Nuova edizione
ottobre 2022

Rapporto

2022

sulla sicurezza ICT
in Italia

SECURITY SUMMIT

Indice

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

Prefazione

I primi sei mesi di quest'anno sono stati mesi molto critici per pubbliche amministrazioni e aziende.

La guerra e in generale le tensioni internazionali hanno portato alla crisi energetica e a una situazione di paura e incertezza come non si vedeva da decenni.

Come era previsto gli attacchi classificati come information warfare sono aumentati notevolmente e se anche in Italia non abbiamo avuto casi di particolare gravità l'attenzione è ai massimi livelli.

Come CLUSIT appoggiamo e supportiamo tutte le Autorità coinvolte nella difesa del Paese perché mai come in questo periodo serve coesione e supporto.

Anche per questo motivo abbiamo promosso la sottoscrizione di un Protocollo di Intesa con L'Autorità Garante per la Protezione dei Dati Personali, e di questo ringrazio il Presidente Pasquale Stanzione, che presenteremo nell'ambito del Security Summit Streaming Edition, alle ore 16.00 del 10 novembre e abbiamo richiesto di poterci associare al Centro di Competenza Italiano sulla cyber security Cyber 4.0, dal quale siamo stati accolti, e di questo ringrazio il Presidente Prof. Leonardo Querzoni.
Porteremo competenze, capacità di ricerca, anche in collaborazione con l'Osservatorio Cybersecurity & Data Protection del Politecnico di Milano, capacità formativa e divulgativa.

Noi siamo convinti che le collaborazioni istituzionali e le sinergie fra associazioni e centri di competenze siano fondamentali per fare progredire il paese e ci stiamo impegnando per fare la nostra parte.

Auspichiamo anche che il nuovo Governo mantenga la massima attenzione sui temi della cyber security e siamo certi che tutto quanto necessario sarà fatto a supporto dei cittadini, della Pubblica Amministrazione e del tessuto imprenditoriale.

La situazione è difficile e dopo gli anni del covid e ora quasi un anno di guerra in Europa il rischio è lo sfinimento.
E invece bisogna resistere perché come tutti i periodi bui della storia, anche questo finirà.

Un'ultima cosa: fra poco più di un mese verrà eletto il nuovo Consiglio Direttivo dell'Associazione.
Tutti i soci sono invitati a candidarsi e ad assumere un ruolo attivo.

Abbiamo bisogno di tutti.

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.
I dati del primo semestre 2022 confermano da un lato le previsioni in merito alla crescita dei casi di Information Warfare ma anche la tendenza a una sempre maggiore gravità dei casi che ci troviamo ad analizzare.

L'Europa è al centro del fenomeno, anche sul cybercrime in senso stretto, anche se probabilmente le medie sono un po' falsate dall'esistenza di paesi che tendono a non far conoscere i casi che accadono.

Sicuramente anche in Europa e in Italia non tutti i casi gravi vengono conosciuti ma più probabilmente sono i casi afferenti ad aziende medio piccole che tendono a non essere divulgati anche per assenza di eco mediatica.

Insomma, uno scenario che resta critico e che come scritto pochi mesi fa non può che considerarsi strutturale.

La speranza è che le tensioni internazionali e soprattutto la guerra finisca al più presto.
Nel frattempo, serve massima attenzione, massima protezione e massima conoscenza dei rischi da parte di tutti.

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 relativo al primo semestre 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

Il Rapporto, come di consueto, inizia con una panoramica degli incidenti di sicurezza più significativi avvenuti a livello globale nel primo semestre 2022, confrontandoli con i dati raccolti nei 4 anni precedenti.
Nel primo semestre 2022 abbiamo registrato **1.141 attacchi** (**+8,4%** rispetto al primo semestre 2021) con una impressionante media di **190 attacchi al mese** (era di 171 l'anno scorso).
Il conflitto europeo si rispecchia decisamente anche nel mondo cyber: il **Cybercrime** è sempre la principale causa di cyber attacchi, ma per la prima volta dal 2018 scende percentualemente sotto l'80% causando il **78%** del totale degli attacchi dei primi 6 mesi (era l'86% nel 2021).
Come ci aspettavamo crescono **Espionage / Sabotage** (**13%**, +2% rispetto al 2021) e **Information Warfare** (**5%**, +3%).
Cresce leggermente anche il fenomeno dell'**Hacktivism** (**3%**, +2%), sfruttato spesso per rivendicazioni da parte di hackitivisti a supporto del conflitto bellico.
Multiple targets torna ad essere il settore più colpito (**22%**, +9% rispetto al 2021), seguito da **Healthcare** (**12%**), Gov / Mil / LE (**12%**) e **ICT** (**11%**).
Crescono gli attacchi verso i settori **Financial / Insurance** (**9%**, +2%), **Manufacturing** (**6%**, +2%) e **News / Multimedia** (**5%**, +2%).
Aumentano (come ci aspettavamo) gli attacchi verso l'**Europa** (**26%**, +5% rispetto al 2021, record assoluto), mentre scendono in percentuale quelli verso l'**America** (**38%**, -7%, anche questo un record).
Crescono nuovamente anche gli attacchi verso **location multiple** (**26%**, +7%), mentre scendono quelli verso **Asia** (**8%**, -4%) e **Oceania** (**1%**, -1%).
Il **Malware** si riconferma la prima tecnica di attacco, ma per la prima volta dal 2018 scende sotto la soglia del 40% (**38%**, -3% rispetto al 2021).
Seguono le **tecniche sconosciute** (**22%**, +1%), **Phishing / Social Engineering** (**13%**, +3%) e lo sfruttamento delle **Vulnerabilità** (**11%**, -5%).
Aumenta rispetto all'anno scorso il ricorso a **tecniche multiple** (8%, +3%) e **DDoS** (**4%**, +2%).
La distribuzione della Severity degli attacchi resta sostanzialmente invariata: sono **Critici** oltre un terzo degli attacchi (**33%**, +1%), mentre quasi la metà (**45%**, -2%) hanno una gravità **Alta**.

In conclusione, gli attacchi sono meno mirati rispetto all'anno scorso, ma sempre in crescita e, il fatto che aumentino tutti i fattori "multipli" (Multiple Targets, Multiple Techniques, Several/Multiple locations), ci fa capire che diventano più complessi, mantenendo alto il fattore di rischio evidenziato dalla Severity.
Segue, nel Rapporto, l'evoluzione degli attacchi in Italia, che è ben rappresentata dalle rilevazioni e segnalazioni della **Polizia Postale e delle Comunicazioni**, che ci hanno fornito dati e informazioni estremamente interessanti su attività ed operazioni svolte nel corso dei primi sei mesi del 2022

Il conflitto tra Russia e Ucraina sta avendo un impatto molto rilevante sulla vita di tutti noi e non poteva mancare un'analisi su **Geopolitica e Cybersecurity,** che cercasse di aiutarci a comprendere come la guerra informatica si inserisce a supporto della guerra convenzionale e delle strategie politiche dei singoli Stati.
Anche quest'anno abbiamo chiesto ad Experis, una società che si occupa di ricerca e selezione del personale, di fotografare la situazione e le tendenze nel settore della Cybersecurity. che emerge dalla loro analisi, intitolata "Profili Cyber ultra-specializzati e nuovi trend del mercato del lavoro (Ultra-specializzazioni, RAL crescenti e strategie di attraction e retention delle aziende)", è di sicuro interesse per tutti gli operatori ed i professionisti del settore.

Questi sono infine i temi trattati nella sezione FOCUS ON:

- **"Operation Technology Security – Ultima chiamata"**, a cura di Fortinet
- "**Effetti della guerra sulla sicurezza delle Infrastrutture Critiche**" - una questione di cyber resilience quale calibrata sintesi di risk management, business continuity & cybersecurity, a cura di Federica Maria Rita Livelli.

Inauguriamo con questa edizione del Rapporto una nuova sezione, dedicata agli attori istituzionali (Autority, Agenzie, Forze dell'Ordine e Centri di Competenza) con cui il Clusit ha stretto accordi operativi per:diffondere la cultura della sicurezza informatica presso le Aziende, la Pubblica Amministrazione e i cittadini. Il format utilizzato per questa sezione è quello dell'intervista.
Iniziamo quindi con **un'intervista al Prof. Leonardo Querzoni, presidente del centro di competenza italiano sulla cybersecurity CYBER 4.0**

Analisi dei cyber attacchi a livello globale più significativi del periodo 2018-2021 e del primo semestre 2022

Introduzione

In questo aggiornamento del Rapporto CLUSIT, giunto al suo undicesimo anno di pubblicazione, analizziamo i **1.141** cyber attacchi noti che abbiamo individuato e classificato a livello globale (Italia inclusa) nel primo semestre 2022 e li confrontiamo con quelli del quadriennio precedente[1].
Nell'ambito di questa ricerca, in 11 anni abbiamo identificato, classificato e valutato oltre **15.000** attacchi informatici gravi. Di questi oltre la metà (**8.285)** si sono verificati negli ultimi 4 anni e mezzo, a causa di un'accelerazione impressionante delle minacce cibernetiche.
La metodologia utilizzata per svolgere questa analisi è stata raffinata e 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. Inoltre, a partire da quest'anno, le tassonomie utilizzate per classificare i dati sono state completamente riviste, ampliate e aggiornate per aderire quanto più possibile a standard riconosciuti a livello internazionale.
In particolare il sistema di classificazione delle **vittime** ora si basa su settori merceologici derivati 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 del triennio 2018-2020 (**5.095**) per renderli confrontabili con quelli del 2021 (**2.049**) e del primo semestre 2022 (**1.141**) 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 2021

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 e 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 e information warfare, che tendono ad essere condotti con grande cautela e pertanto 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 e gli effetti globali del *climate change*.
Lo scopo originario per il quale è nato questo lavoro era dunque di elevare la consapevolezza e migliorare la comprensione del pubblico italiano rispetto all'evoluzione delle minacce cibernetiche, nell'ipotesi (poi dimostratasi drammaticamente esatta) che il problema sarebbe inevitabilmente degenerato con grande rapidità nei mesi e anni successivi, e che la pressoché totale mancanza di sensibilità in materia fosse *una delle principali ragioni* del peggioramento degli scenari.
Questa finalità rimane ancora oggi assolutamente centrale, ma data la criticità della situazione che si è venuta a creare nel frattempo, e considerati i rischi sistemici, esistenziali

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

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

che oggi incombono sulla nostra *civiltà digitale* a causa della crescita straordinaria delle minacce cibernetiche, siamo convinti che innalzare la consapevolezza 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 già 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, anche in base alle diverse tecniche utilizzate.
L'obiettivo è quello 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 *qualitativa* delle dinamiche in atto.

