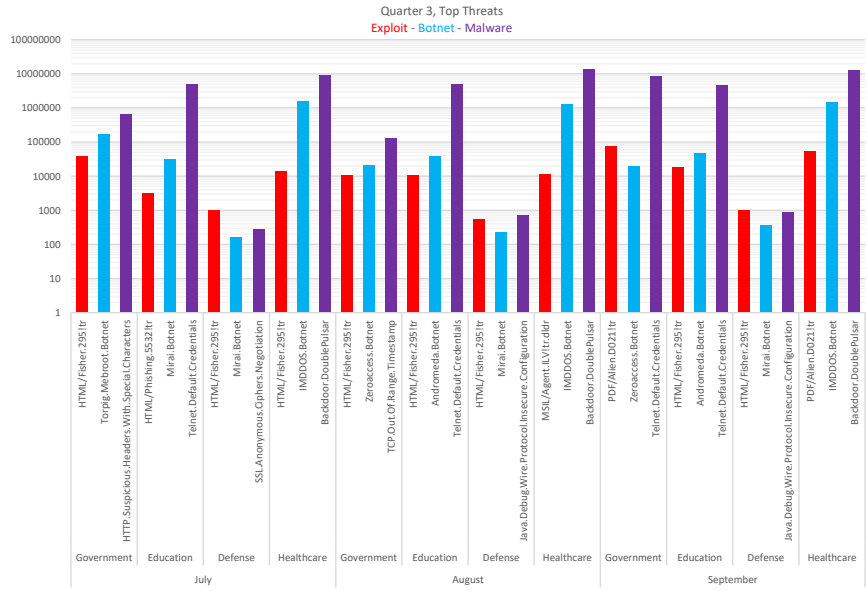


Grafico 3 - *Terzo trimestre, top signature IPS, AV, Botnet nei settori della PA*

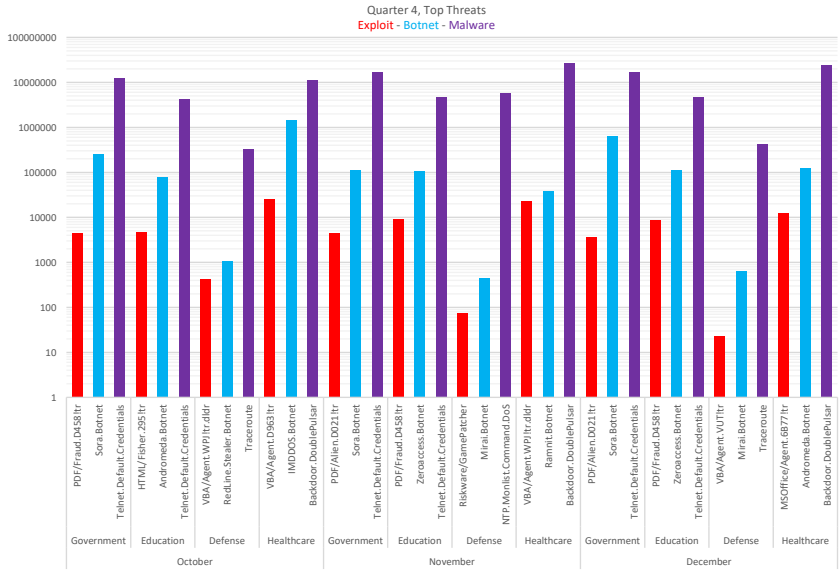


Grafico 4 - *Quarto trimestre, top signature IPS, AV, Botnet nei settori della PA*

Vulnerabilità della libreria log4j

Un altro dato interessante che consente di capire meglio quanto la PA sia appetibile da parte dei criminali informatici è analizzare la numerosità degli attacchi che hanno tentato di sfruttare tra la fine del 2021 e l'inizio del 2022 le recenti vulnerabilità della libreria Java Log4J, ampiamente utilizzata nei server Apache e in altri sistemi per la gestione dei log. Nel corso del mese di dicembre sono state individuate le seguenti vulnerabilità, descritte nei rispettivi CVE (Common Vulnerabilities and Exposures), e nello specifico:

- 10 dicembre 2021, Code Execution, CVE-2021-44228, CVSS 3.1 base score 10.0, Critical
- 14 dicembre 2021, Code Execution 2, CVE-2021-45046, CVSS 3.1 base score 9.0, Critical
- 18 dicembre 2021, Context DoS, CVE-2021-45105, CVSS 3.1 base score 5.9, Medium
- 19 dicembre 2021, variante inclusa in CVE-2021-44228, CVSS 3.1 base score 10.0, Critical

Vengono riportati nei seguenti grafici gli eventi individuati per le seguenti due firme messe a disposizione da Fortinet:

- *Apache.Log4j.Error.Log.Remote.Code.Execution* (CVE-2021-45046, CVE-2021-44228)
- *Apache.Log4j.Error.Log.Thread.Context.DoS* (CVE-2021-45105)

Maggiori dettagli disponibili ai link:

- https://www.fortinet.com/blog/threat-research/critical-apache-log4j-log4shell-vulnerability-what-you-need-to-know
- https://www.fortiguard.com/encyclopedia/ips/51006
- https://www.fortiguard.com/encyclopedia/ips/51050

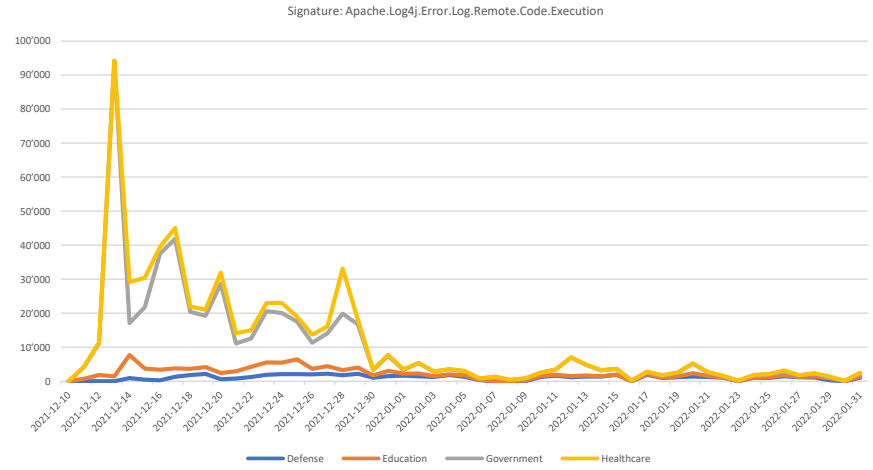


Grafico 5 - *Eventi "code.execution" rilevati nella PA nel periodo dicembre 2021 - gennaio 2022*

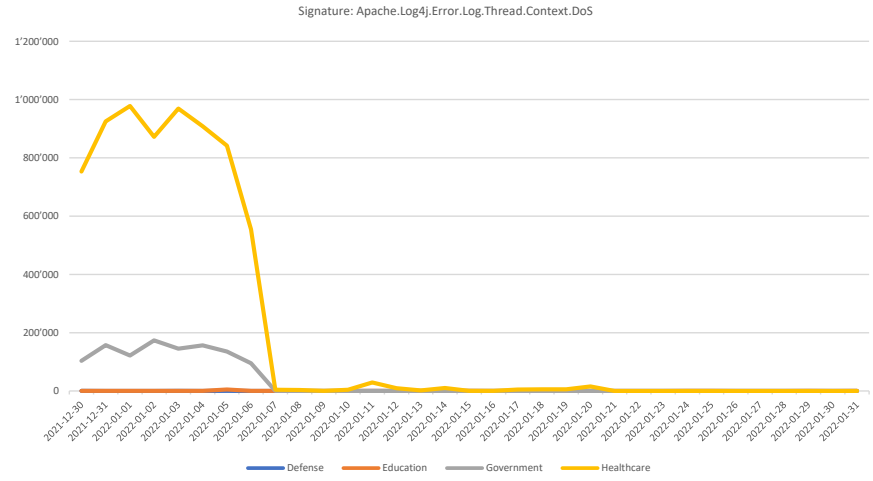


Grafico 6 - *Eventi "context.DoS" rilevati nella PA nel periodo dicembre 2021 - gennaio 2022*

Per permettere una migliore analisi si riportano di seguito gli stessi due grafici mostrati precedentemente ma in questo caso relativi ai settori privati che sono parte integrante delle infrastrutture critiche italiane, quali: Telco/Carrier, Transportation, Finance ed Energy & Utilities.

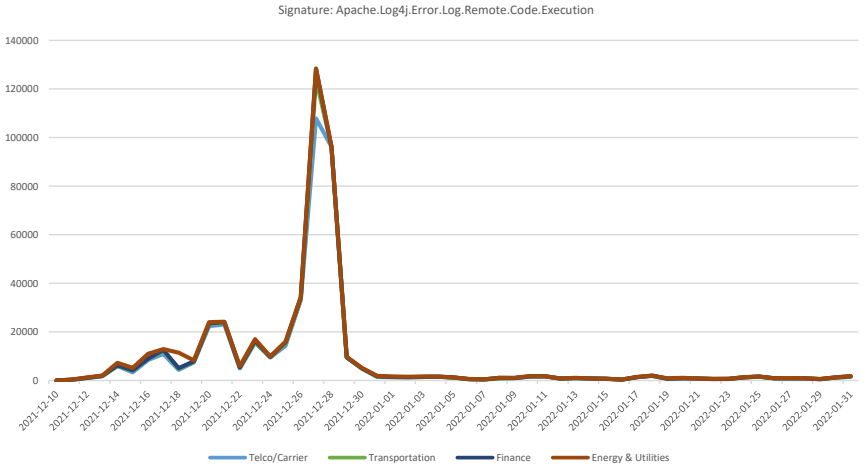


Grafico 7 - *Eventi "code.execution" rilevati nei settori privati nel periodo dicembre 2021 - gennaio 2022*

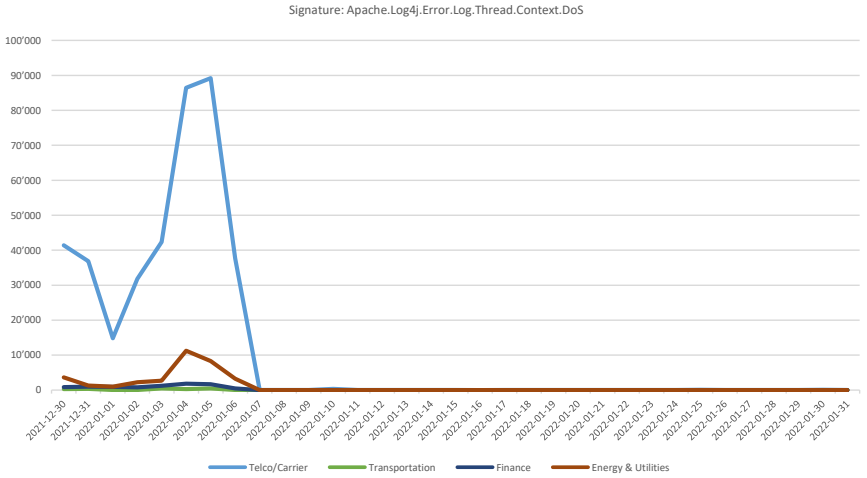


Grafico 8 - *Eventi "context.DoS" rilevati nei settori privati nel periodo dicembre 2021 - gennaio 2022*

In ultimo, per meglio capire in termini statistici l'andamento delle stesse minacce nel mondo e correlare i dati di inizio gennaio tra quanto avvenuto in Italia nei settori pubblici e privati delle infrastrutture critiche e il resto del mondo, si includono i seguenti due grafici che mostrano gli eventi individuati globalmente delle due signature precedentemente descritte.

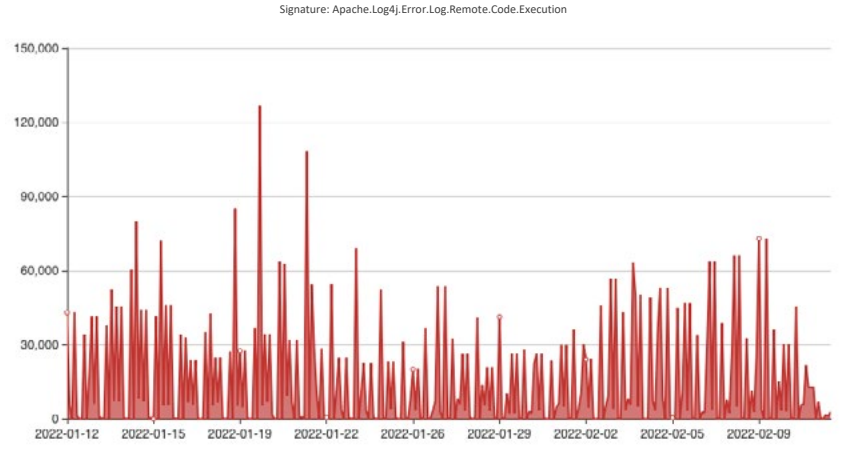


Grafico 9 - *Eventi "code.execution" rilevati nel mondo nel periodo gennaio 2022 - Febbraio 2022*

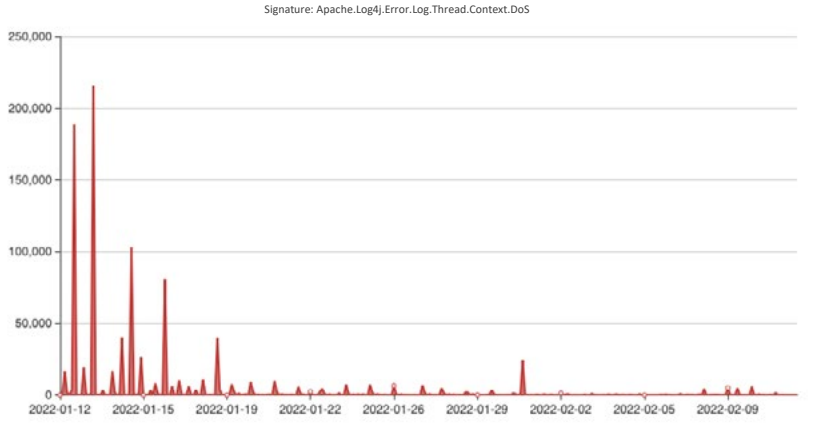


Grafico 10 - *Eventi "context.DoS" rilevati nel mondo nel periodo gennaio 2022 - Febbraio 2022*

Previsioni per il 2022

Secondo lo studio condotto, i cybercriminali stanno perfezionando le proprie strategie e stanno mettendo a punto le loro metodologie per colpire nuove aree così da coprire l'intera superficie di attacco, approfittando in particolar modo del crescente utilizzo del remote working. I criminali informatici stanno cercando altresì di massimizzare le opportunità che derivano dal crescente aumento di dispositivi IoT (Internet of Things) in tutti gli ambienti ma soprattutto in quello domestico, delle reti internet satellitare e dei dispositivi OT (Operation Technology). I trend identificati rivelano le strategie che gli attaccanti informatici sfrutteranno in futuro e si avrà contestualmente un aumento di attacchi in termini di "left-hand" e di "right-hand" secondo la catena di attacco del framework MITRE ATT&CK.