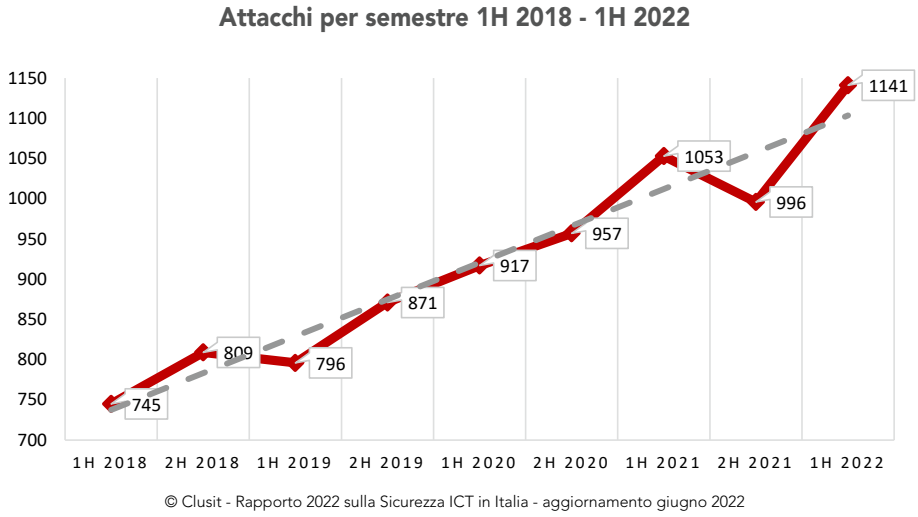
2022, "guerra globale cibernetica"

Anticipando alcune delle conclusioni che seguono possiamo affermare che se il 2021 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 primo semestre 2022.
Osservando la situazione dal punto di vista quantitativo, confrontando i numeri del primo semestre 2018 con quelli del 2022 la crescita degli attacchi è stata del **53%** (da 745 a 1.141). In 4 anni e mezzo la media mensile di attacchi gravi a livello globale è passata da 124 a **190**.
Oltre alla maggiore frequenza, la valutazione della Severity media di questi attacchi (indice di gravità degli attacchi analizzati) 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, al quale evidentemente non è corrisposto un incremento sufficiente delle contromisure adottate dai difensori.
Come abbiamo scritto commentando i dati del 2021, "siamo di fronte a problematiche che per natura, gravità e dimensione travalicano costantemente i confini dell'ICT e della stessa Cyber Security, e hanno impatti profondi, duraturi e sistemici su ogni aspetto della società, della politica, dell'economia e della geopolitica".
Nel primo semestre 2022 a queste dinamiche si è aggiunta la guerra in corso tra Russia e Ucraina, che ha scoperchiato un vaso di Pandora di capacità cibernetiche offensive, utilizzate dai contendenti, dai loro alleati e in generale da tutti i principali attori globali, sia a supporto di attività di cyber-intelligence che di cyber-warfare, in un contesto di guerra "calda" ai confini dell'Europa e di crescenti tensioni internazionali. Questo processo di ra-

pida adozione e messa in campo di strumenti cyber-offensivi sofisticati sarà difficilmente reversibile, e in prospettiva potrebbe causare conseguenze di inaudita gravità.
Riassumendo le nostre impressioni sulla situazione attuale, potremmo affermare che "la guerra globale cibernetica" è cominciata. Oltre agli ingenti danni causati dal cybercrime, d'ora in poi le infrastrutture critiche e molti altri sistemi digitali, meno tutelati a livello normativo ma comunque essenziali per la collettività, saranno bersagli designati, costantemente al centro del mirino di numerosi attori, governativi e non.
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 che 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 salda, che non accetti compromessi e pressioni esterne, e (finalmente) la valorizzazione delle risorse umane con competenze cyber (in termini di talenti e di esperienze) del Paese, e il loro sviluppo in termini quantitativi e qualitativi.
Confidando che anche quest'anno il Rapporto CLUSIT possa apportare un contributo significativo al dibattito nazionale in merito all'accelerazione crescente delle problematiche globali di sicurezza cibernetica e alle sue ricadute sul benessere del Paese, auguriamo a tutti una buona lettura.

Analisi dei principali cyber attacchi noti a livello globale del 2018-2021 e del primo semestre 2022

In questa sezione, come di consueto, offriamo una panoramica degli incidenti di sicurezza più significativi avvenuti a livello globale nel primo semestre 2022, confrontandoli con i dati raccolti nei 4 anni precedenti[6].
Complessivamente al 30 giugno 2022 il nostro database è costituito da **15.151** 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.

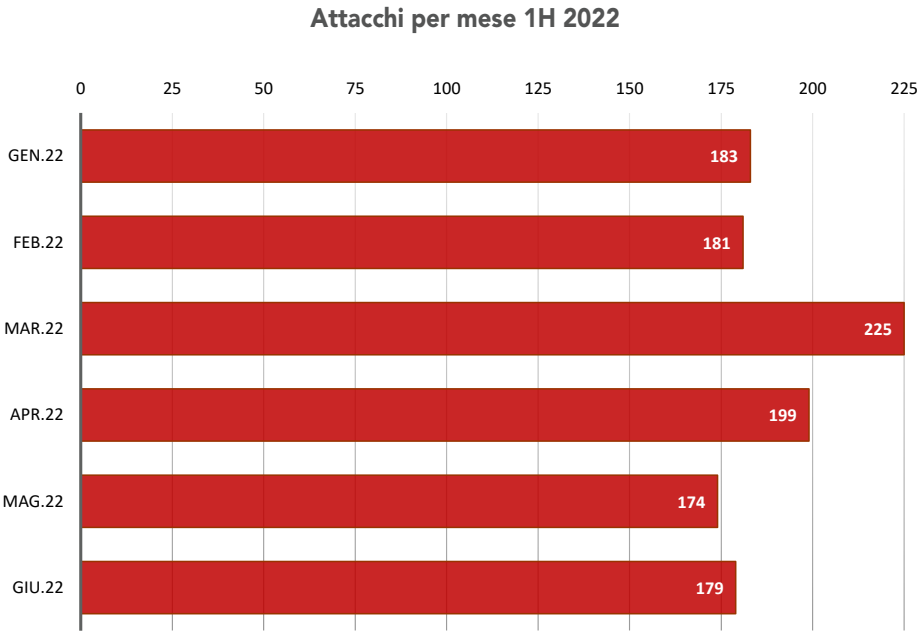


© Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia - aggiornamento giugno 2022

Il campione che esaminiamo nelle pagine seguenti comprende **8.285** attacchi, classificati tra il gennaio 2018 e il giugno 2022 (oltre la metà del totale su 11 anni), di cui **1.874** nel 2020, **2.049** nel 2021 e **1.141** nel 1H 2022, con una media complessiva di 153 attacchi al mese nell'intero periodo considerato (erano 39 nel 2011, 130 nel 2018, 171 nel 2021 e sono 190 nel primo semestre 2022). Il picco massimo di sempre si è avuto a marzo 2022 (225 attacchi).

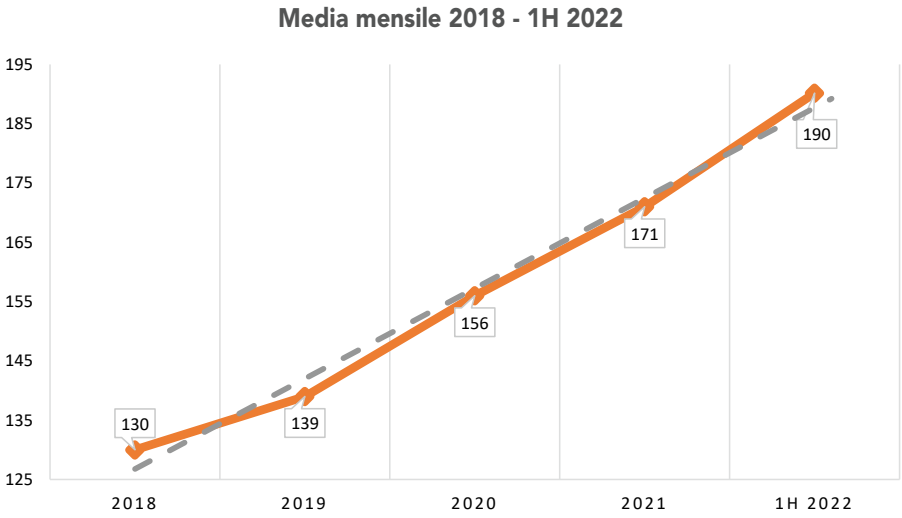
[6] pur avendo iniziato questa ricerca nel 2011, oggi ha poco senso fare confronti con gli anni precedenti al 2018

Questa la distribuzione mensile degli attacchi registrati nel primo semestre 2022.



© Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia - aggiornamento giugno 2022

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



© Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia - aggiornamento giugno 2022

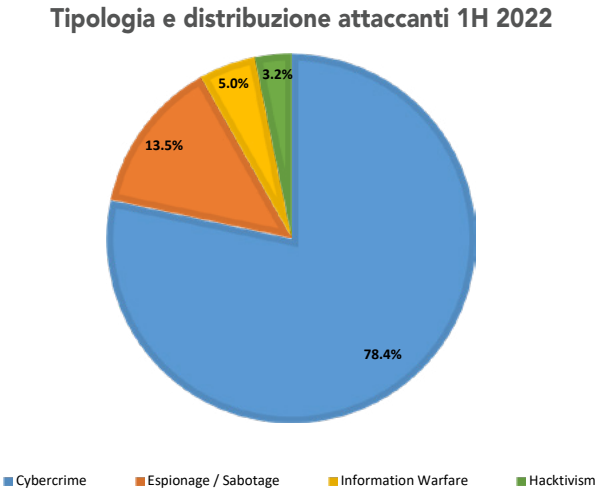
Le tre tabelle e i grafici seguenti rappresentano una sintesi dell'analisi dei dati che abbiamo raccolto. Come in passato abbiamo evidenziato nella colonna più a destra le tendenze osservate.

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.

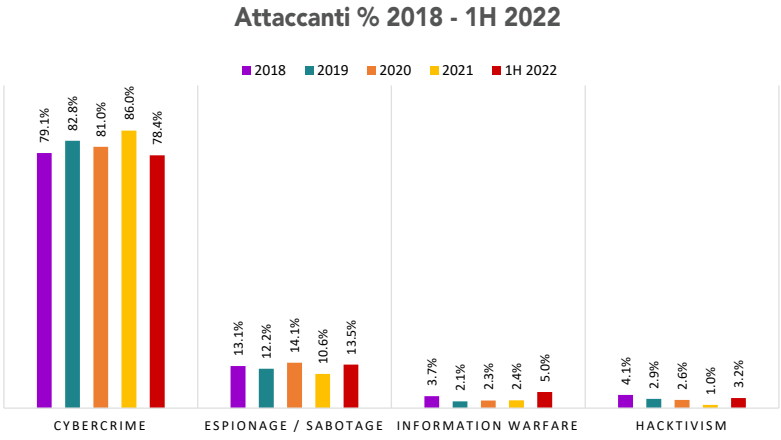
Distribuzione degli attaccanti per tipologia (2018 – 1H 2022)

ATTACCANTI PER TIPOLOGIA	2018	2019	2020	2021	1H 21	1H 22	1H 2021 su 1H 2022	Trend 2022
Cybercrime	1.229	1.381	1.518	1.763	925	894	-3.4%	↗
Espionage-Sabotage	203	203	264	217	95	154	62.1%	↑
Information Warfare	58	35	44	49	26	57	119.2%	↑
Hacktivism	64	48	48	20	7	36	414.3%	↑
Espionage-Sabotage + Inf. Warfare	261	238	308	266	121	211	74,4%	↑
Totale	1.554	1.667	1.874	2.049	1.053	1.141	+8,4%	↗

Per quanto riguarda le 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 primo semestre 2021 il numero di attacchi gravi di dominio pubblico che abbiamo raccolto nel 2022 è in crescita del **8,4%** (1.053 contro 1.141). In termini assoluti nel 1H 2022 la categoria "Espionage" ha fatto registrare il numero di attacchi più elevato degli ultimi 11 anni.
Dal campione emerge chiaramente che rispetto al 2021 le attività riferibili ad attacchi della categoria "**Hacktivism**" tornano ad aumentare sensibilmente (**+414,3%**), principalmente a causa della guerra in Ucraina. Per la stessa ragione sono in forte aumento sia gli attacchi compiuti per finalità di "**Espionage**" (**+62,1%**) che quelli riferibili a "**Information Warfare**" (**+119,2%**).
Diminuiscono leggermente gli attacchi classificati come attività di "**Cybercrime**" (**-3,4%**) dopo il picco straordinario del 2021.
Va sottolineato che, rispetto al passato, oggi risulta più difficile distinguere nettamente tra "Cyber Espionage" e "Information Warfare": sommando entrambe le categorie, nel primo semestre 2022 tali attacchi rappresentano il **18,5%** del totale (erano il 13% nel 2021), con una crescita del **74,4%**.



© Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia - aggiornamento giugno 2022



© Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia - aggiornamento giugno 2022

.

Distribuzione delle vittime per categoria (2018 – 1H 2022)

Come anticipato nell'introduzione, da quest'anno abbiamo introdotto una tassonomia delle vittime derivata da standard internazionali[7], 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 quadriennio 2018-2021.

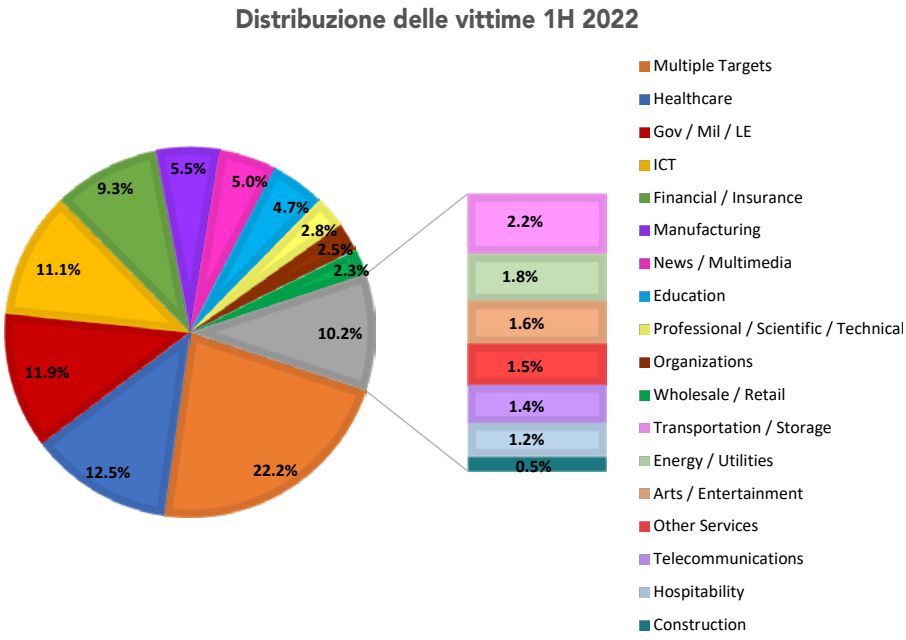
VITTIME PER CATEGORIA	2018	2019	2020	2021	1H 21	1H 22	1H 2021 su 2022	TREND 2022
Gov. / Mil. / LE	220	233	225	307	167	135	-19.2%	↗
ICT	191	233	269	278	113	126	11.5%	↗
Multiple Targets	326	406	401	274	121	252	108.3%	↑
Healthcare	161	186	210	262	139	142	2.2%	↗
Education	106	140	174	174	100	54	-46.0%	↓
Financial / Insurance	162	107	122	137	60	106	76.7%	↑
Prof. / Scientific / Technical	18	19	65	82	50	32	-36.0%	↓
Wholesale / Retail	33	45	54	82	50	26	-48.0%	↓
Transportation / Storage	33	16	39	75	48	25	-47.9%	↓
Manufacturing	34	36	65	72	47	63	34.0%	↑
News / Multimedia	70	69	43	69	38	57	50.0%	↑
Organizations	40	35	46	52	30	28	-6.7%	↗
Energy / Utilities	24	25	39	43	19	20	5.3%	↗
Arts / Entertainment	68	55	40	42	26	18	-30.8%	↓
Telco	13	19	32	36	9	16	77.8%	↑
Hospitability	44	27	22	30	17	14	-17.6%	↗
Other Services	9	14	15	25	13	17	30.8%	↑

[7] 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)

Agriculture / Forestry / Fishing	0	0	5	6	3	2	-33.3%	
Construction	1	2	7	3	3	6	100.0%	
Mining / Quarrying	1	0	1	0	0	2	-	-
TOTALE	**1.554**	**1.667**	**1.874**	**2.049**	**1.053**	**1.141**		

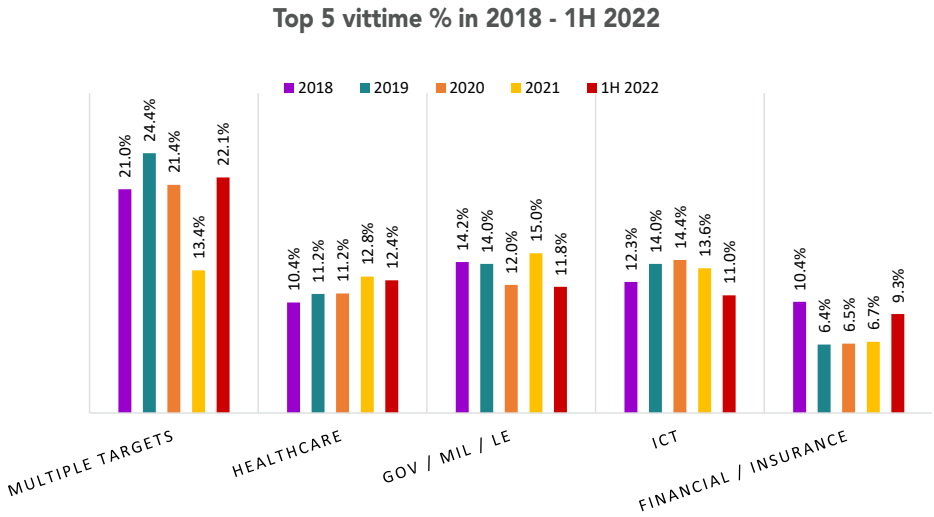
Rispetto al primo semestre 2021, nel 2022 la crescita maggiore nel numero di attacchi gravi si osserva verso le categorie "Multiple targets" (**+108,3%**), "Telecommunications" (**+77,8%**), "Financial / Insurance" (**+76,7%**), "News / Multimedia" (**+50%**), "Manufacturing" (**+34%**), "Other Services" (**+30,8%**) e "ICT" (**+11,5%**), seguite da "Energy / Utilities" (**+5,3%**) e "Healthcare" (**+2,2%**).