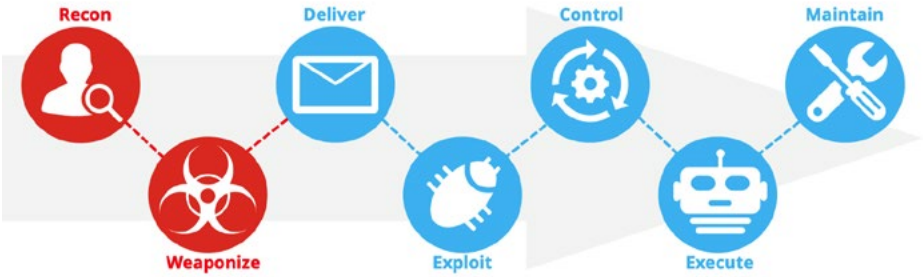


Immagine - *MITRE ATT&CK chain*

Nel "lato sinistro" della catena di attacco (in rosso) è possibile trovare gli sforzi compiuti prima di mettere in atto un'azione malevola, che comprendono attività quali la pianificazione, lo sviluppo e le strategie di acquisizione degli strumenti che verranno utilizzati. Nel "lato destro" (in azzurro) troviamo invece la più familiare fase di esecuzione degli attacchi. Si prevede che i criminali informatici dedicheranno più tempo e sforzi alle attività di ricognizione e all'identificazione di funzionalità zero-day per sfruttare le nuove tecnologie e garantire attacchi di maggior successo. Contestualmente vedremo un aumento della velocità di lancio di nuovi attacchi nel "lato destro" a causa dell'espansione del mercato del Crime-as-a-Service. Si prevede in aggiunta un aumento di nuovi attacchi che prenderanno sempre più di mira le piattaforme Linux. Linux è molto presente nei sistemi di back-end della maggior parte delle aziende e fino a poco tempo fa è stato stranamente ignorato dalla comunità degli attaccanti. Allo stesso modo, Microsoft sta integrando WSL (sotto-sistema Windows per Linux) in Windows 11. WSL permette l'esecuzione nativa di eseguibili binari Linux direttamente su Windows e anche in quest'ultimo caso sono state già individuati file di test malevoli capaci di prendere di mira WSL.

Ci saranno con molta probabilità anche nuovi exploit che mireranno ai provider Internet satellitari, come Starlink, che già dispone di migliaia di satelliti nell'orbita terrestre bassa (Low Earth Orbit) e ipotizza di arrivare a più di 30.000 satelliti interconnessi nel prossimo futuro. Le organizzazioni che utilizzano la connettività satellitare per fornire servizi critici in località remote o fornire servizi a clienti in movimento, come navi e compagnie aeree, dovrebbero usare la dovuta cautela, poiché già delle minacce, come ICARUS, hanno già attacco i servizi Internet basati su reti satellitari.
Un altro tema destinato a destare molta preoccupazione è legato all'evoluzione dell'utilizzo dell'intelligenza artificiale, in particolare i "deep fake" saranno sempre più in grado di sfruttarla per imitare le attività umane così da perfezionare gli attacchi basati sul "social engineering". Tra i vari scopi, uno dei più allarmanti è sicuramente relativo agli attacchi di tipo "impersonation" in tempo reale su applicazioni vocali e video, che potrebbero permettere ai cybercriminali di superare eventuali riconoscimenti biometrici, ponendo sfide sempre più complesse per garantire l'autenticazione degli utenti in sicurezza.
I criminali informatici guarderanno sempre più ad attacchi basati sull'OT, soprattutto perché la convergenza OT e IT sull'edge prosegue. Gli attaccanti tenteranno infatti di prendere in ostaggio questi sistemi e le relative infrastrutture critiche al fine di richiedere un riscatto a scopo di lucro, oltre ad altre conseguenze molto più gravi, inclusi gli impatti sulle vite umane. Tradizionalmente gli attacchi ai sistemi OT sono stati veicolati da attori specializzati, sfortunatamente sempre più spesso queste tipologie di minacce sono incluse nei kit acquistabili da chiunque sul dark web. Contemporaneamente i criminali informatici combineranno sempre più malware ransomware con attacchi DDoS (**Distributed Denial-of-Service**), così da limitare la mitigazione del danno da parte dei SOC (Security Operation Center) delle varie organizzazioni.
Come ultimo aspetto va considerato che il perimetro diventa sempre più frammentato, i team di cybersecurity continuano ad operare spesso in silos e molte organizzazioni stanno passando a un modello multi-cloud o ibrido. Tutti questi fattori uniti contribuiranno oltremodo a creare l'ambiente ideale per i criminali informatici che adotteranno un approccio olistico e sempre più sofisticato. Chi si occupa delle strategie di difesa informatica dovrà pianificare in anticipo le azioni da mettere in campo sfruttando la potenza dell'AI per accelerare la prevenzione, il rilevamento e la risposta alle minacce.

Cybersecurity automotive: rischi, normative e mitigazioni

[A cura di Andrea Tomassi e Giuseppe Faranda]

Il mondo dell'automotive sta vivendo una profonda trasformazione, spinta dalle mutate esigenze del mercato, dallo sviluppo tecnologico e dalle nuove regolamentazioni, soprattutto in termini di sicurezza ed emissioni. Questo si associa ad una transizione, partita nello scorso secolo, dove i controlli elettromeccanici vengono sostituiti da controlli elettronici, comandati dal software distribuito su centraline specializzate. Un veicolo oggi utilizza da 70 a 100 centraline indicate come ECU (Electronic Control Unit) che contengono centinaia di milioni di linee di codice.

Sono quattro i driver principali di questa trasformazione, in genere identificati dall'acronimo CASE: Connected, Autonomous, Shared and Electric. Questo disegna uno scenario di mobilità individuale basata su veicoli connessi, in grado di muoversi in modo autonomo, almeno in determinati scenari, elettrici e condivisi, inteso come fortemente integrati con altre soluzioni di mobilità e, a volte, in car sharing.

Le case automobilistiche, che devono adeguarsi e sfruttare queste nuove tendenze, stanno quindi effondendo enormi sforzi, sia dal punto di visto tecnologico che economico, per adeguare le loro linee di prodotti. Su queste quattro tendenze, indicate dall'acronimo "CASE", si concentra molta parte della competizione sul mercato dell'auto.

Questa trasformazione ha un impatto enorme sulla progettazione dei nuovi veicoli, in particolare rendendo sempre più sofisticate le architetture elettriche/elettroniche che sono alla base dei veicoli elettrici, autonomi e connessi. Architetture che sono basate su reti di bordo che collegano un numero sempre crescente di ECU, ognuna delle quali sovrintende ad una o più funzioni della vettura; indipendentemente dal fatto che siano funzioni legate alla guida, alle prestazioni, all'infotainment o alla sicurezza.

Il ruolo del software sta diventando sempre più importante, tanto da introdurre il concetto di "Software Defined Vehicle", cioè veicoli che si caratterizzano per il software che implementano, e che di conseguenza possono essere aggiornati anche dopo il loro acquisto. Aggiornamento che può avvenire anche in modalità "over the air2.

Ma più i veicoli diventano oggetti "personalizzabili", flessibili ed aperti, più il tema della sicurezza informatica diventa rilevante. Assecondare ciascuno di questi trend rende la vettura più complessa e sofisticata, ma anche potenzialmente più vulnerabile a minacce informatiche.

In generale gli scenari che possono inficiare il corretto comportamento delle funzioni presenti in un'autovettura possono essere: malfunzionamenti dovuti a indisponibilità di funzionalità, malfunzionamenti dovuti a limitazioni di funzionalità, malfunzionamenti dovuti a compromissione di funzionalità e malfunzionamenti dovuti a bias di funzionalità.

Nel corso degli anni si è assistito ad un incremento preoccupante degli attacchi, ed i costruttori stanno sviluppando strategie di difesa sempre più sofisticate.

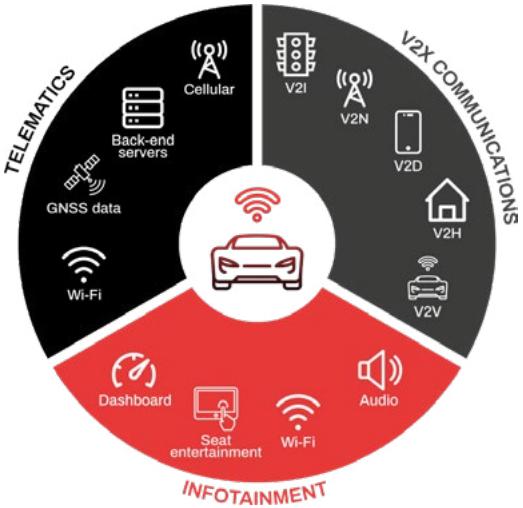


Figura 1 - *Automotive Ecosystem - source: Enisa* (5)

Architetture veicolo

Dal punto di visto elettrico/elettronico, una vettura è un insieme di centraline, ognuna con una sua specializzazione, interconnesse tra di loro che si scambiano messaggi su reti dati di varie tipologie. Similarmente a quanto avviene nelle reti dati tradizionali, anche all'interno della vettura possono essere identificati diverse entità quali ad esempio: gateway, router, centraline specializzate per funzioni differenti (nodo telematico, infotainment, controllo motore, …), sensori ed attuatori.

Ciascuna di queste entità comunica con le altre in maniera punto-punto o broadcast attraverso delle connessioni wired o wireless, interconnesse in maniera gerarchica o funzionale. Esistono per esempio reti dedicate al controllo dei sistemi di ausilio alla guida, del powertrain, del controllo della dinamica veicolo, etc.

Il numero di ECU in una vettura varia a seconda delle funzioni implementate e della configurazione. Per garantire la non interferenza tra funzioni, la safety e le performance, una vettura è solitamente divisa in domini (powertrain, infotainment, ecc.), ad ogni dominio corrisponde una o più sottoreti. L'insieme dei domini realizza quella che viene chiamata architettura elettrica/elettronica, un insieme di router, gateway ed ECU, che deve essere opportunamente ridondata, presidiata e resa sicure al fine di garantire l'integrità di guidatori e passeggeri.

La **figura 2** schematizza 3 possibili tipologie di architetture di bordo, che rispondono a crescenti livelli di complessità delle funzioni veicolo.

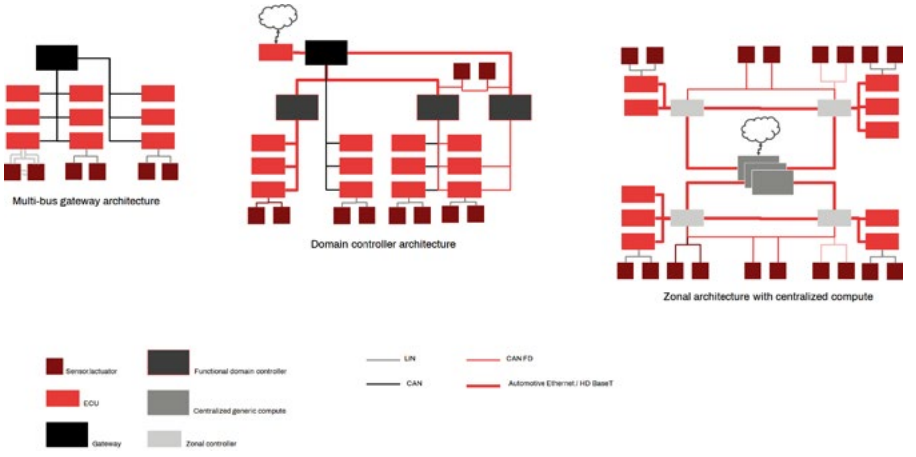


Figura 2 - *Automotive Architetture*

Le reti di bordo possono essere wired (LIN, CAN/CANFD, MOST, Ethernet, Flex-ray…) o wireless (WiFi, Bluetooth, NFC, 2G/3G/4G/5G, DSRC, …). Le prime presiedono principalmente alla comunicazione delle diverse centraline elettroniche con i sensori (eg. Sensore di pioggia) ed attuatori (eg. Attuatore spazzole tergicristalli). Le seconde permettono la comunicazione laddove una connessione via cavo non è possibile o non è opportuna, ad esempio con il sistema di monitoraggio della pressione dei pneumatici, con i dispositivi personali del guidatore e dei passeggeri o con Internet, tramite la rete cellulare.
Le prime reti di bordo sono state introdotte in vettura alla fine degli anni 90 e da allora si sono diffuse fino ad arrivare a gestire il veicolo completo. Anche segnali molto semplici, come ad esempio il comando alza vetri, viaggiano oggi su rete: il pulsante di comando è collegato ad una centralina che invia, tramite cavo, i relativi comandi alla centralina che controlla il sottosistema di attuazione. Apparentemente questo sembra complesso, in realtà semplifica e rende flessibile lo sviluppo di funzioni sempre più complesse. Un caso semplice: quando si chiude la vettura con il telecomando è possibile anche chiudere tutti i finestrini, senza dover agire su più pulsanti. In poche parole, tutto è controllato "by-wire".
La figura 2 mostra 3 diverse tipologie di architetture elettriche/elettroniche:

- Multibus gateway: diverse reti sono interconnesse tra loro e comunicano attraverso un gateway che permette il forwarding dei messaggi rilevanti da una rete ad un'altra. Ad esempio, se un segmento assolve al compito di controllo del powertrain, ed un altro a quello del controllo dei sistemi di interazione con il guidatore, il gateway si occuperà di trasferire, da un segmento ad un altro, il messaggio di "numero giri motore", mentre manterrà locali i messaggi diretti ad ECU sullo stesso segmento di rete
- Domain controller: il secondo modello di architettura di rete utilizza delle centraline con performance superiori alle altre per gestire logiche di dominio; ovvero permette l'imple-

mentazione (ad un livello di astrazione superiore rispetto alle normali ECU) di algoritmi di controllo, per esempio riferite alla gestione dell'assetto della vettura. I domain controller si interfacciano tra di loro per gestire il corretto passaggio di informazioni tra diversi domini.
- Zonal Architecture: il terzo modello proposto è un'evoluzione del secondo, che introduce il concetto di separazione di diverse zone del veicolo rispetto alla loro interazione con i domain controller.

Ognuna di queste architetture risponde ad esigenze di complessità e segmentazione incrementali.
All'evoluzione delle architetture di bordo si associa anche l'estensione delle reti di collegamento verso l'esterno del veicolo. Questo avviene, analogamente ad altri settori industriali, attraverso l'introduzione di reti wireless a lungo (GPRS, LTE, 5G, ecc.) e corto (WiFi, Bluetooth, DSRC, V2X,) raggio. L'estensione è finalizzata a supportare un nuovo set di applicazioni e funzioni quali ad esempio l'integrazione di device personali, la connettività ad Internet, e tutto il set delle funzioni che rientrano sotto la sigla V2X (comunicazione del veicolo con l'infrastruttura, altri veicoli, ecc.).
L'architettura del veicolo quindi si estende al di fuori del veicolo stesso, introducendo in tal modo il concetto di "Extended Vehicle", dove parte dell'architettura del veicolo si espande esternamente fino ad integrare il cloud.
Diventa facile comprendere come collegare in cloud un ecosistema di centraline interconnesse, può portare a scenari di rischio elevatissimi. Si pensi solo alle conseguenze di intercettare il controllo di funzioni di ausilio alla guida da remoto. Questo ha reso indispensabile un ripensamento profondo dello sviluppo delle funzioni del veicolo e delle misure di protezione delle architetture elettriche/elettroniche, introducendo concetti quali il "secure by design" e il "continuous monitoring" delle minacce informatiche.

I rischi informatici nell'automotive

Il fatto che la cybersecurity sia diventata un problema per l'automobile è certificato anche dal sempre crescente numero di report di vulnerabilità individuate su vetture di diversi brand. La **Figura 3** riporta, per i primi mesi del 2020, una lista parziale degli eventi significativi di sicurezza nel mondo automotive.

TOP 2020 CYBER INCIDENTS			
JANUARY	**4,118 vehicles** were stolen in India with cheap electronic devices that enabled the thieves to bypass the engine control module, unlock the vehicle, start the engine, and access the vehicles' computer.	A **Mobileye 630 PRO** and **Tesla Model X** hack fooled the ADAS and autopilot systems to trigger the brakes and **steer into oncoming traffic**.	
FEBRUARY	19 vulnerabilities were found in a **Mercedes-Benz E-Class** car, allowing hackers to control the vehicle remotely, including opening its doors and starting the engine.		
APRIL	Hackers took full control of an **OEM's corporate network** by reverse-engineering a vehicle's TCU and using the telematics connection to infiltrate the network.		
MAY	Hackers found passwords and API tokens for **Daimler's** internal systems after source code of a connected car component was made publicly available.	Hackers **publicly** offered to sell car rental information of 3.5 million **Zoomcar** users on the dark web.	**Toll Group**, an Australian transportation fleet, was hit with a ransomware attack for the second time in 2020, affecting 1,000 servers and 40,000 employees.
JUNE	**Honda** stopped production in a number of its plants after its networks in Europe and Japan were attacked with the Snake ransomware.		
AUGUST	More than 300 vulnerabilities were found in over 40 ECUs developed by 10 Tier-1 companies and OEMs.	A hacker was able to gain control over Tesla's entire connected vehicle fleet by exploiting a vulnerability in the OEM's server-side mechanism.	