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 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 primo semestre 2022 rappresenta il **22%** del totale degli attacchi (era il 13% nel 2021).
È interessante notare che questo aumento degli attacchi verso bersagli multipli nel 2022 non deriva da attività cybercriminali (come avveniva in passato) ma dalla crescita di Hacktivism, Espionage e Information Warfare (che puntano a fare più danni e/o più "rumore", a seconda delle motivazioni).



© Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia - aggiornamento giugno 2022

In termini percentuali nel primo semestre 2022 la categoria "Multiple Targets" torna al primo posto assoluto (**22%** del totale).
Al secondo e terzo posto "Healthcare" e "Gov / Mil / Law Enforcement", ciascuna con circa il **12%** degli attacchi totali, al quarto "ICT" al **11%**, e al quinto "Financial / Insurance", al **9%**.
Le successive 6 categorie merceologiche (che sommate rappresentano il 23% degli attacchi rilevati) sono comprese tra il 6% e il 2% 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 10% residuo sul totale.



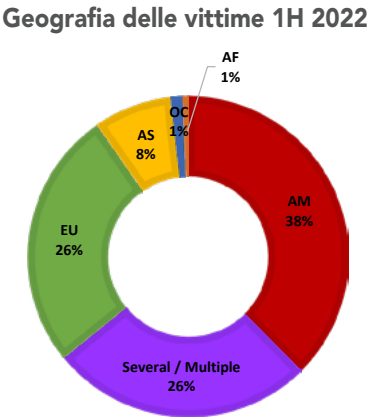
© Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia - aggiornamento giugno 2022

Osservando questo grafico delle prime 5 categorie più colpite tra il 2018 e il 1H 2022, si può apprezzare la netta variazione della categoria "Multiple Targets" rispetto al 2021, dovuta alle ragioni sopra esposte.

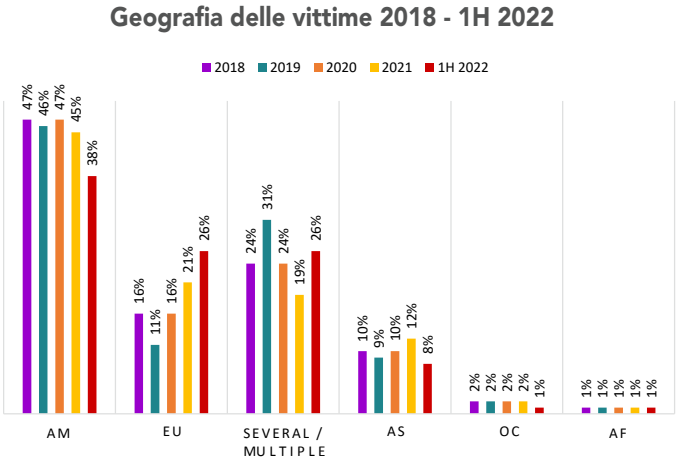
Distribuzione generale delle vittime per area geografica (1H 2022)

Nel 2022 diminuiscono le vittime di area americana (dal 45% al **38%**), mentre gli attacchi verso realtà basate in Europa aumentano sensibilmente (dal 21% al **26%**) e scendono leggermente quelli rilevati contro organizzazioni asiatiche (dal 12% al **8%**).

Percentualmente aumentano gli attacchi gravi verso bersagli con sedi distribuite in diversi Paesi (categoria "Several / Multiple"), che dal 19% del 2021 passano al **26%**.



© Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia - aggiornamento giugno 2022



© Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia - aggiornamento giugno 2022

Distribuzione delle tecniche di attacco (2018 – 1H 2022)

Come già detto per la classificazione delle vittime, da quest'anno introduciamo una nuova tassonomia delle tecniche di attacco derivata da framework internazionali[8], articolata su **8** macro-categorie e ben **54** sotto-categorie.

Tecniche di attacco	2018	2019	2020	2021	1H 21	1H 22	2021 su 2020	TREND
Malware	601	737	775	850	454	433	-4.6%	↗
Unknown	429	309	372	433	230	253	10.0%	↗
Vulnerabilities	143	158	200	320	164	120	-26.8%	↓
Phishing / Social Engineering	170	291	299	203	94	154	63.8%	↑
Multiple Techniques	64	57	86	103	48	93	93.8%	↑
Identity Theft / Account Cracking	67	71	90	76	31	35	12.9%	↗
Web Attack	43	21	18	33	20	4	-80.0%	↓
DDoS	37	23	34	31	12	49	308.3%	↑
TOTAL	**1.554**	**1.667**	**1.874**	**2.049**	**1.053**	**1.141**		

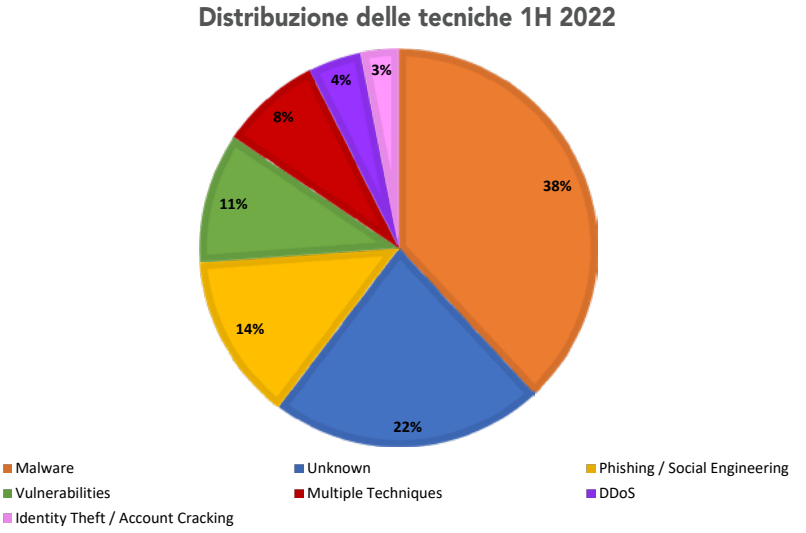
Nel primo semestre 2022 la categoria che mostra numeri assoluti maggiori è "Malware", che sia pure in leggera flessione (**-4,6%**) rappresenta il **38%** del totale. Le tecniche sconosciute (categoria "Unknown") tornano al secondo posto, con un aumento del **10%** rispetto al primo semestre 2021, superando la categoria "Vulnerabilità" (**-26,8%**) e "Phishing / Social Engineering" (in netta crescita, **+63,8%**), mentre "Tecniche Multiple" sale del **+93,8%**, in conseguenza della natura sempre più complessa degli attacchi.

In concomitanza con l'aumento di attività riferibili ad Hacktivism e Information Warfare, rispetto al totale gli attacchi gravi con finalità di "Distributed Denial of Service", pur pochi in valori assoluti, crescono di un significativo **308,8%**, così come quelli realizzati tramite "Identity Theft / Account Hacking" (**+12,9%**).

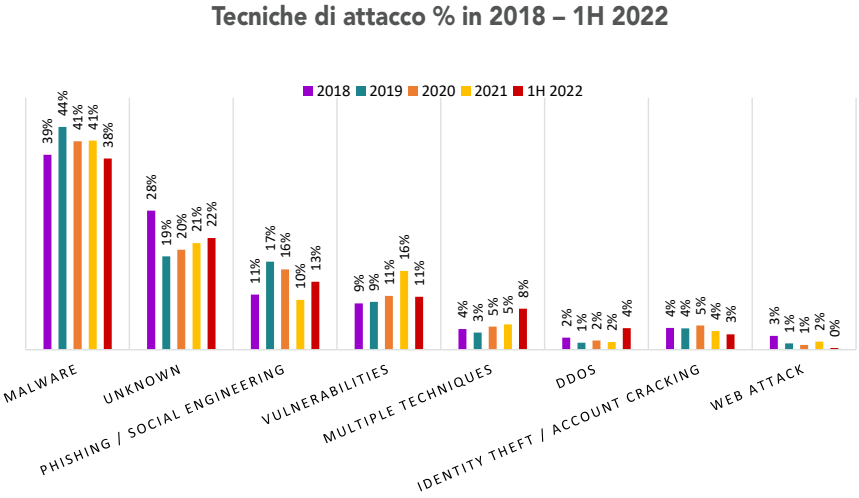
Il **22%** di "tecniche sconosciute" è principalmente dovuto al fatto che molti attacchi analizzati (oltre un quinto del totale) diventano di dominio pubblico a seguito di un "data breach",

[8] Non esistendo una tassonomia standard per le tecniche di attacco, le 54 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.