Figura 3 - *Automotive Attack – source Upstream Security (2)*

Il report di Upstream Security indica anche quali sono i principali vettori di attacco, evidenziando che il 73% di essi è stato effettuato tramite connessione remota e solo il 27% tramite accesso fisico alla vettura (**Figura 4**).

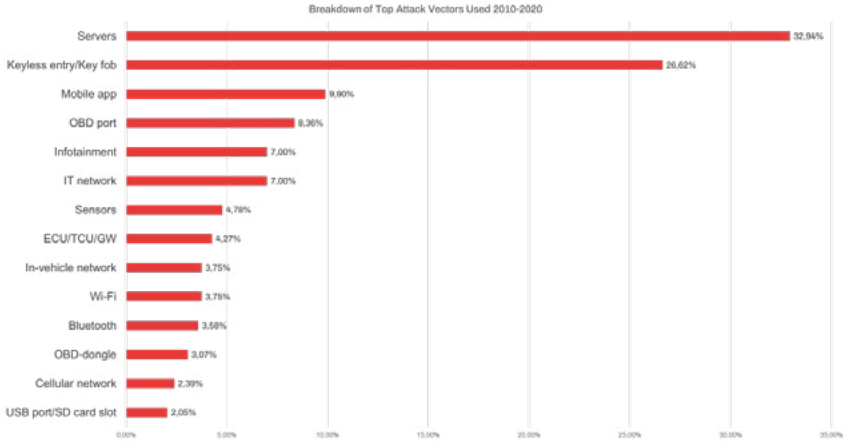


Figura 4 - *Automotive Attack Vector - source Upstream Security (2)*

L'impatto degli attacchi è riassunto nella figura 5:

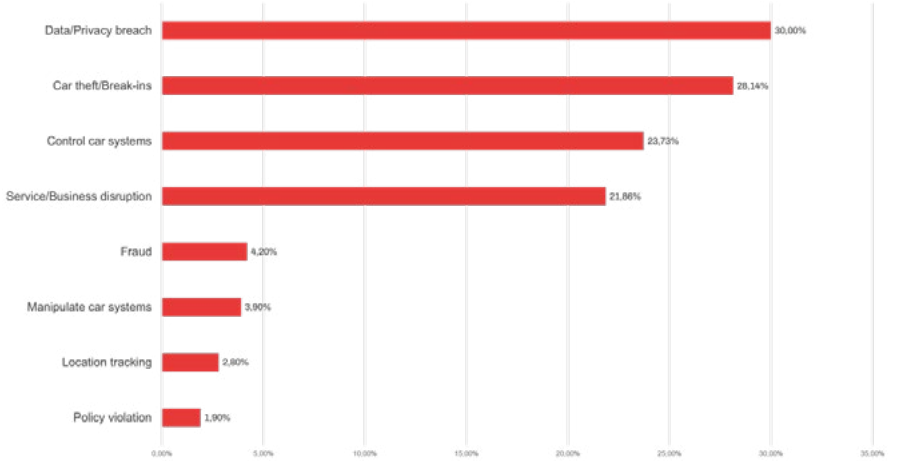


Figura 5 - *Automotive Attack Impact - source Upstream Security (2)*

Il problema è particolarmente serio nel momento in cui gli attacchi possono portare a rischi severi rispetto alla sicurezza degli occupanti, degli altri utenti della strada e dell'intero ecosistema di mobilità.
Il report ENISA intitolato "Good Practice for security on smart cars", e pubblicato nel Novembre 2019 (1), riassume in maniera sintetica ed efficace gli scenari di attacco nelle vetture cosiddette "smart", cioè connesse, con sistemi di ausilio alla guida e sistemi innovativi di powertrain (elettrici, ibridi, ecc.):

1. **Vulnerabilità nello stack di comunicazione**: sfruttando le vulnerabilità nello stack di comunicazione della rete intraveicolare è possibile arrivare alle centraline, riprogrammarle e prenderne il controllo
2. **Ottenere l'accesso al veicolo attaccando le app dell'infotainment:** un hacker può essere in grado di prendere il controllo del veicolo sfruttando le vulnerabilità delle applicazioni mobili ed integrate nel sistema di infotainment
3. **Attaccare server remoti per influenzare il comportamento dei veicoli**: prevedono la compromissione di servizi esterni al veicolo a cui questo si connette per ottenere influenzare le performance del veicolo e la sua sicurezza
4. **Inviare aggiornamenti firmware malevoli**: attraverso l'uso di Base Transceiver Station (BTS), Wi-Fi router, RSU, modificati ad-hoc è possibile distribuire malware facendolo passare per aggiornamenti legittimi compromettendo le funzionalità del veicolo

5. **Attaccare le RSU con l'intento di diffondere traffico malevolo**: nell'ambito dei veicoli a guida autonoma, le RSU (Road Side Unit, centraline dati/sensori a bordo strada) rappresentano un nodo cruciale che se compromesso può portare alla diffusione di messaggi non corretti ed impattando la safety
6. **Attaccare le interfacce V2V**: un utente malevolo potrebbe introdurre dei veicoli atti a diffondere messaggi non autentici riguardo le condizioni di traffico al fine di modificare il comportamento di altri veicoli compromettendone la safety.
7. **Compromissione dei sensori**: uno scenario d'attacco plausibile prevede la manomissione in maniera mirata di sensori impedendone il loro corretto funzionamento.
8. **Communication jamming**: producendo interferenze radio è possibile saturare i canali delle reti wireless in modo che i veicoli non possano più emettere o ricevere messaggi V2X.
9. **GNSS spoofing**: un attaccante può ingannare un servizio di terze parti facendo risultare il veicolo in un punto dello spazio diverso da quello reale, o addirittura in momento diverso.
10. **Bloccare messaggi safety critical**: un attaccante può bloccare messaggi critici come quelli di controllo degli attacchi DoS evitando così che i veicoli semiautonomi possano reagire in maniera appropriata

(source ENISA (1))

Questa lista consente di immaginare i rischi possibili e le conseguenze di una incorretta gestione della sicurezza, ad esempio, su vetture a guida autonoma comunicanti tra di loro e connesse ad Internet.
Un elemento distinguente del settore Automotive, rispetto ad altri settori dove sono presenti sistemi ICT, è rappresentato dal numero considerevole di **fornitori** impiegati per la realizzazione dei componenti, centraline, sensori ed attuatori. Le possibili minacce che possono emergere e i conseguenti rischi, devono essere analizzati e gestiti su tutta la filiera dello sviluppo prodotto e di conseguenza un continuo scambio di informazioni deve essere mantenuto tra i diversi attori dell'ecosistema.

Alla luce di quanto indicato, si comprende quanto un componente essenziale per una strategia di sicurezza completa sia la promozione di un **ISAC** (Information Sharing and Analysis Center) in ambito Automotive. Disporre di un ISAC Automotive (che esiste ad esempio in Nord America), permette di reagire tempestivamente ed adeguatamente ad un attacco, evitando la sua propagazione nell'intero ecosistema della mobilità su strada.

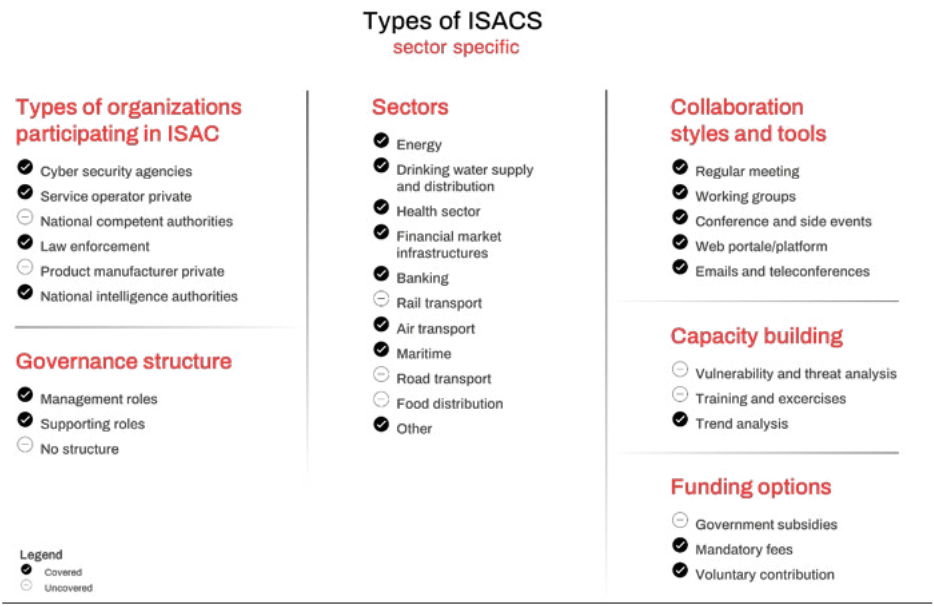


Figura 6 - *Types of ISAC - - source Enisa (5)*

Accesso ai dati vettura

Attraverso le reti di bordo, su cui viaggiano i segnali che sovrintendono alle funzioni di guida, e la connettività verso i server Internet, una vettura di ultima generazione può generare e condividere una quantità di dati enorme, che possono essere utilizzati per gli scopi più diversi, sia commerciali che tecnici.

Questi dati sono in grado di generare opportunità di business per un vasto numero di player dell'ecosistema della mobilità quali, ad esempio, costruttori automobilistici, fornitori indipendenti di servizi di riparazione o manutenzione, assicurazioni, per arrivare anche ai distributori di carburanti, servizi di ricarica o ai fornitori di servizi logistici (hotel, ristoranti…).

I dati generati a bordo veicolo sono sensibili e quindi rientrano nell'ambito della normativa denominata General Data Protection Regulation (GDPR). Da un punto di visto tecnologico, le scatole telematiche, presenti in vettura grazie anche all'approvazione della normativa EU sull'obbligatorietà del servizio di "chiamata di emergenza", rendono possibile, al costruttore, scaricare in tempo reale i dati di interesse.

A seconda dei casi, poi, questi dati vengono messi a disposizione degli altri player attraverso dei server "off line" tramite i quali è possibile accedere ai dati di una specifica vettura, alle condizioni definite dal costruttore auto. Ad oggi la tecnologia a cui i costruttori guardano per la condivisione dei dati veicolo è quella del cosiddetto "Extended Vehicle", ovvero trasferire i dati di ogni veicolo, organizzati e strutturati, su dei server che rappresentano appunto

un'estensione, a terra, dei veicoli. Il concetto di "Extended Vehicle" è standardizzato dalla ISO 20077 "Road Vehicle - Extended Vehicle (ExVe) Methodology".
Pur sembrando una soluzione ragionevole, l'Extended Vehicle, presenta difetti, che lo rendono poco pratico ed inefficiente per alcune applicazioni. Inparticolare la mediazione necessaria con il costruttore del veicolo, che rende necessario, affinché una applicazione possa essere diffusa su tutti i veicoli indipendentemente dal brand, un coinvolgimento di tutti i costruttori. Una soluzione più equilibrata, promossa da diversi attori, è quello di definire dei servizi di accesso ai dati direttamente su vettura e senza la mediazione di terze parti. Questa soluzione è stata caldeggiata all'interno del Motor Vehicle Working Group della Commissione Europea, gruppo di lavoro che coordina le azioni normative sul veicolo a livello Europeo. uestq Questo secondo modello, pur avendo indubbi vantaggi sotto l'aspetto sia della concorrenza equa tra i diversi fornitori di servizi che della libertà di scelta del fornitore di servizi da parte del proprietario del veicolo, ha delle implicazioni importanti dal punto di vista della cyber security. Le iniziative di studio di modelli di questo tipo sono diverse, citiamo ad esempio "C-ITS: Cooperative Intelligent Transport Systems and Services" (ISO/TS 21184:2021).

La normativa

Il 2022 sarà l'anno che vedrà una diffusione massiccia della cybersecurity nell'industria automotive europea (e non solo). Entra in vigore la General Safety Regulation (GSR) che prevede, oltre a tutta una serie di misure per migliorare la sicurezza del veicolo, anche l'applicazione della normativa UNECE R155, che impone il rispetto delle "best practices" della sicurezza ed i concetti legati al "secure by design". GSR definisce insomma l'insieme di regole da rispettare per ottenere l'omologazione di una vettura nell'Unione Europea. UNECE (United Nation Economic Council for Europe), dal canto suo, è un organismo che si occupa di definire i regolamenti relativi a diversi aspetti della società e dell'industria, e attraverso il gruppo di lavoro WP 29 si occupa in particolare delle normative per l'omologazione dei veicoli. UNECE, attraverso la Regulation 155 (approvata dalla UE nel 2019 e obbligatoria per tutti i nuovi modelli veicolo omologati a partire dal Luglio 2022), definisce una roadmap e gli obblighi per i Car Maker rispetto la cyber sicurezza. UNECE ha anche approvato una seconda regulation (R 156) che va a regolamentare, sempre nel campo automotive, la sicurezza nell'aggiornamento del software, con particolare attenzione alla modalità "over the air".
Come si diceva, la UNECE R 155, definisce una roadmap ed un insieme di requisiti. Dal punto di vista dei requisiti, la R 155, copre tutto il ciclo di vita del veicolo, partendo dal concept, passando per il design, la produzione, le operation, l'assistenza ed arrivando infine alla sua rottamazione. Si intuisce da quanto detto che l'impatto sul car maker, e su tutta la filiera dei fornitori è decisamente importante. Infatti, la normativa richiede che il costruttore automobilistico, coinvolga i suoi fornitori (passando in cascata i requisiti di cyber sicurezza) nel processo di sviluppo di una vettura "secure by design" e nel processo di "continuous monitoring" dei rischi e dei threat di sicurezza. Cosi come per ogni altro sistema digitale, per un

veicolo è necessario predisporre un sistema di sorveglianza attiva sui rischi e le vulnerabilità che dovessero manifestarsi sul prodotto una volta introdotto sul mercato.
Per dare linee guida uniformi sia ai costruttori di veicoli che ai loro fornitori su come implementare la cybersecurity sia nei processi aziendali e sia nei prodotti sviluppati, è stato definito ed approvato lo standard ISO/SAE 21434 Road Vehicles - Cybersecurity Engineering. Uniformarsi a questo standard garantisce una adeguata copertura della regulation R155. Un secondo standard, ISO 24089 (Road Vehicles – Software Update Engineering), che copre la parte relativa alla regulation R156 sul Software Update, è invece in corso di definizione da parte dell'ente normatore internazionale.

Threat Analysis and Risk Assessment (TARA)

Come definito e descritto nello standard ISO/SAE 21434 (4), il processo di analisi della cybersecurity di un prodotto automotive, deve seguire la metodologia denominata "Threat Analysis and Risk Assessment" (TARA), una metodologia utile per dettagliare tutte le possibili minacce (*threats*) a cui un prodotto può essere soggetto e assegnare a queste un livello di rischio basandosi su parametri, sempre descritti nello standard ISO/SAE 21434, che coprono l'ambito della safety, della privacy dell'utente, dell'impatto economico e dell'impatto sull'operatività del prodotto e del veicolo.

Questa analisi è necessaria per poter assegnare una priorità alle contromisure di Cybersecurity da implementare per rendere il sicuro un veicolo.
La TARA è una metodologia ingegneristica che ha l'obiettivo di identificare, dare priorità e rispondere alle minacce informatiche, attraverso l'applicazione di contromisure che riducono la suscettibilità agli attacchi digitali.
L'input principale di analisi è *l'Item Definition*, in cui vengono definite le caratteristiche principali del componente da proteggere, inclusi i suoi limiti, le interfacce e l'*Operational Environment*.
L'*Item Definition* è usato principalmente per determinare l'*Asset*, ovvero la proprietà che deve essere protetta dai rischi di cybersecurity (può trattarsi di un oggetto fisico, ad esempio un sensore o un firmware, oppure di una funzionalità).
L'*asset* è poi analizzato in modo da definire uno o più *Damage scenario*, ovvero condizioni che portano a un danneggiamento dell'*asset* e a conseguenze negative per l'utilizzatore finale.
Ogni *Damage Scenario* viene poi associato a uno o più *Threat Scenario*, che corrispondono a realizzazioni concrete di damage scenarios in cui le proprietà di un asset vengono attaccate e/o compromesse. Per ogni *Threat Scenario* (che deve prendere in esame tutti gli asset e damage scenarios identificati) viene calcolato un impatto basato sul tipo (ad esempio, se la minaccia potrebbe avere conseguenze negative sulla sicurezza o se può solo incidere su assetti finanziari o di operatività) e sulla gravità dei danni.
L'impatto dei threat scenario si collega anche al *Cybersecurity Assurance Level* (CAL), che è un indicatore dinamico dello sforzo necessario per garantire la sicurezza di un elemento, derivante dai rischi relativi a tutti i suoi asset.

Al fine di analizzare i passi necessari a un aggressore per attuare un damage scenario, e di quantificare i rischi relativi alle minacce, il percorso di attacco viene analizzato attraverso metodi descrittivi strutturati, come *l'Attack Tree Analysis* (ATA).
Questo rende anche più semplice calcolare l'*Attack Feasibility Rating*, anch'esso basato sulle caratteristiche dell'aggressore preso a modello (modelled attacker) (ad esempio posizione, competenza, finestra di opportunità etc.)
L'impact rating e l'attack feasibility rating vengono poi utilizzati per quantificare i rischi associati a ogni threat scenario. I rischi sono riportati su una scala discreta (tra 1 e 5) che indica il grado di gravità.
Al termine del processo TARA, viene impostato un trattamento di rischio per ogni threat scenario, in modo da determinare le azioni di cybersecurity necessarie per eliminare, ridurre, condividere o memorizzare i rischi.
Nell'ottica di un costruttore di veicoli, l'analisi potrebbe partire identificando ogni centralina come "item" da analizzare (ad esempio una centralina di controllo motore):

Item	Asset	Damage Scenario	Threat Scenario
Centralina controllo motore	Funzione per il controllo della coppia	Il motore non risponde alle richieste dell'utente	Un attaccante, sfruttando la possibilità della centralina di ricevere aggiornamenti, potrebbe compromettere l'integrità e l'autenticità dei parametri di configurazione del veicolo.

Dall'analisi di questo *threat* e prendendo in considerazione le tabelle ISO/SAE 21434 dove viene descritta la *severity* di un *threat* divisa per ogni categoria (Operational, Safety, Financial e Privacy), ci si ritrova con un rischio sull'operatività molto elevato dato che il veicolo non risponderebbe alle richieste dell'utente così come è stato impostato dal produttore a seguito di un processo di taratura e calibrazione. In più, se le conseguenze dell'attacco dovessero verificarsi mentre il veicolo è in moto, ad alta velocità ed in una strada molto trafficata, la severity risulterebbe molto alta anche nel campo della safety. Da non tralasciare anche il danno d'immagine, quindi finanziario, per l'azienda. Da questa analisi è facile intuire che delle contromisure di sicurezza dovranno essere implementate al fine di proteggere l'asset della funzione che controlla la coppia del motore ed i dati da essa utilizzati.
All'interno del processo di TARA è importante, inoltre, sviluppare un corretto modello di *risk framing* (un esempio può esser quello della figura successiva), che permetta di individuare il set di requisiti di sicurezza partendo dalle vulnerabilità, dai vettori di attacco e dall'analisi delle possibili tecniche ed obiettivi dell'attacco stesso.

Figura 7 - *Risk Framing*

Conclusa la parte di analisi dei rischi, si deve passare alla fase *di identificazione delle contromisure*, ovvero la definizione dei requisiti di sicurezza che faranno parte del "secure design" del sistema. La definizione corretta dei requisiti è una delle operazioni più delicate, e non solo perché la loro corretta identificazione permette di fornire al veicolo il giusto livello di protezione, ma anche perché ciascun requisito ha un diretto impatto sui costi di sviluppo e produzione. Il corretto *sizing* dei requisiti e delle contromisure deve essere allineato al livello di rischio accettabile da parte del produttore di veicoli.

Conclusioni

Dal punto di vista della sicurezza informatica, le vetture connesse, autonome e all'interno di ecosistemi evoluti (ITS, Intelligent Transport System) presentano gli stessi elementi di rischio di un qualunque oggetto (PC, telefono, server…) connesso alla rete Internet (Security and Privacy). Con l'ulteriore complicazione legata al fatto che ogni attacco su una vettura, può causare gravi conseguenze sull'incolumità di guidatori e passeggeri (Safety).

I potenziali rischi sull'ecosistema di mobilità e sulla salute pubblica hanno spinto il legislatore verso la definizione di una normativa cogente che mira ad aumentare l'attenzione rispetto al tema della cybersecurity dei veicoli. Il rispetto dell'applicazione delle best practice di sicurezza nella progettazione delle vetture ed il continuous monitoring degli attacchi e dell'insorgere di nuove vulnerabilità, diventano requisiti omologativi al pari, ad esempio, del rispetto dei requisiti sulle emissioni.

Le best practice di sicurezza (**Figura 8**) dovranno essere applicate a tutti gli ambiti che caratterizzano il ciclo di vita di una vettura. Dal design all'uscita dal mercato.

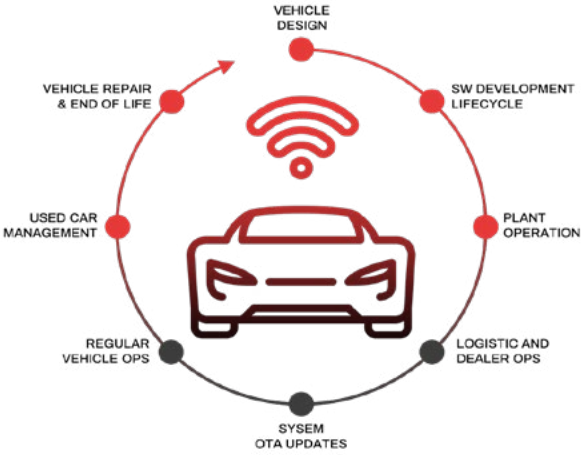


Figura 8 - *Automotive Security Best Practice*

Per dirla in breve, nuovi modelli di vettura non protetti dai rischi informatici non potranno più essere introdotti sul mercato a partire da Luglio 2022.

Referenze

(1) Good practices for security of smart cars – ENISA – Nov 2019
(2) Global Automotive cybersecurity report 2021 – Upstream Security
(3) Developing Cyber-Resilient Systems: A Systems Security Engineering Approach – Ross, Pillitteri, Graubart, Bodeau, McQuaid – Dec 2021 – NIST
(4) Standard ISO/SAE 21434 "Road vehicle cybersecurity engineering" – Nov 2021
(5) Information Sharing and Analysis Center (ISACs) - Cooperative models - ENISA – Feb 2018

L'importanza della incorporazione della Cybersecurity nelle strategie di Resilienza Operativa

[A cura di Federica Maria Rita Livelli]

Scenario

Gli ultimi due anni di pandemia - unitamente all'aumento esponenziale degli attacchi cyber e alla supply chain disruption - hanno insegnato alle organizzazioni quanto sia fondamentale e strategico conoscere a fondo, non solo il contesto interno, ma anche quello esterno, individuandone interconnessioni ed interrelazioni. Ovvero si tratta di superare i silos funzionali per considerare l'organizzazione come "uno, il tutto", in modo tale da andare oltre ai piani di ripristino e dimostrarsi operativamente resilienti e meglio preparate per le interruzioni.
Pertanto, urge sviluppare il "muscolo" della Resilienza Operativa in tutta l'organizzazione attraverso la comprensione, l'esecuzione e il mantenimento di un framework maggiormente strutturato e sinergico scaturito dalla implementazione dei sistemi di gestione di Risk Management, Business Continuity & Cybersecurity in modo tale che le persone, i processi ed i sistemi informativi possano essere in grado di anticipare, prevenire, rispondere/recuperare e adattarsi per far fronte alle mutevoli condizioni secondo un approccio *risk & resilience-based*.

Come conseguire la Resilienza Operativa

La Resilienza è oramai una priorità strategica per le organizzazioni. Inoltre, la Resilienza Informatica ricopre un ruolo fondamentale a fronte anche del processo accelerato di digitalizzazione e innovazione, dell'impiego sempre più diffuso di dispositivi Iot ed applicazioni di intelligenza artificiale.
Nella sua forma più semplice, la Resilienza può essere definita come la capacità di riprendersi a fronte di una crisi, incidente, interruzione o evento dirompente; mentre la Resilienza Operativa è la capacità di sostenere le operazioni aziendali durante qualsiasi evento più o meno dirompente, compreso un attacco informatico. Essa richiede una visione strategica e olistica oltre la necessità di intraprendere un viaggio *"sine die"* che mira a:

- Ridurre al minimo l'impatto di un'interruzione sugli stakeholder esterni e sull'economia in generale.
- Sapere dove si trovano le vulnerabilità della propria organizzazione e sviluppare quegli elementi fondamentali (i.e. Resilienza Informatica, Aziendale, di Terze Parti e Tecnologica) che contribuiscono ad una ripresa più rapida dell'organizzazione, riducendo al minimo i danni.
- Comprendere e gestire la propensione al rischio dell'organizzazione, o la tolleranza per una varietà di rischi a cui è esposta l'organizzazione.

Molte organizzazioni dispongono di programmi di Disaster Recovery e Business Continuity; tuttavia, ora si tratta di garantire la resilienza operativa che implica andar oltre le attività tattiche per garantire l'operatività dei sistemi e dei server, concentrandosi anche sui pro-

cessi di business supportati da tali sistemi e servizi. Si tratta, quindi, di mantenere i servizi aziendali in funzione durante qualsiasi tipo di evento oltre ad implicare la governance del programma, il cambiamento tecnologico per migliorare la fase di recupero e l'adozione di un cambiamento culturale per incorporare la Resilienza Operativa all'interno dell'organizzazione a 360 gradi.
Ogni organizzazione deve definire la propria "stella polare" di Resilienza Operativa partendo dalla definizione di cosa significa essere resilienti in modo tale che ogni stakeholder - interno ed esterno - sia in grado di lavorare nelle stessa direzione, indipendentemente dal ruolo e dalla funzione ricoperta, quale *conditio sine qua non* per avere una visione olistica degli ecosistemi operativi dell'organizzazione e del settore in cui opera.

Figura 1 - *Fonte: www.fusion.com – "La galassia della Resilienza Operativa"*

Cybersecurity vs. Resilienza Operativa

La gamma e la sofisticatezza delle minacce informatiche provenienti da stati nazionali, hacker e criminali organizzati, impattano profondamente sul modo in cui le organizzazioni raggiungono la Resilienza Operativa. Ne consegue che la Cybersecurity si converte, insieme al Risk Management e Business Continuity, in una leva strategica attraverso la quale le organizzazioni raggiungono questo obiettivo.
Le organizzazioni dovrebbero utilizzare la Cybersecurity per migliorare la Resilienza Operativa complessiva e, al contempo, rafforzare le tradizionali capacità di Business Continuity. È quanto mai necessario effettuare una revisione strutturata delle attuali strategie e roadmap

informatiche per garantire che i dati e i processi siano integrati con i sistemi di Risk Management, sia verticalmente che orizzontalmente.
Le buone pratiche di Cybersecurity dovrebbero permeare tutto ciò che riguarda la tecnologia in un'azienda considerando come le policy, le persone e i processi siano strettamente collegati tra loro, senza dimenticare la valutazione delle terze parti, creando in questo modo una cultura della consapevolezza informatica e garantendo la consapevolezza dell'utente finale attraverso la comunicazione e la formazione.

L'organizzazione va in analisi

Le organizzazioni, per dimostrare di avere una resilienza operativa in grado di far fronte alle minacce informatiche devono, oggigiorno, metaforicamente parlando, "andare in analisi".
Pertanto, ogni organizzazione dovrà necessariamente compiere diverse fasi atte a:

Conoscere il proprio business, ovvero cosa è importante e cosa è fondamentale, oltre ad individuare i punti di forza e di debolezza inerenti alla sicurezza informatica dell'organizzazione.

Analizzare in profondità il livello della propria Cybersecurity in termini di: asset digitali, valore aziendale da proteggere e potenziali attacchi hacker.

Garantire una buona gestione del rischio organizzativo e come integrare la componente di Cybersecurity, misurando gli impatti di eventi cyber sui processi/servizi critici tenendo in considerazione la risk tolerance definita dall'organizzazione.

Effettuare analisi di scenari e test in termini di abilità dell'organizzazione di rispettare i parametri di risk tolerance, documentando eventuali problematiche e tenendo traccia delle *lesson learned*.

Progettare ed attuare strategie di risposta e recupero e relativi piani da esercitare al momento del bisogno. Eventuali piani di crisi esistenti dovranno essere riesaminati e testati regolarmente per garantirne l'adeguatezza.

Garantire un approccio pragmatico ed iterativo atto ad acquisire la necessaria resilienza operativa, attuando i necessari cambi di paradigma a livello organizzativo ed operativo.

Attuare un processo di digitalizzazione ed innovazione armonico che presuppone mettere al centro le persone, dal momento che, troppo spesso, la Cybersecurity è caratterizzata come un'accelerazione nell'acquisizione di tecnologia, dimenticando che lo sviluppo della Resilienza Operativa si basa sia sul cambiamento culturale sia comportamentale di tutti gli attori coinvolti.

Garantire il commitment e coinvolgimento del Top Management in quanto un'efficace Resilienza Operativa dovrebbe venire dall'alto verso il basso.

Monitorare continuamente il Sistema di Resilienza Operativa ogni qual volta necessario, a fronte di cambiamenti organizzativi e di processo ed almeno una volta all'anno, effettuando periodicamente analisi di scenario.

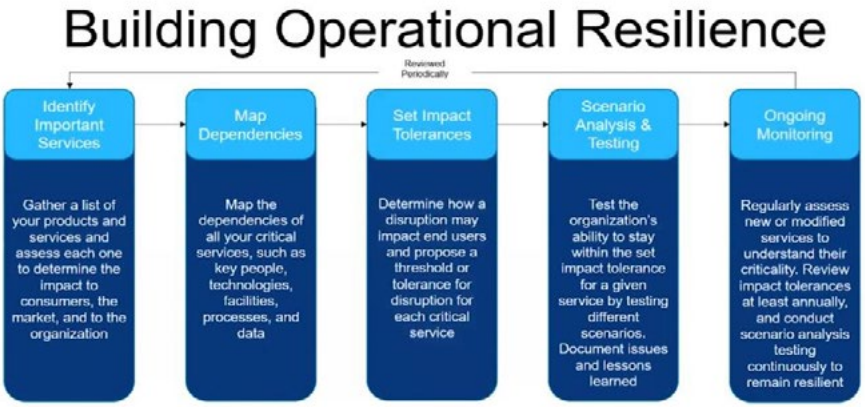


Figura2 - *Fonte: www.archer.com - Principali step per il conseguimento della Resilienza Operativa & Revisione periodica*

Solo attraverso una sinergica e strutturata interazione dei principi di Risk Management Business Continuity e Cybersecurity, i.e. quello che io definisco *"golden team"*, sarà possibile garantire altresì la governance e la compliance, rendendo l'organizzazione agile, anti-fragile ed adattiva ed in grado di garantire la Resilienza Operativa, superando i limiti di un approccio per *silos* - che rende i cambi di paradigma più gravosi e lenti - e riprogettando la struttura interna, i.e. il *modus operandi* e *pensandi* dell'organizzazione.