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).



© Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia - aggiornamento giugno 2022

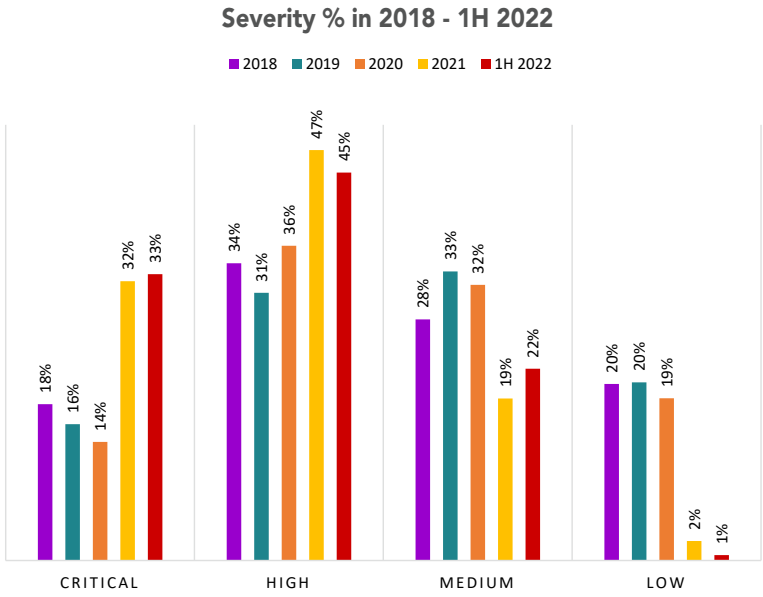


© Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia - aggiornamento giugno 2022

Analisi della "Severity" degli attacchi

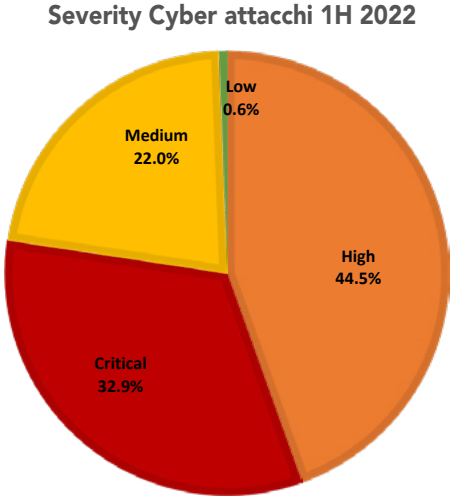
Come anticipato nell'introduzione, anche per il primo semestre 2022 presentiamo una valutazione della Severity degli attacchi analizzati.
Obiettivo di questa analisi infatti è individuare non solo le categorie di attaccanti, di vittime e di tecniche di attacco che crescono maggiormente in termini assoluti 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 dei danni per ogni singolo attacco analizzato 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 analizzando un campione di attacchi molto eterogenei): Basso, Medio, Alto e Critico.
Applicando questa modalità di valutazione degli impatti ai dati degli ultimi 4 anni e mezzo, si evidenziano fenomeni molto interessanti:



© Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia - aggiornamento giugno 2022

Nel 2020 gli attacchi con impatto "Critico" rappresentavano il **14%** del totale, quelli di livello "Alto" il **36%**, quelli di livello "Medio" il **32%** e 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 era già molto diversa e francamente impressionante: gli attacchi gravi con effetti molto importanti (High) erano il **47%**, quelli devastanti (Critical) il **32%**, quelli di impatto significativo (Medium) il **19%**, e quelli con impatto basso solo il **2%**. Fenomeno che si conferma anche nel primo semestre 2022, in cui gli attacchi con impatto Critical e High sono il **78%** del totale.

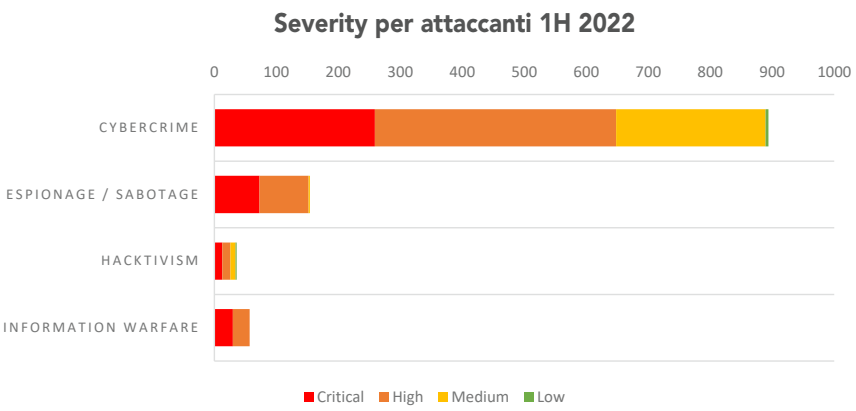


© Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia - aggiornamento giugno 2022

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

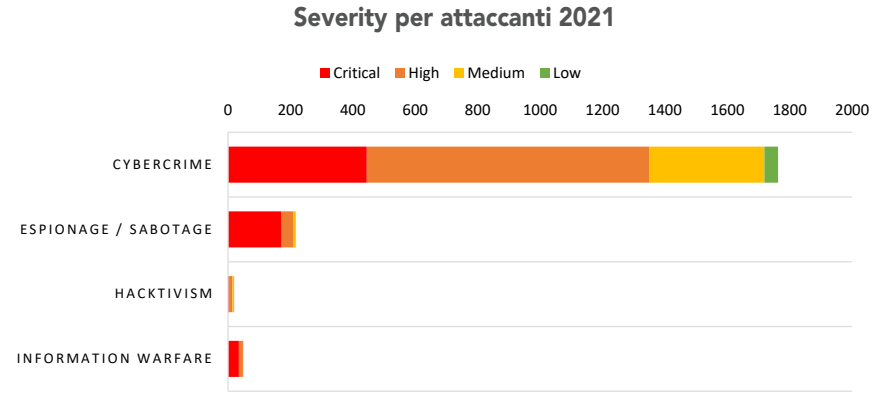
Severity per tipologia di attaccante

Di seguito il raggruppamento per tipologia di attaccante. In passato il maggior numero di attacchi classificati come "Critici" riguardava le categorie Espionage e 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 2022 sulla Sicurezza ICT in Italia - aggiornamento giugno 2022

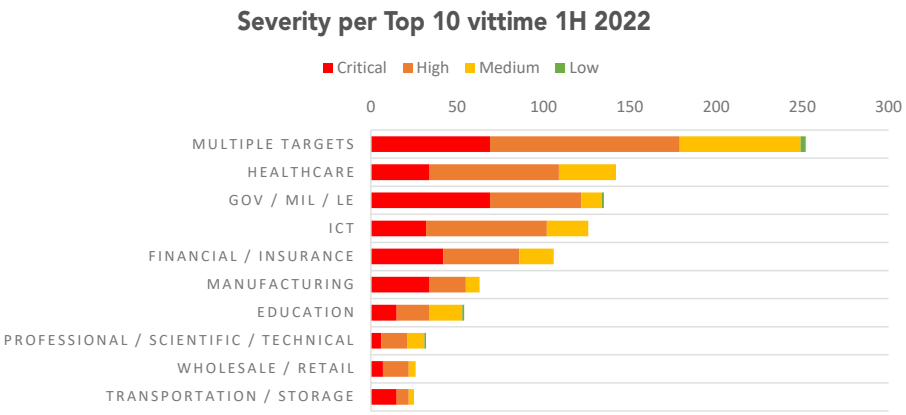
Come si evince confrontando i due grafici, così come nel 2021 anche nel 2022 gli attacchi con Severity "Critical" realizzati per finalità cybercriminali sono sensibilmente aumentati rispetto agli anni 2018-2020, il che desta grande preoccupazione e denota chiaramente un cambio di strategia da parte degli attaccanti.



© Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia

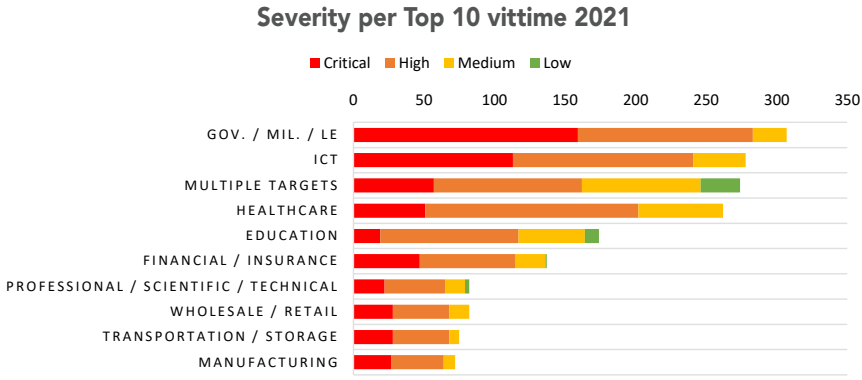
Severity per tipologia di vittima

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 "Multiple Targets", "Financial / Insurance", "Healthcare", "Manufacturing" e "ICT", mentre le categorie con il maggior numero di attacchi con impatti di livello "Alto" sono "Multiple Targets", "Healthcare", "ICT" and "Gov".



© Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia - aggiornamento giugno 2022

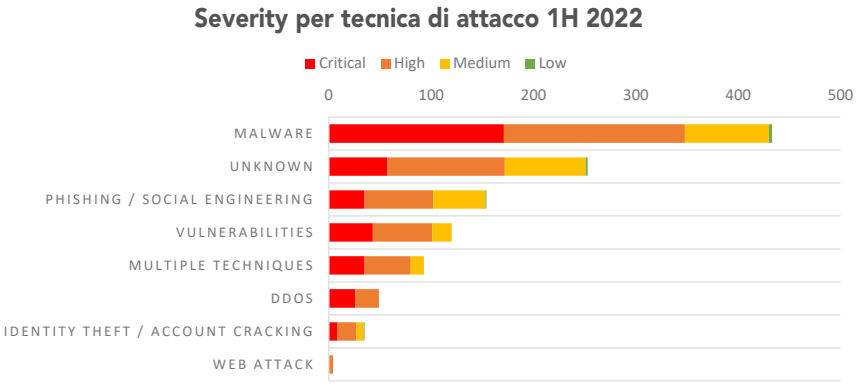
La situazione era simile nel 2021, con la principale differenza che la Severity media degli attacchi verso "Multiple targets" era sensibilmente più bassa, e che per tutte le categorie di vittime gli attacchi con Severity bassa sono ormai quasi assenti.



© Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia

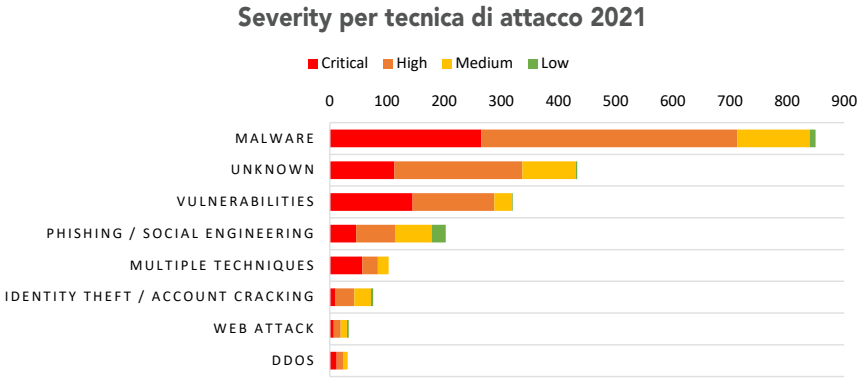
Severity per tecniche di attacco

Dal punto di vista delle tecniche di attacco nel 2022 gli incidenti con impatto più critico sono quelli realizzati tramite Malware, Tecniche Sconosciute, Vulnerabilità Note e Tecniche Multiple.



© Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia - aggiornamento giugno 2022

Aumenta in modo significativo anche la severity media degli attacchi realizzati tramite DDoS e Phishing.



© Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia

Colpisce in particolare l'incremento significativo di attacchi con impatto "Critical" realizzati tramite Malware, compiuti principalmente per finalità cybercriminali.

Attività e segnalazioni della Polizia Postale e delle Comunicazioni nel primo semestre del 2022

L'impegno della Polizia Postale e delle Comunicazioni si è indirizzato, anche nei primi 6 mesi del 2022, verso la prevenzione ed il contrasto di un insieme assai vasto ed eterogeneo di attacchi informatici, diretti a colpire il patrimonio personale dei cittadini come l'integrità del tessuto economico-produttivo del Paese, la regolarità dei servizi pubblici essenziali come il mondo delle professioni, la sicurezza e la libertà personale di adulti e ragazzi, con particolare riferimento alla protezione dei bambini e delle persone più vulnerabili.
Andiamo di seguito ad elencare le principali attività svolte dalla Specialità nel periodo interessato.

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

Nel primo semestre del 2022 l'impegno della Polizia Postale e delle Comunicazioni 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 *sex offenders* e pedofili avvezzi all'uso del web e dei suoi servizi di comunicazione.

Nell'ambito della prevenzione, la capillare attività di sensibilizzazione e informazione svolta su tutto il territorio nazionale dalla Polizia Postale in favore di scolaresche, genitori e insegnanti risulta essere ancora il principale strumento che produce effetti di ridimensionamento del fenomeno e riduzione del rischio.
L'effetto di accelerazione imposto dalla pandemia rispetto al coinvolgimento di minori in qualità di autori di reati online, sembra rallentare la sua velocità: negli ultimi anni si erano registrati, incrementi progressivi nel numero di reati commessi da minori riconducibili soprattutto alla pedopornografia, sia come esito del *sexting*, che come diffusione di immagini illegali via messaggistica. Tale incremento sembra stabilizzarsi e per il periodo di riferimento si registra un numero di casi vicino a quello dell'anno precedente; la progressiva ripresa delle attività nella direzione di un lento recupero della normalità, nonché l'uscita dallo stato di emergenza, hanno probabilmente contribuito a ridurre l'isolamento sociale, facendo rilevare nel periodo di riferimento una flessione relativa alla circolazione globale di materiale pedopornografico su circuiti internazionali, con una conseguente diminuzione dei casi trattati (-5%), che non ha però inciso sull'attività di contrasto. Infatti, è stato registrato un lieve aumento dei soggetti arrestati per violazioni connesse ad abusi in danno di minori.

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

L'analisi dei dati dei primi 6 mesi del 2022 ha fatto registrare una lieve diminuzione dei casi trattati, anche relativamente alle segnalazioni pervenute da organismi internazionali di protezione dei minori in rete, che però hanno evidenziato episodi di maggior gravità, tale da mettere in evidenza un maggior numero di individui sottoposti a pene detentive.

In particolare, nell'ambito dell'attività di contrasto svolta dal Centro sono stati trattati complessivamente **2670** casi, che hanno consentito di indagare **778** soggetti, di cui **73** tratti in arresto per reati connessi alla materia degli abusi tecnomediati in danno di minori, con un aumento di persone tratte in arresto di circa il **9%** rispetto allo stesso periodo dell'anno precedente.
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 **13194** siti, di cui **2587** inseriti in black list e oscurati, in quanto presentavano contenuti pedopornografici.

Adescamento online

Nel periodo di riferimento sono stati trattati **210** i casi per adescamento online, anche quest'anno la fascia di età 10-13 è quella più coinvolta con la maggior parte dei casi, **115** rispetto al totale.
Degno di attenzione è anche il dato che riguarda il numero dei casi che coinvolgono bambini sotto i 10 anni: casistica numericamente quasi assente prima della pandemia, è attualmente presente a riprova del fatto che le restrizioni dovute all'emergenza sanitaria hanno indotto un numero sempre più grande di piccoli internauti sul web, determinando per queste potenziali fragili vittime un incremento repentino del rischio di essere esposti ad approcci sessuali online da parte di adulti.
Compaiono tra i luoghi di contatto tra minori e adulti pedofili anche i videogiochi, sia su app che con consolle di gioco connesse ad internet, a riprova ulteriore del fatto che il rischio si concretizza con maggiore probabilità quando i bambini e i ragazzi si esprimono con spensieratezza e fiducia, nei linguaggi e nei comportamenti tipici della loro età.

Cyberbullismo

Nel primo semestre dell'anno in corso, è stata registrata una flessione anche dei casi di cyberbullismo che coincide con la normalizzazione delle abitudini dei ragazzi: non si può escludere che tale stato di cose e la fine delle restrizioni, abbiano avuto un'influenza positiva sulla qualità delle interazioni sociali, delle relazioni tra coetanei e che la costanza dell'opera di sensibilizzazione svolta dalla Polizia Postale, presso le strutture scolastiche, abbia mantenuto alta l'attenzione degli adulti significativi e dei ragazzi stessi sulla necessità di agire responsabilmente e correttamente in rete. Nel periodo di riferimento sono stati trattati **160** casi di cyberbullismo[1].

[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

Sextortion

È un fenomeno che di solito colpisce gli adulti in modo violento e subdolo, fa leva su piccole fragilità ed esigenze personali, minacciando, nel giro di qualche click, la tranquillità delle persone. Recentemente la sextortion impatta su vittime minorenni, con effetti lesivi potenziati: la vergogna che i ragazzi provano impedisce loro di chiedere aiuto ai genitori o ai coetanei di fronte ai quali si sentono colpevoli di aver ceduto alla tentazione e di essersi fidati di perfetti e "avvenenti" sconosciuti. Il senso di intrappolamento che sperimentano le vittime è amplificato spesso dalla difficoltà che hanno nel pagare le somme di denaro richieste. Dal 1/1/2022 al 30/6/2022 sono stati trattati **41** casi, la maggior parte dei quali nella fascia 14-17 anni, ma anche il dato che riguarda i minori di età compresa tra i 10-13 anni può destare preoccupazione.

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:

- **OPERAZIONE *"MEET UP"***, condotta in modalità sotto copertura dal personale del Compartimento Polizia Postale Piemonte e Valle D'Aosta, all'interno di canali *Telegram* dedicati alla diffusione, anche mediante sottoscrizione di abbonamenti a pagamento, di contenuti realizzati mediante sfruttamento sessuale di minori. Gli investigatori, interagendo direttamente in *chat* con gli utenti responsabili della diffusione, anche grazie alla capitalizzazione delle tracce informatiche e finanziarie enucleate, hanno potuto identificare gli utilizzatori dei *nicknames* destinatari dei 26 decreti di perquisizione emessi dall'A.G. procedente, che hanno consentito di indagare 26 persone, 3 delle quali tratte in arresto.