Figura 3 - *Fonte: FMRLivelli ©copyright 2022 – "Golden Team per la Resilienza Operativa"*

Un importante appuntamento

Le nuove regole e linee guida della FCA (*Financial Conduct Authority*), atte ad assicurare livelli sufficienti di resilienza operativa del settore finanziario entreranno in vigore il 31 marzo 2022. Inevitabilmente, tali regole sono destinate a diffondersi anche alle organizzazioni di servizi non finanziari, dal momento che tutti viviamo in una società strettamente connessa e come "vasi comunicanti" dobbiamo essere in grado di garantire il flusso operativo, o meglio l'eccellenza operativa, considerando l'ulteriore accelerazione della trasformazione digitale. Sfruttando il "filo digitale" comune - dall'ingegneria alle operazioni - che utilizza l'intelligenza delle prestazioni, sarà possibile migliorare l'agilità, l'affidabilità e l'efficienza, costruendo la Resilienza Operativa e, al contempo, la sostenibilità delle nostre organizzazioni.

Figura 4 - *Fonte: THE ICOR - www.build-resilience.org – Il framework della Resilienza Operativa*

Conclusioni

I tempi in cui viviamo comportano l'imprevedibile certezza dei rischi; pertanto, la Resilienza Operativa, attraverso piani di Business Continuity, Disaster Recovery e di emergenza che devono essere puntualmente testati, è il quadro necessario di cui dobbiamo disporre per mantenere la continuità aziendale durante qualsiasi circostanza imprevista. La Resilienza Operativa, come una "pozione" accuratamente "miscelata" di approcci, consentirà alle organizzazioni, alle persone, ai processi ed ai sistemi informativi di adattarsi ai mutevoli scenari in cui si trovano ad operare e, precisamente: un piano di Business Continuity (BCP) garantirà il ripristino della funzionalità dei sistemi di un'organizzazione; le misure di Cybersecurity proteggeranno l'organizzazione; i Piani di Disaster Recovery (DRP) consentiranno una risposta efficace agli inevitabili incidenti informatici. Inoltre, tutti nell'organizzazione dovranno essere sempre più consapevoli del ruolo importante da svolgere in termini di Cybersecurity, in quanto tale ruolo non può essere delegato unicamente a un team di professionisti IT.

GLOSSARIO

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

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

Botnet	Insieme di dispositivi (compromessi da *malware*) connessi alla rete utilizzati per effettuare, a loro insaputa, un attacco ad esempio di tipo *DDOS*.
Buffer overflow	Evento che ha luogo quando viene superato il limite di archiviazione predefinito di un'area di memorizzazione temporanea.
Business continuity	Soluzioni di natura tecnica ed organizzativa predisposte per garantire la continuità dell'erogazione di un servizio (eventualmente con uno SLA ridotto).
BYOD (Bring You Own Device)	Politica che consente l'uso di dispositivi personali anche per finalità aziendali.
CAL (Cybersecurity Assurance Level)	Indicatore dinamico dello sforzo necessario per garanzia la sicurezza di un elemento, derivante dai rischi relativi a tutti i suoi asset.
Captatore informatico	Software che viene immesso in dispositivi elettronici portatili al fine di intercettare comunicazioni o conversazioni tra presenti, il cui uso è specificatamente regolamentato dal Codice Penale, nel corso di indagini su alcuni specifici crimini.
Carding	Scambio e compravendita di informazioni riguardanti carte di credito, debito o account bancari, che vengono poi utilizzate per eseguire truffe di carattere finanziario acquistando beni o trasferendo fondi ai danni dei legittimi proprietari.
CEO Fraud	Tipi di attacco phishing mirati verso figure aziendali ad altissimo profilo, generalmente amministratori delegati, presidenti dell'azienda, direttori finanziari, etc.
CERT (Computer Emergency Response Team)	Struttura destinata a rispondere agli incidenti informatici e alla rilevazione e contrasto alle minacce. Fra i principali obiettivi di un CERT (vedi CERT Nazionale): - fornire informazioni tempestive su potenziali minacce informatiche che possano recare danno a imprese e cittadini; incrementare la consapevolezza e la cultura della sicurezza; cooperare con istituzioni analoghe, nazionali ed internazionali, e con altri attori pubblici e privati coinvolti nella sicurezza informatica promuovendo la loro interazione; - facilitare la risposta ad incidenti informatici su larga scala; - fornire supporto nel processo di soluzione di crisi cibernetica.

Cifratura "at rest" o "a riposo"	Cifratura dei dati nello storage.
Cifratura omomorfa	Tecnica utilizzata nell'ambito dell'e-voting. Con questo sistema di cifratura è possibile sommare due numeri cifrati o compiere altre operazioni algebriche senza decifrarli.
CISP **(Card-based Payment Instrument Issuing Service Provider)**	Prestatori di servizi di pagamento emittenti strumenti di pagamento basati su carta, che potranno emettere carte di debito a valere su conti di pagamento detenuti dai clienti presso Istituti di Credito diversi.
CLOSINT **(Close Source Intelligence)**	Processo di raccolta di informazioni attraverso la consultazione di fonti chiuse, cioè non accessibili pubblicamente: intelligence feed, fonti governative, informazioni classificate, etc.
Cloud weaponization	Tipo di attacco nel quale l'attaccante ottiene un primo punto d'ingresso nell'infrastruttura cloud attraverso la compromissione e il controllo di alcune machine virtuali. L'attaccante utilizza poi questi sistemi per attaccare, compromettere e controllare migliaia di altre macchine, incluse altre appartenenti allo stesso service provider cloud dell'attacco iniziale, e altre appartenenti ad altri service provider pubblici.
CNOs **(Computer Network Operations)**	Tipologia di *Information warfare* finalizzato all'attacco e distruzioni delle informazioni presenti sui sistemi informativi avversari, alla distruzione delle reti e dei sistemi stessi e alla difesa delle proprie.
CNP **(Card-Not-Present)**	Indica un pagamento effettuato senza la presenza fisica di una carta di pagamento, ad esempio su Internet.
CoA **(Courses of Action)**	Nella dottrina militare identifica un piano che descrive le strategie e le azioni operative scelte per portare a termine una determinata missione. Nell'ambito della *Cyber Intelligence* rappresenta le attività poste in essere rispettivamente dagli attaccanti o dai difensori per la conduzione o il contrasto delle azioni funzionali ad un attacco cyber.
Cognitive Securityg	Applicazione all'ambito della sicurezza delle soluzioni di Cognitive Computing.
Constituency	Nell'ambito di un *CERT* indica a chi è rivolto il servizio (ad esempio Pubblica Amministrazione Centrale, Regioni e Città metropolitane).

Context-based access	Tecnica che condiziona l'accesso alla valutazione dinamica del rischio della singola transazione, modulando eventuali azioni aggiuntive di verifica. Ad esempio le soluzioni di autenticazione e autorizzazione, sia nel caso di login che di disposizione di operazioni, non si limitano più ad autorizzare o bloccare un'operazione, ma offrono una gamma intermedia di possibilità, come ad esempio autorizzare un'operazione, ma con dei limiti, oppure richiedere verifiche aggiuntive.
C&C (Command &Control)	I centri di comando e controllo (C&C) sono quegli host utilizzati per l'invio dei comandi alle macchine infette (bot) dal *malware* utilizzato per la costruzione della *botnet*. Tali host fungono da ponte nelle comunicazioni tra gli host infetti e chi gestisce la *botnet*, al fine di rendere più difficile la localizzazione di questi ultimi.
Counterintelligence	Identificazione, valutazione, neutralizzazione e sfruttamento delle attività di intelligence svolte da entità avversarie.
Course of action matrix	Metodologia per l'identificazione, la prioritizzazione e la rappresentazione sinottica delle azioni da intraprendere, in caso di possibili intrusioni. È composta da: due azioni passive: Discover e Detect cinque attive - Deny, Disrupt, Degrade, Deceive, Destroy).
Credential Stuffing	Attacco nel quale vengono utilizzate coppie di user id/password raccolte in precedenza in modo fraudolento.
Cryptojacking	Processo che sfrutta illegalmente le risorse informatiche di una vittima per generare criptovaluta. In sostanza gli aggressori sottraggono potenza di calcolo installando un'applicazione di mining di criptovaluta sul sistema della vittima, che sia un PC o uno smartphone. La generazione di valuta virtuale, nota anche come criptovaluta, è molto dispendiosa in termini di potenza di elaborazione, motivo per cui gli aggressori devono infettare un vasto numero di vittime e utilizzarne la potenza di calcolo per generare nuove unità monetarie virtuali.
Cryptolocker	*Malware* che ha come finalità criptare i file presenti nel dispositivo infetto al fine di richiedere un riscatto alla vittima per renderli nuovamente intellegibili.

Cryptovaluta	Token digitale che costituisce uno strumento di pagamento. È possibile includere nei messaggi di pagamento ulteriori informazioni cosichè i token possono rappresentare digitalmente anche altri asset materiali o immateriali.
CTW (Check-the-Web)	Piattaforma tecnologiche appositamente creata in ambito *IRU* a supporto del monitoraggio e delle indagini nell'ambito di terrorismo in Internet, il cui ruolo principale è di anticipare e prevenire l'abuso terroristico di strumenti online, nonché di svolgere un ruolo consultivo proattivo a tale riguardo nei confronti degli Stati membri dell'UE e del settore privato.
CVSS versione 3 (Common Vulnerability Scoring System)	Sistema di valutazione delle vulnerabilità che fornisce un modo per acquisire le principali caratteristiche di una vulnerabilità e per produrre un punteggio numerico che rifletta la sua gravità, nonché una rappresentazione testuale di tale punteggio. Il punteggio numerico può quindi essere tradotto in una rappresentazione qualitativa (come bassa, media, alta e critica) per aiutare le organizzazioni a valutare e prioritizzare in modo adeguato i loro processi di gestione delle vulnerabilità. (https://www.first.org/cvss/specification-document)
CSIRT (Computer Security Incident Response Team)	Struttura sostanzialmente simile ad un *CERT*.
CTI (Cyber Threat Intelligence)	Disciplina che si occupa di raccogliere e analizzare dati eterogenei - provenienti da diverse sorgenti informative interne ed esterne -per estrarre informazioni utili a conoscere le caratteristiche dell'attore della minaccia, in modo da poter attribuire un profilo di rischio specifico per i propri asset e sviluppare azioni di contrasto efficaci. In particolare, le attività di CTI si esplicano attraverso un processo di raccolta, classificazione, integrazione e analisi di dati grezzi relativi a minacce che operano nel cyberspazio.
Cyber crime	Attività criminali effettuate mediante l'uso di strumenti informatici.

Cyber Diplomacy	"Incoraggiamo tutti gli Stati a impegnarsi in comportamenti rispettosi delle leggi e delle norme e che concorrano al rafforzamento della fiducia nel rispettivo uso delle TIC. Approcci collaborativi contribuirebbero anche a lottare contro l'uso del cyberspazio ad opera di attori non-Stato, a scopo terroristico e criminale". (Dichiarazione del G7 sul comportamento responsabile degli stati nel cyberspazio) www.esteri.it/mae/resource/doc/2017/04/declaration_on_cyberspace_ita.doc
Cyber espionage	Attività di spionaggio effettuata mediante l'uso di tecniche informatiche illecite.
Cyber intelligence	Attività volte a raccogliere e rielaborare informazioni al fine prevedere possibili minacce (non esclusivamente di natura informatica) agli asset oggetto di tutela.
Cyber Kill Chain	La cyber kill chain è un modello definito dagli analisti di Lockheed Martin come supporto decisionale rispetto alla rilevazione e risposta alle minacce. Esso include le seguenti fasi: reconnaissance, weaponization, delivery, exploitation, installation and persistence, command and control (C2), actions.
Cybersquatting	Attività volta ad appropriarsi di nomi di dominio di terzi, in particolare di marchi commerciali di rilievo, al fine di trarne profitto.
Cyber resilience	Capacità di un'organizzazione di resistere preventivamente o ad un attacco e di ripristinare la normale operatività successivamente allo stesso.
Cyber security	Gruppo di attività e competenze multidisciplinari, complesse e sofisticate, molte delle quali non informatiche, che sono oggettivamente di difficile integrazione con le prassi esistenti di gestione dell'ICT e di allocazione dei budget relativi, poiché la loro implementazione richiede di superare paradigmi tecnologici e silos organizzativi costruiti negli anni a partire da esigenze di compliance e da metodi e strumenti propri della sicurezza informatica "tradizionale". lo scopo complessivo di questo insieme di discipline è il proteggere tutti quegli asset materiali ed immateriali che possono essere aggrediti tramite il "cyberspazio" ovvero che dipendono da esso, garantendo allo stesso tempo la governance, l'assurance e la business continuity di tutta l'infrastruttura digitale a supporto.

Cyber-reasoning systems	Sistemi sviluppati per individuare automaticamente le vulnerabilità delle reti più complesse implementando algoritmi cognitivi.
Cyber-weapon	*Malware* (o anche hardware) progettato o utilizzato per causare danni attraverso il dominio cyber. (NATO Cooperative Cyber Defence Centre of Excellence).
CYBINT (Cyber Intelligence)	Disciplina che trae origine dalla declinazione classica delle attività di intelligence con riferimento alle peculiarità del dominio di ricerca informativa in ambito cyber. L'attività CYBINT si evolve includendo attività di analisi strategica e analisi di contesto su trend di eventi, scenari geopolitici e previsionali.
CVV2 (Card Verification Value 2)	Codice di sicurezza utilizzato sulle carte di pagamento.
Dark web	Parte oscura del World Wide Web, sottoinsieme del deep web, accessibile mediante l'uso di apposite applicazioni software.
Data Leakage	Trasferimento non autorizzato di informazioni riservate.
Data breach	La violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati. (Art. 4.12 GDPR) Alcuni possibili esempi: l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati; il furto o la perdita di dispositivi informatici contenenti dati personali; la deliberata alterazione di dati personali; l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.; la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità; la divulgazione non autorizzata dei dati personali. (Garante per la protezione dei dati personali)

DDoS (Distributed Denial of Service)	Attacchi *DOS* distribuiti, cioè basati sull'uso di una rete di apparati, costituenti in una botnet dai quali parte l'attacco verso l'obiettivo.
DDoS-for-hire	Letteralmente servizio DDoS da noleggiare.
Deep Fake	Algoritmi di deep learning in grado di creare foto o video falsi.
Deep Web	L'insieme dei contenuti presenti sul web e non indicizzati dai comuni motori di ricerca (Google, Bing…).
Defacement	Manipolazione del contenuto di una pagina web (tipicamente la home page) a scopi dimostrativi.
DES (Data Encryption Standard)	Algoritmo per la cifratura dei dati a chiave simmetrica.
DGA (Domain generation algorithms)	Algoritmo utilizzato da alcuni *malware* per la generazione di migliaia di nomi di dominio alcuni dei quali sono utilizzati dai loro server *C&C*.
Diamond Model	Framework strutturato per l'analisi tecnica di possibili intrusioni. (Adversary, Infrastructure, Victim, Capability).
Digital Scarcity	In una *blockchain* la capacità di rendere non riproducibili informazioni digitali come file o pagamenti.
Directory Traversal	
DNS (Domain Name System)	Indica sia l'insieme gerarchico di dispositivi, sia il *protocollo*, utilizzati per associare un indirizzo IP ad un nome di dominio tramite un database distribuito.
DNS cache poisoning	Tipo di attacco nel quale l'attaccante inserisce corrispondenze Indirizzo-IP alterate all'interno della cache del meccanismo di risoluzione degli indirizzi IP. Come risultato la cache userà l'indirizzo IP alterato in tutte le successive transazioni. L'indirizzo che comparirà nella barra URL di un browser sarà quello corretto e desiderato, ma il corrispondente indirizzo IP utilizzato sarà quello alterato e tutto il traffico di rete sarà quindi reindirizzato verso il sito replica controllato dai cyber criminali e nel quale si simulano log in per tracciare tutti i fattori di autenticazione inseriti.
DNS Open Resolver	Sistemi vulnerabili utilizzati come strumento per perpetrare attacchi informatici di tipo *DDOS* amplificati.

DNSSEC (Domain Name System Security Extensions)	Insieme di specifiche per garantire alcuni aspetti di sicurezza delle informazioni fornite dai *DNS*.
Dos (Denial of Service)	Attacchi volti a rendere inaccessibili alcuni tipi di servizi. Possono essere divisi in due tipologie: • applicativi, tesi a generare un numero di richieste maggiore o uguale al numero di richieste massimo a cui un server può rispondere (ad esempio numero di richieste web HTTP/HTTPS concorrenti); • volumetrici, tesi a generare un volume di traffico maggiore o uguale alla banda disponibile in modo da saturarne le risorse. Se vengono utilizzati più dispositivi per l'attacco coordinati da un centro di C&C si parla di *DDOS* (Destribuited Denial of Service).
Double extortion	Attacchi ransomware che, oltre a cifrare i file, ne fanno anche una copia di "sicurezza" con il loro trasferimento sui computer dei cyber criminali minacciando di procedere alla loro diffusione pubblica e/o metterli all'asta nel dark web per la vendita al miglior offerente.
Downloader	Software deputati a scaricare ulteriori componenti malevoli dopo l'infezione iniziale.
DPIA (Data Protection Impact Assessment)	Valutazione d'impatto sulla protezione dei dati. Una valutazione d'impatto sulla protezione dei dati è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli. (Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679)
Drive-by exploit kit	Il fenomeno dei drive-by *exploit kit* è particolarmente insidioso e si realizza inducendo l'utente a navigare su pagine web che nascondono attacchi, appunto gli *exploit kit*, per versioni vulnerabili di Java o dei plug-in del browser. Questi attacchi sono in grado di sfruttare macchine utente vulnerabili, impiantandovi malware, con la semplice navigazione sulle pagine malevole anche in assenza di interazione dell'utente con la pagina.

DRdos (Destribuited Reflection Denial of Service)	Sfruttando lo *spoofing* dell'indirizzo IP di una vittima, un utente malintenzionato può inviare piccole richieste ad un host vulnerabile inducendolo ad indirizzare le risposte alla vittima dell'attacco. Questa tipologia di *DDOS* permette al malintenzionato di amplificare la potenza del suo attacco anche di 600 volte, come dimostrato nel caso del *protocollo NTP*.
Dropper	Codice che installa il *malware* sul computer della vittima.
Dual use	I prodotti a duplice uso sono beni e tecnologie che possono avere un impiego sia civile che militare, includendo prodotti che possono in qualche modo servire nella fabbricazione di armi nucleari o di altri congegni esplosivi nucleari. (da Regolamento (CE) n. 428/2009 - regime comunitario di controllo delle esportazioni, del trasferimento, dell'intermediazione e del transito di prodotti a duplice uso)
Eavesdropping	Nell'ambito VOIP è un attacco del tutto simile al classico man-in-the-middle. L'attaccante si inserisce in una comunicazione tra due utenti con lo scopo di spiare, registrare e rubare informazioni
EDR (Endpoint Detection and Response)	Dispositivi la cui finalità è quella di mantenere un costante monitoraggio di eventi sospetti al fine di garantire una reazione preventiva e continua alle minacce.
eIDAS	REGOLAMENTO (UE) N. 910/2014 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE finalizzato a garantire il buon funzionamento del mercato interno perseguendo al contempo un adeguato livello di sicurezza dei mezzi di identificazione elettronica e dei servizi fiduciari.
Evasion	Nell'ambito delle applicazioni di IA attacco che consiste nel confondere la classificazione del dato in ingresso, da parte di un algoritmo precedentemente addestrato, manipolandone il contenuto.
E-voting	Con l'espressione "sistema di e-voting" ci si riferisce al momento in cui una tecnologia elettronica è impiegata in una o più fasi di un processo elettorale, scrutinio compreso, senza che sia necessariamente sfruttata la rete Internet.

Exploit	Codice con cui è possibile sfruttare una *vulnerabilità* di un sistema. Nel database Common Vulnerabilities and Exposures (cve.mitre.org) sono presenti sia le *vulnerabilità* note, sia i relativi exploit.
Exploit kit	Applicazioni utilizzabili anche da attaccanti non esperti, che consentono di sfruttare in forma automatizzata le *vulnerabilità* di un dispositivo (di norma browser e applicazioni richiamate da un browser).
Extended Vehicle	Tecnologia che consiste nel trasferire i dati di ogni veicolo, organizzati e strutturati, ai fini della loro condivisione, su dei server che rappresentano un'estensione, a terra, dei veicoli. Il concetto di "extended vehicle" è standardizzato dalla ISO 20077 "Road Vehicle - Extended Vehicle (ExVe) Methodology".
Fake news	Notizie destituite di fondamento relative a fatti od argomenti di pubblico interesse, elaborate al solo fine di condizionare l'opinione pubblica, orientandone tendenziosamente il pensiero e le scelte.
Fast flux	Tecnica che permette di nascondere i *DNS* usati per la risoluzione dei domini malevoli dietro ad una rete di macchine compromesse in continua mutazione e perciò difficili da mappare e spegnere.
FIDO2	Meccanismo di autenticazione avanzata che standardizza l'uso dei dispositivi di autenticazione per l'accesso ai servizi online, sia in ambiente mobile che desktop.
Fix	Codice realizzato per risolvere errori o *vulnerabilità* nei software.
GDPR	REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).
Ghost broking	Pratica secondo la quale il frodatore, spacciandosi per agente di un'impresa assicurativa, a seguito del pagamento di un "premio" rilascia al cliente una polizza assicurativa, ovviamente falsa.

GRE (Generic Routing Encapsulation)	Protocollo di tunneling che incapsula vari protocolli di livello rete all'interno collegamenti virtuali point-to-point.
GSR (General Safety Regulation)	REGOLAMENTO (UE) 2019/2144 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 novembre 2019 relativo ai requisiti di omologazione dei veicoli a motore e dei loro rimorchi, nonché di sistemi, componenti ed entità tecniche destinati a tali veicoli, per quanto riguarda la loro sicurezza generale e la protezione degli occupanti dei veicoli e degli altri utenti vulnerabili della strada…
Hacktivism	Azioni, compresi attacchi informatici, effettuate per finalità politiche o sociali.
Hate speech	Il Comitato dei ministri del Consiglio d'Europa definisce gli hate speech come le forme di espressioni che diffondono, incitano, promuovono o giustificano l'odio razziale, la xenofobia, l'antisemitismo o più in generale l'intolleranza, ma anche i nazionalismi e gli etnocentrismi, gli abusi e le molestie, gli epiteti, i pregiudizi, gli stereotipi e le ingiurie che stigmatizzano e insultano. RECOMMENDATION No. R (97) 20 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES ON "HATE SPEECH" - Adopted by the Committee of Ministers on 30 October 1997
Hit & Run (*o Pulse wave*)	Attacchi di breve durata, ma frequenti nell'arco di poche ore.
HMI (Human Machine Interface Systems)	Componente fondamentale dei sistemi IT industriali, che permette all'operatore umano di interagire con gli ambienti di controllo, supervisione e acquisizione dati (supervisory control and data acquisition - SCADA).
Honeypot	Letteralmente barattolo del miele. Indica un asset esca isolato verso cui indirizzare e raccogliere informazioni su eventuali attacchi, al fine di tutelare il reale sistema informativo.

HTTP POST DoS Attack	Attacco che sfrutta un difetto di progettazione di molti server web. L'attaccante inizia una connessione http del tutto lecita verso un server web andando ad abusare del campo 'Content-Lenght'. Visto che la maggior parte dei server web accetta dimensioni del payload del messaggio anche di 2Gb, l'attaccante comincia ad inviare il corpo del messaggio ad una ridottissima velocità (anche 1byte ogni 110 secondi). Ciò comporta che il server web resta in ascolto per molto tempo, lasciando aperti i canali http (del tutto leciti) andando quindi a saturare tutte le sue risorse visto che le connessioni restano aperte.
HUMINT (HUMan INTelligence)	Disciplina intelligence consistente nella ricerca ed elaborazione di notizie di interesse per la sicurezza nazionale provenienti da persone fisiche. Le sue specificità sono legate alla tipicità della fonte e si sostanziano soprattutto in particolari modalità di gestione. (Tratto da: Glossario intelligence – Il linguaggio degli Organismi informativi - www.sicurezzanazionale.gov.it)
Kill Switch	Termine generico per indicare un dispositivo che serve a bloccare in modo forzato un'attività.
IBAN Swapping	Sostituzione delle coordinate di pagamento IBAN o del wallet elettronico; questo ultimo caso soprattutto per i malware sui dispositivi mobili.
ICMP (Internet Control Message Protocol)	Protocolli che consentono ai dispositivi di una rete di comunicare informazioni di controllo e messaggi.
ICS (Industrial Control System)	Sistemi di controllo industriale.
IDS (Intrusion detection system)	Dispositivo in grado di identificare modelli riconducibili a possibili attacchi alla rete o ai sistemi.
IMEI (International Mobile Equipment Identity)	Codice univoco che identifica un terminale mobile
IMSI (International Mobile Subscriber Identity)	Codice univoco internazionale che combina SIM, nazione ed operatore telefonico.

Incident handling	Gestione di un incidente di sicurezza informatica. ENISA classifica le fasi di tale gestione in Incident report, Registration, Triage, Incident resolution, Incident closure, Post-analysis.
Information warfare	Insieme di tecniche di raccolta, elaborazione, gestione, diffusione delle informazioni, per ottenere un vantaggio in campo militare, politico, economico…
Infostealer	*Malware* finalizzato a sottrarre informazioni, quali ad esempio credenziali, dal dispositivo infetto.
Instant phishing	Tecnica di attacco nella quale nell'istante in cui l'utente inserisce le credenziali, o più in generale le informazioni all'interno del sito clone, il cyber criminale apre una sessione verso il vero sito della banca e utilizza, quasi in real time, queste informazioni per effettuare azioni dispositive.
Interception and Modification	Nell'ambito VOIP intercettazione di comunicazioni lecite tra utenti ed alterazione delle stesse con lo scopo di arrecare disservizi come l'abbassamento della qualità delle conversazioni e/o l'interruzione completa e continua del servizio.
Intrusion software	*Spyware* (definizione della Commissione Europea nell'ambito della regolamentazione dell'esportazione di prodotti *dual use*). Un "intrusion software", ad esempio, può essere utilizzato da una società di security per testare la sicurezza di un sistema informatico e al contempo essere usato da uno Stato non democratico per controllare e intercettare le conversazioni dei propri cittadini.
IoA **(Indicatori di attacco)**	Informazioni funzionali all'individuazione di un potenziale attacco anche prima che ci sia contatto diretto tra attaccante e attaccato.
IoC **(Indicatori di compromissione)**	Qualsiasi informazione che possa essere utilizzata per cercare o identificare sistemi potenzialmente compromessi (indirizzo IP/nome dominio, URL, file hash, indirizzo email, X-Mailer…) (Common Framework for Artifact Analysis Activities – ENISA)
IP Fragmentation	Tipo di attacco *DDOS* (Destribuited Denial of Service) che sfrutta il principio di frammentazione del protocollo IP.

IPMI (Intelligent Platform Management Interface)	Specifica di una interfaccia di basso livello utilizzata da diversi costruttori che consente ad un amministratore di sistema di gestire server a livello hardware. Attraverso la BMC (Baseboard Management Controller) consente, tra le altre cose, l'accesso al BIOS, ai dischi ed ai dispositivi hardware in generale e, di fatto, il controllo del server. IPMI contiene una serie di vulnerabilità ampiamente descritte e conosciute e, in definitiva, non dovrebbe essere aperto all'esterno.
IPS (Intrusion prevention system)	Dispositivo in grado non solo di identificare possibili attacchi, ma anche di prevenirli.
IRU (Internet Referral Unit di Europol)	Unità all'interno di Europol preposta a rilevare ed investigare i contenuti malevoli su internet e social media.
Keylogger	*Malware* (o dispositivi hardware) in grado di registrare quello che la vittima digita sulla tastiera (o altrimenti inserisce), comunicando tali informazioni all'attaccante.
MAAS (Malware as a Service)	Modello di erogazione del codice malevole dove un team di esperti "produce" malware, sviluppa exploits e si occupa della loro ricerca e sviluppo, mentre una catena di distributori si occupa di procacciare i clienti.
Malvertising	Tecniche che utilizzano l'ambito della pubblicità on line come veicolo di diffusione di *malware*.
Malware	Definizione generica di applicazioni finalizzate a arrecare in qualche modo danno alla vittima (ad esempio raccogliendo o intercettando informazioni, creando malfunzionamenti nei dispositivi sui quali sono presenti, criptando i file al fine di richiedere un riscatto per renderli nuovamente intellegibili…).
Man in the browser	Tecnica che consente di intercettare le informazioni trasmesse dalla vittima, quali le credenziali di accesso al sito di una banca, al fine di poterle riutilizzare.
Memcached	Software spesso usato sui server web per effettuare caching di dati e per diminuire il traffico sul database o sul backend. Il server memcached è pensato per non essere esposto direttamente su Internet, per questo nella sua configurazione di default non richiede autenticazione e risponde sia via TCP che via UDP.

MFA **(Multi-Factor Authentication)**	Autenticazione a più fattori, nella quale si combinano più elementi di autenticazione per rendere più complessa la compromissione del sistema.
MFU **(Malicious File Upload)**	Attacco ad un web server basato sul caricamento remoto di *malware* o più semplicemente di file di grandi dimensioni.
Mining	Creazione di nuova criptovaluta attraverso la potenza di calcolo degli elaboratori di una *blockchain*.
MitC **(Man in the Cloud)** *Definizione coniata dall'azienda Imperva*	Tipo di attacco nel quale la potenziale vittima è indotta a installare del software malevolo attraverso meccanismi classici come l'invio di una mail contenente un link a un sito malevolo. Successivamente il malware viene scaricato, installato, e ricerca una cartella per la memorizzazione di dati nel cloud sul sistema dell'utente. Successivamente, il malware sostituisce il token di sincronizzazione dell'utente con quello dell'attaccante.
Mix-nets schemi	Tecnica utilizzata nell'ambito dell'e-voting. Gli schemi di voto mix-nets sono sistemi basati su insiemi di server con cui è possibile crittare e permutare i voti espressi, in modo da rendere pressoché impossibile ricostruire la coppia voto-elettore.
Mules	Soggetti che consentono di "convertire" attività illegali in denaro (cash out) ad esempio attraverso attività di riciclaggio.
Netizen	Soggetto che partecipa attivamente alla attività su internet. Letteralmente cittadino della rete.
NIS **(Network and Information Security)**	DIRETTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.
NTP **(Network Time Protocol)**	*Protocollo* che consente la sincronizzazione degli orologi dei dispositivi connessi ad una rete.