- **OPERAZIONE *"GREEN OCEAN"***, svolta in modalità sotto copertura dal Compartimento Polizia Postale e delle Comunicazioni di Palermo su piattaforme di *file sharing* e di messaggistica utilizzate per la diffusione di contenuti di pornografia minorile. All'esito dell'indagine sono state eseguite, su tutto il territorio nazionale, coordinate dal C.N.C.P.O. del Servizio Polizia Postale e delle Comunicazioni, 32 perquisizioni nei confronti di altrettanti indagati, che hanno consentito di trarre in arresto 13 persone per detenzione di ingente quantità di materiale pedopornografico. In un caso, la perquisizione informatica effettuata sui dispositivi ha messo in luce l'esistenza di abusi fisici in danno di 2 minori, all'epoca dei fatti dell'età di 2 e 3 anni.
  L'attività in argomento ha consentito, inoltre, di individuare centinaia di account riconducibili a utenti esteri, per i quali sono stati interessati i relativi collaterali.

---

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.

- **OPERAZIONE *"FAMIGLIE DA ABUSI"***, svolta in modalità sotto copertura nell'ambito del contrasto alla pedopornografia online inerente al gruppo *Telegram* "Famiglie da Abusi" e condotta dai Compartimenti di Roma, Bologna, Milano, Napoli e Catania, coordinati dal C.N.C.P.O. del Servizio Polizia Postale e delle Comunicazioni, ha consentito di arrestare 5 persone ritenute responsabili di diffusione e detenzione di materiale di sfruttamento sessuale di minori online.
  In particolare, gli indagati appartenevano a una comunità ristretta dedita allo scambio di materiale pedopornografico, anche autoprodotto dagli stessi partecipanti.

- **OPERAZIONE *"REVELATUM"***, condotta dal Compartimento Polizia Postale e delle Comunicazioni per la Puglia nell'ambito del contrasto alla pedopornografia online, ha visto coinvolti 72 indagati, destinatari di altrettanti decreti di perquisizione su tutto il territorio nazionale, emessi dall'A.G. procedente.
  L'indagine, avviata alla fine del 2020, ha preso le mosse dall'analisi delle tracce informatiche collegate a un *link* afferente a un *cloud* attestato sulla piattaforma di *file hosting* "Mega.nz".
  Gli Uffici territoriali della Polizia Postale, coinvolti nella fase esecutiva dell'operazione e coordinati dal C.N.C.P.O. del Servizio Polizia Postale e delle Comunicazioni, hanno denunciato 59 persone per detenzione e diffusione di materiale pedopornografico e altre 7 sono state tratte in arresto in flagranza di reato per detenzione di ingente quantitativo di materiale realizzato mediante sfruttamento dei minori degli anni 18.

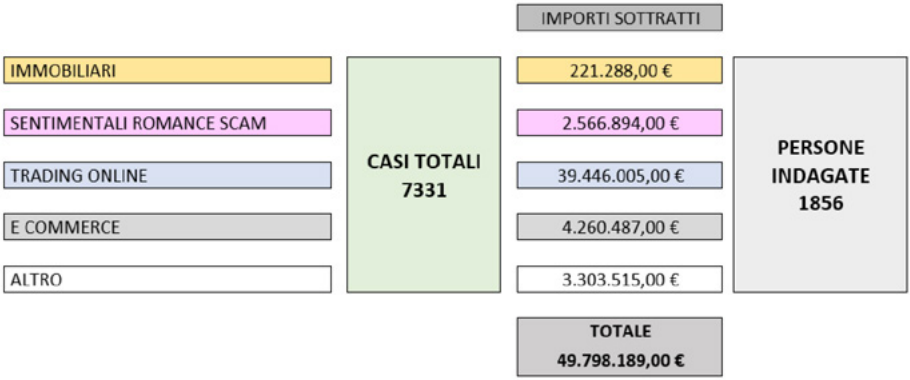
- **OPERAZIONE *"BROKEN DREAMS"***, avviata dal C.N.C.P.O. del Servizio Polizia Postale e delle Comunicazioni a seguito di una segnalazione di operazioni sospette pervenuta, tramite Banca d'Italia, dalla società statunitense *Paypal*, dedita alla fornitura di servizi di pagamento e trasferimento digitale di denaro.
  Dall'analisi di un portafoglio elettronico riconducibile a una minore di nazionalità dominicana residente in Italia, gli investigatori hanno ricostruito le tracce relative alle transazioni in ingresso, caratterizzate da causali riconducibili alla sottoscrizione di abbonamenti periodici afferenti a sessioni di *"Live Distant Child Abuse"*, realizzate in *streaming* su piattaforme di videochat. L'indagine ha consentito di individuare 18 soggetti per i quali l'Autorità giudiziaria ha emesso altrettanti decreti di perquisizione, attività che si sono concluse con 17 indagati, due dei quali in stato di arresto.

- **OPERAZIONE *"LUNA"***, avviata dal Compartimento Polizia Postale e delle Comunicazioni per il Friuli Venezia Giulia sulla scorta delle risultanze emerse a seguito dell'analisi forense eseguita sui supporti informatici sequestrati a un indagato nell'ambito di altra operazione di polizia giudiziaria, si è conclusa con la denuncia di 25 persone, 7 delle quali minorenni e una tratta in arresto. L'attività, che ha coinvolto tutti gli Uffici territoriali della Specialità, coordinati dal C.N.C.P.O. del Servizio Polizia Postale e delle Comunicazioni, ha consentito di indagare 25 soggetti, di cui uno in stato di arresto.

Sezione Operativa

- È stata intensificata l'azione di contrasto alle truffe online, agevolate anche da un sempre più diffuso utilizzo della rete internet per effettuare acquisti o vendite di beni di ogni genere, cosa questa che ha prodotto una crescita nel settore dei c.d. *market place*.

SEZIONE OPERATIVA: report relativo alle truffe online - primo semestre 2022



In tale contesto delittuoso, un fenomeno in forte espansione è quello delle truffe attuate tramite proposte di investimenti di capitali online (*trading online*). Già dallo scorso anno si è evidenziata una decisa crescita delle denunce e dei capitali investiti, con un coinvolgimento di vittime non più circoscritto a soggetti vulnerabili come gli anziani, ma esteso a diverse tipologie di "investitori", segno della sempre maggiore capacità organizzativa della struttura criminale, ramificata per lo più all'estero. In virtù di queste peculiarità è stata implementata l'attività di collaborazione con le strutture preposte, a livello internazionale, al coordinamento tra le varie Forze di Polizia nel contrasto alle più svariate forme di crimine (SCIP, Europol ed Interpol).

Altro fenomeno in aumento sono le truffe romantiche (*romantic scam*), la cui proliferazione sembra essere correlata ad un uso sempre maggiore dei social network e dei siti di *dating*. Proprio alcune recenti indagini hanno evidenziato che gli autori, pur essendo originari di paesi nord-africani, prevalentemente Nigeria, Costa d'Avorio, Benin e Burkina Faso, operano in maniera strutturata sul territorio italiano, dal quale esportano ingenti somme di denaro anche attraverso servizi di Money Transfer verso i paesi natii. Queste organizzazioni sembrano, inoltre, aver sviluppato una capacità di "azione" in diversi campi, agendo anche nell'ambito delle cd *"sextortion"* e delle truffe legate al *trading on line*, mostrando una elevata capacità criminale con l'individuazione delle potenziali vittime anche attraverso sistematiche operazioni di *social engineering*.

- **Con riferimento al contrasto dei reati contro la persona**, particolare attenzione è stata dedicata al *revenge porn*, al *cyber stalking* e a tutte quelle forme di aggressione espressamente contrastate anche attraverso la recente normativa del c.d. "codice rosso" che, avendo introdotto una maggiore tempestività nella risposta giudiziale, ha reso più agevole l'individuazione degli autori della condotta criminosa e quindi una più efficace protezione delle vittime.

SEZIONE OPERATIVA: report reati contro la persona - primo semestre 2022

	CASI TRATTATI	PERSONE INDAGATE
STALKING	69	32
DIFFAMAZIONE ON LINE	1054	282
MINACCE	405	75
REVENGE PORN	111	37
MOLESTIE	283	27
SEXTORTION	466	37
ILLECITO TRATTAMENTO DATI	425	15
SOSTITUZIONE DI PERSONA	1669	61
FENOMENO HATE SPEECH	52	17
PROPOSITI SUICIDARI	16	
TOTALE	**4550**	583

Sono stati programmati specifici servizi di monitoraggio dei canali di diffusione dei contenuti multimediali, siti web, piattaforme di vendita, profili e pagine presenti sui social network più noti (Facebook, Twitter, Instagram, Telegram, Pinterest e Youtube), finalizzati ad arginare la diffusione del linguaggio d'odio, c.d. *hate speech*, in costante collaborazione con l'Osservatorio per la Sicurezza contro gli Atti Discriminatori.

- **Sono state oggetto di attività di pubblico soccorso** le numerose segnalazioni, ricevute per il tramite del Commissariato di P.S online, dai vari social network e dal Servizio di Cooperazione Internazionale, per i manifesti intenti suicidari, fenomeno che, in particolare durante la fase di pandemia, ha visto una consistente crescita.
- **L'attività di contrasto alle infiltrazioni della criminalità nel mondo sportivo**, vede impegnato questo Servizio che, ravvisando l'esigenza di potenziare le investigazioni

sul fenomeno delle scommesse illecite on line, al fine di garantire la correttezza dello svolgimento delle manifestazioni sportive, ha esteso a tutti i Compartimenti dislocati sul territorio nazionale, i compiti di monitoraggio della rete, con particolare riguardo ai siti e agli spazi web (blog, gruppi social e siti di settore) dediti ai giochi e alle scommesse on line, anche attraverso una sempre più stretta interazione con la Procura Federale della Federazione Italiana Giuoco Calcio e l'Agenzia delle Dogane e Monopoli. 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.