OF2CEN (On line Fraud Cyber Centre and Expert Network)	Piattaforma in cui far confluire tutte le segnalazioni provenienti da banche e Forze di polizia su transazioni sospette che avvengono in Rete, in modo da poter analizzare e condividere in tempo reale ogni informazione e bloccare così le operazioni illegali. "Eu-of2cen" (European Union Online Fraud Cyber Centre Expert Network) è il progetto ideato dalla Polizia di Stato, gestito dalla Polizia postale e delle comunicazioni, e finanziato dall'Unione europea per il contrasto al cybercrime finanziario. (https://www.poliziadistato.it)
OPSEC (Operation Security)	Processo mediante il quale, durante un'operazione di intelligence, si previene l'esposizione involontaria di informazioni sensibili/riservate/classificate riguardanti le proprie attività, intenzioni o capacità.
Oracoli	Fonti esterne (API di un sito, output di un oggetto IoT…) alla *blockchain* per alimentare uno smart contract e scatenarne o influenzarne l'esecuzione.
OSINT (Open Source INTelligence)	Attività di intelligence tramite la consultazione di fonti aperte di pubblico accesso.
OT (Operation Technology)	Componenti hardware e software dedicati al monitoraggio ed alla gestione di asset fisici in ambito industriale, trasporti…
OTP (One Time Password)	Dispositivo di sicurezza basato sull'uso di password utilizzabili per una sola volta, di norma entro uno spazio temporale limitato.
Payload	Letteralmente carico utile. Nell'ambito della sicurezza informatica è la parte di un *malware* che arreca danni.
Password hard-coded	Password inserite direttamente nel codice del software.
Pharming	Tecnica che consente di indirizzare la vittima verso un sito bersaglio simile all'originale (ad esempio un sito bancario) al fine di intercettare ad esempio le credenziali di accesso.
PHI (Protected Health Information)	Informazioni personali relative alla salute fisica o mentale di una persona fisica, comprese le relative valutazioni, cure… ed i relativi pagamenti, indipendentemente dalla forma o dal media utilizzato per la loro rappresentazione.

Phishing	Tecnica che induce la vittima, mediante una falsa comunicazione in posta elettronica, a collegarsi verso un sito bersaglio simile all'originale (ad esempio il sito di una banca) al fine di intercettare informazioni trasmesse, quali le credenziali di accesso.
Phone hacking	Attività di hacking che ha come oggetto i sistemi telefonici; ad esempio mediante l'accesso illegittimo a caselle vocali.
Ping flood	Attacco basato sul continuo ping dell'indirizzo della macchina vittima. Se migliaia e migliaia di computer, che fanno parte di una *botnet*, effettuano questa azione continuamente, la vittima esaurirà presto le sue risorse.
Ping of Death	Attacco basato sull'inoltro di un pacchetto di ping non standard, forgiato in modo tale da mandare in crash lo stack di networking della macchina vittima.
PIR (Priority Intelligence Requirements)	Requisiti informativi che orientano le priorità nella pianificazione delle attività di intelligence.
PISP (Payment Initiation Service Provider)	Prestatori di servizi di disposizione di ordini che trasmettono un ordine di pagamento emesso da un cliente che detiene un conto online presso un Istituto di Credito a favore di un conto di un beneficiario o operatore commerciale (e-merchant).
Plausible Deniability	Capacità di un soggetto, in genere in posizione gerarchica elevata, di negare di essere a conoscenza di azioni dannose commesse da soggetti di livello più basso, in assenza di prove che possano dimostrare il contrario.
Poisoning	Nell'ambito delle applicazioni di IA attacco che consiste nel contaminare i dati di addestramento per impedire al sistema di funzionare correttamente.
Port Sweeping	Scansione di vari sistemi alla ricerca di una specifica porta in ascolto.
Price tracer	Software di tracciamento dei prezzi.
Protocollo di comunicazione	Insieme di regole che disciplinano le modalità con cui i dispositivi connessi ad una rete si scambiano informazioni.

PSD2 (**Direttiva sui servizi di pagamento nel mercato interno**)	DIRETTIVA (UE) 2015/2366 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE che stabilisce le regole in base alle quali gli Stati membri distinguono le varie categorie di prestatori di servizi di pagamento.
PSYOPs (**Psychological Operations**)	"Operazioni psicologiche" consistenti nel far giungere a comunità, organizzazioni e soggetti stranieri informazioni selezionate al fine di orientarne a proprio vantaggio opinioni e comportamenti. (Tratto da: Glossario intelligence – Il linguaggio degli Organismi informativi - www.sicurezzanazionale.gov.it)
Pulse Wave (*o Hit & Run*)	Hit & Run (o Pulse wave)
QTSP (**Qualified Trust Service Provider**)	Un *prestatore di servizi fiduciari* che presta uno o più servizi fiduciari qualificati e cui l'organismo di vigilanza assegna la qualifica di prestatore di servizi fiduciari qualificato.
Ransomware	*Malware* che induce limitazioni nell'uso di un dispositivo (ad esempio criptando i dati (crypto-ransomware), o impedendo l'accesso al dispositivo (locker-ransomware).
RDP (**Remote Desktop Protocol**)	Protocollo per la comunicazione remota fra computer (in particolare per le comunicazioni tra Terminal Server e il client Terminal Server).
Resilienza	"La capacità di un'organizzazione di assorbire gli shock e di adattarsi ad un contesto in continua evoluzione". Definizione da ISO 22316:2017
Resource ransom	Tecnica di attacco che nel mondo cloud consiste nel tentare di bloccare l'accesso a risorse nel cloud compromettendo l'account cloud pubblico della vittima e tentando di cifrare o limitare in altro modo l'accesso al maggior numero possibile di risorse cloud.
Retrieving data	Fase di ricerca e raccolta dei dati relativi all'obiettivo individuato durante un'attività *OSINT*. In questa fase gli analisti sfruttano i motori di ricerca, scandagliano i siti web alla ricerca di documenti di interesse avendo cura di conservare ogni traccia raccolta come ad esempio testi, URL, video, immagini, documenti, etc.

Rootkit	*Malware* che consente sia il controllo occulto di un dispositivo, sia di nascondere la presenza propria e di altri malware.
Sandboxing	Ambiente protetto nel quale è possibile testare applicazioni senza compromettere l'intero sistema informatico.
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.
SOCMINT (Social Media Intelligence)	Ramo dell'Open Source Intelligence specificatamente dedicato alla raccolta di informazione attraverso i social network.
SOP (Standard Operating Procedure)	Procedure operative standard che indicano i passi da seguire durante la conduzione di indagini *OSINT*, consentendo di rendere efficiente l'esecuzione di operazioni ripetitive e di ottenere uniformità nelle prestazioni, nella qualità degli output ed evitando il mancato rispetto di standard e normative di settore, eventualmente imposte dalla propria organizzazione.
Spear phishing	*Phishing* mirato verso specifici soggetti.
Spoofing	Modifica di una informazione, ad esempio l'indirizzo mittente di un pacchetto IP.
Spyware	*Malware* che raccoglie informazioni sul comportamento della vittima trasmettendole all'attaccante.
SQL injection	Tecnica di attacco basata sull'uso di query indirizzate a database SQL che consentono di ricavare informazioni ed eseguire azioni anche con privilegi amministrativi.
SSDP (Simple Service Discovery Protocol)	*Protocollo* che consente di scoprire e rendere disponibili automaticamente i dispositivi di una rete.
SSH (Secure Shell)	*Protocollo* cifrato che consente l'interazione remota con apparati di rete o di server permettendone, ad esempio, l'amministrazione.

STIX (Structured Threat Information eXpression)	Linguaggio strutturato che consente la descrizione e condivisione automatizzata di cyber threat intelligence (CTI) fra organizzazioni, utilizzando il protocollo *TAXII*.
Tampering	An intentional but unauthorized act resulting in the modification of a system, components of systems, its intended behavior, or data.
TARA (Threat Analysis Risk Assessment)	Metodologia utile per dettagliare tutti i possibili threat a cui un prodotto può essere soggetto e assegnare un rischio basandosi su parametri, sempre descritti nello standard ISO/SAE 21434, che coprono l'ambito della safety, della privacy dell'utente, dell'impatto economico e dell'impatto sull'operatività del prodotto e del veicolo.
TAXII (Trusted Automated eXchange of Indicator Information)	Protocollo che consente lo scambio (in HTTPS) di CTI (cyber threat intelligence) descritti mediante *STIX*.
TCP Synflood	Tipo di attacco nel quale tramite pacchetti SYN in cui è falsificato l'IP mittente (spesso inesistente) si impedisce la corretta chiusura del three-way handshake, in quanto, nel momento in cui il server web vittima invia il SYN/ACK, non ricevendo alcun ACK di chiusura, essendo l'IP destinatario inesistente, lascerà la connessione "semi-aperta". Con un invio massivo di pacchetti SYN in concomitanza ad un alto tempo di timeout delle connessioni, il buffer del server verrebbe presto saturato, rendendo il server impossibilitato ad accettare ulteriori connessioni TCP, anche se legittime.
TDM (Time-division multiplexing)	Tecnica che consente la condivisione, da parte di più dispositivi, di un canale di comunicazione per un tempo limitato predefinito.
Tecniche di amplificazione degli attacchi	Sfruttando lo *spoofing* dell'indirizzo IP di una vittima, un utente malintenzionato può inviare piccole richieste ad un host vulnerabile inducendolo ad indirizzare le risposte alla vittima dell'attacco. Ad esempio nel caso del *protocollo NTP* si può amplificare la potenza dell'attacco anche di 600 volte.

Tecniche di riflessione degli attacchi (DRDoS – Distributed Reflection Denial of Service)	La tecnica più diffusa sfrutta host esposti sulla Big Internet come riflettori del traffico a loro indirizzato sfruttando le *vulnerabilità* intrinseche ad alcuni protocolli quali *NTP* o *DNS*.
Telnet	Protocollo utilizzato per la gestione di host remoti, accessibile da riga di comando.
TLP (Traffic Light Protocol)	Protocollo per facilitare la condivisione delle informazioni "sensibili" che definisce il grado di possibile diffusione (red, amber, green, white) stabilito dalla controparte inviante.
TLS (Transport Layer Security)	Protocollo per la comunicazione sicura su reti TCP/IP successivo al SSL (Secure Sockets Layer).
TOR	Rete di dispositivi che consente l'uso dei servizi internet in modalità anonima (www.torproject.org).
Tradecraft	Combinazione di metodi, capacità e risorse che un attaccante sfrutta nel compimento delle proprie azioni.
Trojan horse	*Malware* che si installa in modo occulto su un dispositivo con diverse finalità, quali ad esempio raccogliere informazioni.
TSP (Trust Service provider)	Una persona fisica o giuridica che presta uno o più servizi fiduciari, o come *prestatore di servizi fiduciari qualificato* o come prestatore di servizi fiduciari non qualificato.
UBA (User Behavior Analytics)	Tecnologia atta ad apprendere il "normale" comportamento degli utenti di un sistema informativo mediante l'analisi di rilevanti quantità di dati (log…), e di segnalare successivamente il verificarsi di attività anomale messe in atto dagli stessi.
UDP Flood	Il *protocollo* UDP non prevede l'instaurazione di una connessione vera e propria e possiede tempi di trasmissione/risposta estremamente ridotti. Tali condizioni offrono maggiori probabilità di esaurire il buffer tramite il semplice invio massivo di pacchetti UDP verso l'host target dell'attacco.
UpnP (Universal Plug and Play)	*Protocollo* di rete che consente la connessione e condivisione automatica di dispositivi ad una rete.
VNC (Virtual Network Computing)	Strumento di condivisione del desktop da remoto.

Vetting	Il processo di identificazione dei partecipanti ad una *blockchain*.
VHUMINT (Virtual Human Intelligence)	Estensione al mondo virtuale del concetto di Human Intelligence, cioè di una metodologia investigativa imperniata sulla raccolta di informazioni per mezzo di contatti interpersonali. Attraverso la VHUMINT vi è dunque l'interazione proattiva con gli attori della minaccia al fine di raccogliere informazioni di contesto necessarie a mitigare efficacemente la minaccia.
Vishing	Variante "vocale" del *phishing*.
Volume Boot Record	Il VBR è una piccola porzione di disco allocata all'inizio di ciascuna partizione che contiene codice per caricare in memoria e avviare il sistema operativo contenuto nella partizione.
Vulnerabilità	Debolezza intrinseca di un asset (ad esempio un'applicazione software o un *protocollo* di rete) che può essere sfruttata da una minaccia per arrecare un danno.
Watering Hole	Attacco mirato nel quale viene compromesso un sito web al quale accede normalmente l'utente target dell'attacco.
Weaponization	Modifica di file e documenti per trasformali in vere e proprie armi per colpire i sistemi e gli utenti e per favorire l'installazione di codice malevolo.
Web Injects	Tecnica che consente di mostrare nel browser dell'utente informazioni diverse rispetto a quelle originariamente presenti sul sito consultato.
Whaling	Letteralmente "caccia alla balena"; è un'ulteriore specializzazione dello *spearphishing* che consiste nel contattare una persona interna all'azienda spacciandosi per un dirigente della stessa. Di solito si tratta di truffe finanziarie e il bersaglio è l'amministrazione con l'obiettivo di indurre la vittima a eseguire, con l'inganno, un pagamento a beneficio del truffatore.
XSS (Cross Site Scripting)	Vulnerabilità che sfrutta il limitato controllo nell'input di un form su un sito web mediante l'uso di qualsiasi linguaggio di scripting.
Zero-day attach	Attacco compiuto sfruttando *vulnerabilità* non ancora note/risolte.

Zero Trust	Paradigma i cui principi fondamentali sono: si assuma che l'ambiente sia ostile, non si distingua tra utenti interni ed esterni, non si assuma "trust" (da cui il nome), si eroghino applicazioni solo a device e utenti riconosciuti e autenticati, si effettuino analisi dei log e dei comportamenti utente. In pratica occorre trattare tutti gli utenti nello stesso modo, utenti della stessa azienda o esterni, che siano nel perimetro della rete aziendale o meno, che i dati a cui vogliono accedere siano dentro l'azienda o da qualche parte nel cloud.
Zoom bombing	Irruzione virtuale in una videoconferenza finalizzata a creare disturbo.

Gli autori del Rapporto Clusit 2022

Ivan Antozzi, ha conseguito la laurea magistrale in Ingegneria Informatica presso il Politecnico di Milano nel 2018. Un anno più tardi ha iniziato a lavorare negli Osservatori Digital Innovation occupandosi di trasformazione digitale e Cloud. Attualmente è ricercatore sui temi del Cloud e della Cybersecurity & Data Protection.

Walter Arrighetti, è esperto in *cyber threat intelligence* presso il Computer Emergency Response Team della Banca d'Italia. Ha conseguito la Laurea in Ingegneria Elettronica e un Dottorato di Ricerca presso l'Università degli Studi di Roma La Sapienza. Ha maturato nel tempo significative esperienze nella cybersecurity, nella sua più ampia accezione, avendo lavorato sia nel settore pubblico che in quello privato: dalla prevenzione e gestione diretta di incidenti, alla preparazione e conduzione di audit per conto di *major film studios*, sino alla *governance* e alla stesura di normativa. Collaborando con la Commissione Europea, l'Agenzia per l'Italia Digitale e l'Istituto Poligrafico e Zecca dello Stato, si è specializzato nella sicurezza di servizi fiduciari elettronici e identità digitali, italiane (SPID e CIE) ed europee. Ha al suo attivo numerose pubblicazioni, standard tecnologici e brevetti internazionali, e svolge regolarmente incarichi di docenza presso atenei italiani e statunitensi.

Mario Boemi, ha conseguito la Laurea Magistrale in Informatica presso l'Università degli Studi di Messina nel 2012. Vanta un'esperienza di circa 10 anni nel settore della Sicurezza Informatica, durante i quali si è specializzato in tematiche di Cyber Security in contesti CERT e SOC e acquisito certificazioni in ambito di gestione e risposta agli incidenti di sicurezza. Dal 2020 è Cyber Security Professional all'interno del gruppo CSIRT di Fastweb, dove si occupa attivamente di Incident Response, Cyber Threat Intelligence e Threat Hunting.

Laura Bongiorno, laureata in Fisica, è entrata in Fastweb nel 2000. Lavora nella funzione Security & Real Estate dal 2018, dove ha assunto prima la responsabilità della funzione Security by Design, poi anche la responsabilità della funzione Fraud Management. Da ottobre 2021 ha la reponsabilità di Incident e Fraud Management. Il mondo della gestione delle frodi la entusiasma e le permette di conciliare molte delle competenze acquisite e sviluppate in questi anni, dall'analisi dei casi all'analisi dei processi, alla valutazione del rischio frode, alla definizione dei controlli, insieme al suo team. Rilevante è la collaborazione con le funzioni aziendali impattate e con gli omologhi team antifrode del settore. Le esperienze sviluppate nell'ambito della Sicurezza Informatica la aiutano nella detection di fenomeni sempre più evoluti e che sfruttano modalità di attacco e strumenti propri del mondo cyber.

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 21 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.

Simone Ciccarone, lavora in Banca d'Italia dal 2015, prima nella Divisione Infrastrutture e Sicurezza, occupandosi di *IT risk analysis* e *pre-production security assessment*, e successivamente, dalla sua fondazione, nel Computer Emergency Response Team della Banca d'Italia dove si occupa di *cyber threat intelligence* e *security awareness*. Ha conseguito la Laurea Magistrale in Ingegneria Informatica, un corso universitario di perfezionamento in diritto penale dell'informatica e diverse certificazioni in ambito *cyber security*. È docente universitario a contratto presso la Libera Università Internazionale degli Studi Sociali Guido Carli (LUISS) e ha precedentemente svolto attività didattica presso l'Università Cattolica del Sacro Cuore e l'Università degli Studi di Roma Tor Vergata. È stato membro del Consiglio Direttivo dell'associazione IISFA (International Systems Forensics Association – Italian chpater). È autore di diverse pubblicazioni e ha partecipato in qualità di relatore a diversi seminari, anche a livello internazionale.

Francesco De Francesca, ricopre attualmente il ruolo di esperto in *cyber threat intelligence* presso il Computer Emergency Response Team della Banca d'Italia. Ha conseguito nel 2003 la laurea in Ingegneria Informatica presso l'Università della Calabria (UNICAL) e un Master universitario di secondo livello in Information & Communication Technology presso il CEFRIEL – Politecnico di Milano. Da oltre 15 anni si occupa di sicurezza delle informazioni per grandi aziende e Istituzioni, in cui ha ricoperto ruoli che spaziano dalla *security governance* alla *security operation*. Nella sua carriera ha svolto attività di *information security risk management*, ha gestito le certificazione di sicurezza dei processi aziendali rispetto a standard internazionali, ha condotto attività di audit, *risk assessment* e formazione, ha avviato e gestito processi di *incident management & response* e seguito la realizzazione di diversi progetti complessi e di piattaforme di sicurezza.

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.

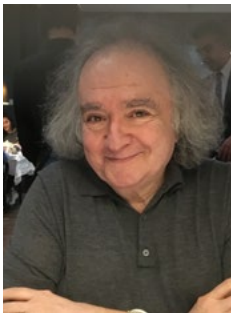
Pasquale Digregorio, è un ex-Ufficiale d'Accademia, attualmente Vice Capo Divisione del Computer Emergency Response Team della Banca d'Italia, dove mette al servizio dell'Istituto la sua esperienza in cyber intelligence e cybersecurity, sviluppata in 20 anni di servizio, svolti presso il Ministero della 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 e 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.

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. Ha recentemente conseguito l'Executive Master in Management presso il MIP Politecnico di Milano.

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. E' 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.

Giuseppe Faranda Cordella, ha esperienza nello sviluppo di prodotti elettronici da più di 30 anni, esperienza sviluppata in diverse società multinazionali del settore automotive. In particolare, è stato responsabile dello sviluppo sistemi di infotainment, di comunicazione e di security per diverse case automobilistiche. Nel 2017 ha fondato Drivesec srl, di cui è amministratore unico, con lo scopo di sviluppare soluzioni di sicurezza digitale per i sistemi IOT in generale, ed automotive in particolare.

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



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.

Sergio Inglima Modica, ha conseguito la Laurea Magistrale in Informatica presso l'Università degli Studi di Palermo nel 2016. Da sempre appassionato di Sicurezza Informatica, oggi ricopre il ruolo di Technical Analyst e Cyber Security Professional presso il gruppo CSIRT di Fastweb. Certificato nella gestione degli incidenti e delle minacce Cyber, segue e monitora eventi notevoli e nuovi vettori di attacco. Si occupa altresì delle tematiche di Threat Intelligence strutturando il processo di raccolta e verifica delle fonti d'intelligence.

Michele Lestingi, Enterprise Security Engineer presso il Security Operations Center di Fastweb, si occupa di consulenza in ambito sicurezza per i clienti Enterprise. Nella sua esperienza di oltre 10 anni nel settore ICT e Cyber Security, ha lavorato su progetti per le Forze dell'Ordine e in diversi Security Operation Centers in attività di ricerca, advisory e cyber defence. Possiede la certificazione CISSP ed è laureato in Informatica e Comunicazione Digitale presso l'Università degli studi di Bari. Collabora per il progetto di Sicurezza Digitale per la pubblica amministrazione del Team per la Trasformazione Digitale.

Federica Maria Rita Livelli, in possesso della certificazione Business Continuity - AMBCI BCI, UK e CBCP DRI, USA, Risk Management FERMA Rimap ®, consulente di Business Continuity & Risk Management, svolge attività di diffusione e di sviluppo della cultura della resilienza presso varie istituzioni ed università. È socia AIPSA (Italian Association of Security Managers) ed UNI (Italian Regulatory Institute). È membro de: Board del BCI Italy Chapter; Board ANRA; Advisory Board di LIUC-ODES Project; Advisory Board EU SIMARGL Project; Comitato Scientifico di CLUSIT; Conduct Professional Committee – BCI, UK; Judge at the International Organizational Resilience Awards; 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 dell'Associazione Donne 4.0 (Coordinatrice Commissione Reti) e Women for Security (Comitato Tecnico). Docente di moduli di introduzione di: ISO 22301 - Business Continuity & Resilience (Università POLIMI–BOCCONI e Università di Verona, Università di Cagliari, Master Ambientale Università di Padova, Università di Castellanza LIUC); ISO 31000 - Risk Management (Università Statale di Milano e Università di Castellanza, LIUC). Relatrice e moderatrice in diversi seminari, conferenze nazionali ed internazionali. Autrice di numerosi articoli su diverse riviste online.

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.

Pier Luigi Rotondo, è Technical Specialist per le soluzioni di Threat Management di IBM Italia. Ha contribuito a molti progetti internazionali su soluzioni per il Threat Management, l'Identity e l'Access Management, il Single Sign-on, e la Threat Intelligence. Con una laurea in Scienze dell'Informazione presso Sapienza Università di Roma, Pier Luigi è coinvolto in attività accademiche su temi di sicurezza delle informazioni in Corsi di Laurea e Master presso l'Università di Roma e di Perugia. Per conto di IBM Italia scrive articoli divulgativi, e contribuisce permanentemente dal 2015 al Rapporto Clusit sulla Sicurezza ICT in Italia sul cybercrime nel settore finanziario, presentando i risultati IBM e le tendenze del mercato della cyber security. È membro del Comitato Scientifico del CLUSIT.

Rodolfo Saccani, CTO in Libraesva, vive l'IT dal 1994. 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, siede nel board della European Hang-gliding and Paragliding Union, è expert presso il CEN (Comitato Europeo di Normazione) e partecipa alla stesura delle norme europee di certificazione delle attrezzature da volo libero.

Mirko Santocono, nato nel 1975, si laurea in Ingegneria delle Telecomunicazioni presso il Politecnico di Torino e l'università ParisTech in Francia. Ha iniziato la sua carriera nell'ambito della consulenza IT per poi orientare la sua attività nel Product Marketing, dopo un Master in Germania. Ha lavorato presso importanti player ICT dove ha maturato competenze sia in ambito tecnologico che business, principalmente per il segmento Enterprise. Entrato in Fastweb nel 2008, ricopre oggi il ruolo di responsabile Marketing nel team Product Design & Delivery per lo sviluppo dei servizi Security, Cloud e IoT.

Sofia Scozzari, appassionata di tecnologia da sempre, ha maturato oltre 15 anni di esperienza nella Cyber Security. Ha lavorato come System Administrator, ICT Consultant, Project Manager, Pre-sale, Cyber Security Consultant e Cyber Security Manager per principali società Italiane e multinazionali. Già CEO e COO di iDIALOGHI, società di consulenza e formazione in ambito Cyber Security, è stata anche co-founder di Security Brokers, cooperativa di Global Cyber Defense & Security Services. Da 4 anni risiede negli Emirati Arabi Uniti dove ha fondato e dirige Hackmanac, con cui elabora dati sulle minacce Cyber a supporto di attività di Threat Intelligence e Risk Management. È nel Comitato Direttivo di Women For Security, la Community delle Cyber Ladies italiane con cui partecipa ad iniziative a supporto della Cyber Security Awareness, dai corsi di formazione per scuole ed aziende ad eventi di settore. Membro del Comitato Scientifico CLUSIT, fin dalla prima edizione nel 2011 contribuisce come co-autore al Rapporto Clusit, curando l'analisi di migliaia di attacchi informatici ogni anno e diversi approfondimenti verticali. È inoltre autrice di diversi articoli e guide in tema di Cyber Security, e co-autrice dei paper «La Sicurezza dei Social Media» (2014, Oracle Community for Security), e «Blockchain & Distributed Ledger: aspetti di governance, security e compliance» (2019, CLUSIT). È infine speaker ad eventi e convegni di Cyber Security, sia in Italia che in UAE.

Girolamo Tesoriere, si è laureato in Ingegneria delle Telecomunicazioni presso il Politecnico di Bari. 10+ anni di esperienza nel settore delle TLC con una specializzazione nella consulenza sui servizi di Network Security e Cyber Security. Dopo aver lavorato per diversi anni come Technical Consultant in ambito networking e reporting operativo, nel 2013 partecipa allo start-up del Security Operations Center Enterprise di Fastweb. Ha lavorato per Eni come Cyber Security Engineer e al momento occupa la posizione di Enterprise Security Architect in Fastweb. Contribuisce allo sviluppo delle nuove soluzioni di sicurezza da erogare ai clienti TOP, grandi aziende e pubblica amministrazione.

Andrea Tomassi, ASRG Europe Leader & CISO, è Presidente e fondatore di ASRG Italian Chapter. Si è laureato in ingegneria delle telecomunicazioni presso l'Università degli studi Tor Vergata di Roma, con tesi svolta presso la Fondazione Ugo Bordoni. Professionista con più di venti anni di esperienza in ambito ICT, ha ricoperto ruoli differenti in aziende del settore per le quali ha realizzando progetti di Enterprise Security, Service Development, Automotive, Data Center & Cloud Architecture. Durante l'attività professionale ha conseguito le certificazioni: DPO, CISA, CDPSE, LA ISO 27001, LA 22301, LA Privacy e CCSK. Scrive frequentemente per riviste on line di settore.

Alessandro Vallega, Senior partner in Rexilience.eu da ottobre 2021, società che si occupa di cybersecurity. In precedenza, in Partners4Innovation (programmi di innovazione della capogruppo, scouting, acquisizioni, contratti di partnership, cybersecurity e GRC) e in Oracle EMEA con il ruolo di business development su sicurezza e 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 dodici pubblicazioni su diversi temi legati alla sicurezza (misure, rischio, frodi, ritorno dell'investimento, compliances, privacy, cloud, IA...) liberamente scaricabili dal sito Clusit (http://c4s.clusit.it). Al momento è impegnato nella produzione della 13esima pubblicazione che tratterà il tema del rischio in ambito digitale (previsto per marzo 2022). Contribuisce fin dal 2012 ai Rapporti Clusit sulla Sicurezza ICT in Italia. Insegna Analisi e gestione del rischio all'Università Statale di Milano e 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. E' 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 interna-

zionale in materia di Cyber Defense. È spesso chiamato come relatore a conferenze ed a tenere lezioni presso Università, sia in Italia che all'estero. Come docente Clusit tiene corsi di formazione su temi quali Cyber Crime, Mobile Security, Cyber Intelligence e Social Media Security, e partecipa come speaker alle varie edizioni del Security Summit, oltre che alla realizzazione di white papers (FSE, ROSI v2, Social Media) in collaborazione con la Oracle Community for Security. Fin dalla prima edizione (2011) del "Rapporto Clusit sulla Sicurezza ICT in Italia", si è occupato della sezione relativa all'analisi dei principali attacchi a livello internazionale, ed alle tendenze per il futuro.

Clusit
Associazione Italiana per la Sicurezza Informatica

Il Clusit, nato nel 2000 presso il Dipartimento di Informatica dell'Università degli Studi di Milano, è la più numerosa ed autorevole associazione italiana nel campo della sicurezza informatica. Oggi rappresenta oltre 600 organizzazioni, appartenenti a tutti i settori del Sistema-Paese.

Gli obiettivi

- Diffondere la cultura della sicurezza informatica presso le Aziende, la Pubblica Amministrazione e i cittadini.
- Partecipare alla elaborazione di leggi, norme e regolamenti che coinvolgono la sicurezza informatica, sia a livello nazionale che europeo.
- Contribuire alla definizione di percorsi di formazione per la preparazione e la certificazione delle diverse figure professionali operanti nel settore della sicurezza.
- Promuovere l'uso di metodologie e tecnologie che consentano di migliorare il livello di sicurezza delle varie realtà.

Le attività e i progetti in corso

- Formazione specialistica: i Webinar CLUSIT.
- Ricerca e studio: Premio "Innovare la Sicurezza delle Informazioni" per la migliore tesi universitaria arrivato alla 17a 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 Cybersecurity), ITU (International Telecommunication Union), OCSE, UNICRI (Agenzia delle Nazioni Unite che si occupa di criminalità e giustizia penale), le principali Associazioni Professionali del settore (ASIS, CSA, ISACA, ISC², ISSA, SANS) e le associazioni dei consumatori.

Security Summit è il più importante appuntamento italiano per tutti coloro che sono interessati alla sicurezza dei sistemi informatici e della rete e, più in generale, alla sicurezza delle informazioni.
Progettato e costruito per rispondere alle esigenze dei professionals di oggi, Security Summit è un convegno strutturato in momenti di divulgazione, di approfondimento, di formazione e di confronto. Aperto alle esperienze internazionali e agli stimoli che provengono sia dal mondo imprenditoriale che da quello universitario e della ricerca, il Summit si rivolge ai professionisti della sicurezza e a chi in azienda gestisce i problemi organizzativi o legali e contrattuali dell'Ict Security.
La **partecipazione è libera e gratuita**, con il solo obbligo dell'iscrizione online.
Il Security Summit è organizzato dal Clusit e da Astrea, agenzia di comunicazione ed organizzatore di eventi di alto profilo contenutistico nel mondo finanziario e dell'Ict.
Certificata dalla folta schiera di relatori (più di 700 sono intervenuti nelle scorse edizioni), provenienti dal mondo della ricerca, dell'Università, delle Associazioni, della consulenza, delle Istituzioni e delle imprese, la manifestazione è stata frequentata da oltre 18.000 partecipanti, e sono stati rilasciati circa 14.000 attestati validi per l'attribuzione di oltre 46.000 crediti formativi (CPE).

L'edizione 2022

La 14esima edizione del Security Summit parte con una edizione tutta in streaming, che si terrà dal 15 al 17 marzo. Nella seconda parte dell'anno si terranno altri 2 Security Summit, presumibilmente in presenza, a Roma e Verona. Continuano gli **Atelier della Security Summit Academy**, che si terranno tutto l'anno. Continueranno anche gli **Eventi Verticali** programmati in maggio (Energy & Utilities), giugno /Health Care), settembre (Finance) e ottobre (Manufacturing). Tra i temi più in evidenza per il 2022: 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

SECURITY SUMMIT

www.securitysummit.it