- L'uso dilagante dell'informatica e più in particolare della rete internet in ogni settore della vita sociale, ha agevolato la consumazione di numerosi reati, sia contro la persona che contro il patrimonio, e da ultimo anche **contro la proprietà intellettuale**. Ciò ha determinato il diretto coinvolgimento della Polizia Postale e delle Comunicazioni anche nella prevenzione e repressione dei reati in violazione del diritto d'autore, qualora consumati con l'utilizzo della rete Internet.

L'attività condotta dalla Polizia Postale e delle Comunicazioni ha permesso di riscontrare che tutti i servizi della Rete, di volta in volta, sono stati coinvolti nel mercato parallelo ed abusivo di opere intellettuali e artistiche: software, opere cinematografiche e musicali sono state oggetto di una divulgazione massiccia nella Rete, una volta dietro corrispettivi irrisori, oggi addirittura gratuitamente. In particolare, il fenomeno si è sviluppato dalla contraffazione di copie all'utilizzo domestico della Rete che, attraverso chat, community, file-sharing, siti web, offre gratuitamente opere tutelate dal diritto d'autore appena presentate al mercato, con notevole danno per il mercato legittimo e per le industrie che vi operano.

Principali operazioni 1 gennaio 2022 - 30 giugno 2022

Operazione "Rear Window"

Grazie a una complessa e articolata attività di polizia giudiziaria, durata oltre un anno, ad esito della quale sono state eseguite su tutto il territorio nazionale 10 perquisizioni, gli investigatori della Polizia Postale e delle Comunicazioni, coordinati dalla Procura della Repubblica di Milano, sono riusciti a disarticolare un vero e proprio "sistema" criminale finalizzato alla violazione, mediante intrusioni informatiche, di impianti di videosorveglianza installati per lo più presso private abitazioni.

Nell'ambito dei due gruppi criminali scoperti dagli investigatori (per uno dei quali - il più corposo - si configura una vera e propria associazione per delinquere), gli indagati avevano ruoli e compiti ben definiti: i più esperti in materia informatica scandagliavano la rete alla ricerca di impianti di videosorveglianza connessi ad internet; una volta individuati, li facevano oggetto di veri e propri attacchi informatici che consentivano, ricorrendo determinate condizioni, di scoprire le password degli NVR (ossia dei videoregistratori digitali a cui normalmente vengono collegate le telecamere di videosorveglianza) e di accedere ai relativi

impianti. Raccolte le credenziali di accesso, era compito di altri appartenenti ai gruppi criminali verificare la tipologia degli impianti, gli ambienti inquadrati e la qualità delle riprese, allo scopo di individuare telecamere che riprendessero luoghi particolarmente "intimi", come bagni e camere da letto. L'obiettivo finale era infatti quello di carpire immagini che ritraessero le ignare vittime durante la consumazione di rapporti sessuali o atti di autoerotismo. In alcuni casi, le immagini facevano riferimento a telecamere installate presso alberghi, studi medici e spogliatoi di palestre e piscine. Al termine di tale selezione, le credenziali di accesso venivano affidate ad altri sodali che, attraverso "vetrine" online create ad hoc, le mettevano in vendita sulla rete. I proventi illeciti venivano reinvestiti nell'acquisto di sempre più aggiornati software per l'effettuazione degli attacchi informatici.

Operazione "Network Evolution"

La Polizia Postale e delle Comunicazione, ha individuato un'associazione a delinquere, finalizzata a compiere truffe informatiche, composta da undici soggetti.
I criminali, dopo aver selezionato gli annunci di vendita presenti sulle varie piattaforme di commercio on line, contattavano i venditori, fingendosi fortemente interessati all'acquisto della merce e desiderosi di effettuare il pagamento nel più breve tempo possibile.
I malfattori convincevano l'ignara vittima a recarsi presso uno sportello automatico, per ricevere l'accredito della somma pattuita direttamente sulla propria carta, quindi, sfruttando la non perfetta conoscenza degli strumenti bancari delle vittime, i truffatori fornivano loro tutta una serie di istruzioni e codici, grazie ai quali, invece di ricevere il pagamento sul proprio conto, i malcapitati erano indotti a ricaricare una carta di pagamento nella disponibilità del sodalizio criminale. In numerosi casi il malcapitato addirittura è stato indotto a compiere numerose ricariche, prima di accorgersi di essere caduto in un tranello.
Per garantirsi l'anonimato ed eludere così l'attività investigativa, i membri dell'organizzazione erano soliti ricorrere a sistemi di "anonimizzazione" delle conversazioni o ad applicazioni crittografate come Telegram ed ICQ.
Al momento si stima che i proventi dell'attività dell'organizzazione criminale possano ammontare a svariati milioni di euro.

Mandante omicidio sul darkweb

La Polizia Postale e delle Comunicazioni, attraverso complesse indagini connotate dall'elevato contenuto tecnico, è giunta all'identificazione di un utente che, approfittando dell'anonimato garantito dalla cosiddetta "parte oscura" della Rete, il DARKWEB, aveva effettuato un pagamento in criptovalute per commissionare ad un altro utente, amministratore di un sito specializzato in omicidi su commissione, l'uccisione di un rivale in amore.
L'intera vicenda trae origine da un'attività di cooperazione internazionale di polizia con l'FBI americano che informava il Servizio Polizia Postale che un quarantacinquenne del trevigiano era stato indicato come potenziale vittima di un "servizio" a pagamento di omicidio su commissione. I primi accertamenti sulla rete hanno permesso di dare un nome e cognome alla vittima, che, grazie all'attività di controllo del territorio, veniva discretamente "vigilato"

per garantirne l'incolumità.
Ulteriori approfondimenti sulle informazioni comunicate dagli americani, hanno permesso di individuare importanti tracce telematiche connesse alle transazioni in criptovaluta effettuate, riuscendo così a risalire al "mandante" e richiedente il particolare servizio criminale, un trentaquattrenne della provincia trevigiana.

Truffa Paypal

La Polizia Postale e delle Comunicazioni ha effettuato 25 perquisizioni nei confronti di altrettanti indagati componenti un sodalizio criminale dedito alle truffe in danno di una società che opera attraverso una piattaforma di mediazione per i pagamenti on-line.
L'attività investigativa ha consentito di accertare che gli indagati hanno acquistato con conti incapienti merce on-line da numerosi venditori italiani ed esteri.
I venditori ricevevano il pagamento dei beni, dato che gli acquisti avvenivano tramite la piattaforma PayPal, ma quest'ultima subiva un danno economico di circa due milioni di euro poiché i conti correnti di riferimento erano privi di giacenza.
Tale modus operandi ha consentito al sodalizio criminale di acquistare fraudolentemente i più svariati beni: orologi di lusso, preziosi, smartphone di ultima generazione, apparecchi per la casa e finanche generi alimentari.
Nel corso delle perquisizioni è stato sequestrato un ingente quantitativo di materiale al vaglio degli inquirenti per i successivi accertamenti.

Operazione "Pangea XV"

L'attività della Specialità è stata caratterizzata, inoltre, da un sempre maggiore impegno nella cooperazione internazionale, con l'adesione a specifici programmi di contrasto al **commercio illegale di farmaci ed al fenomeno della contraffazione**. La Polizia Postale e delle Comunicazioni ha aderito per la prima volta all'Operazione denominata "Pangea XV" 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 di Ancona che, unitamente al Compartimento di Pescara, 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 Ancona 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 43 siti, rendendoli irraggiungibili dall'Italia, così da interrompere la vendita, sul territorio nazionale, di farmaci non autorizzati.

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

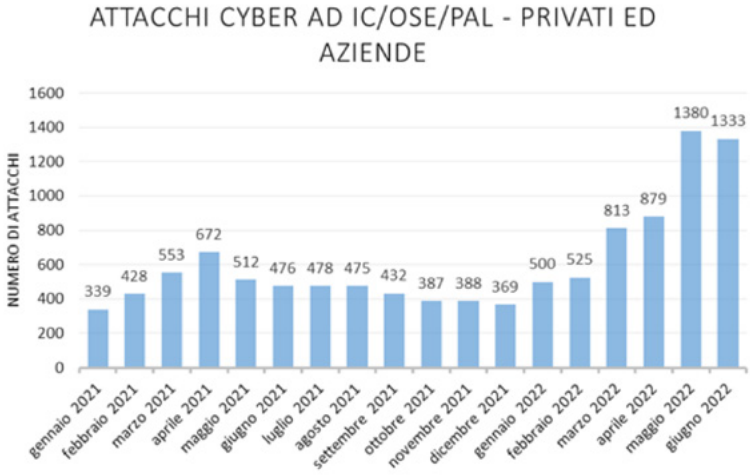
Nell'attuale e particolare contesto internazionale, l'*escalation* di tensione geopolitica in Ucraina ha avuto significativi riverberi anche in materia di sicurezza cibernetica e protezione delle infrastrutture critiche nazionali.
In particolare, sono emerse campagne massive a livello internazionale dirette verso infrastrutture critiche, sistemi finanziari e aziende operanti in settori strategici quali comunicazione e difesa, tra le quali figurano campagne di *phishing*, diffusione di *malware* distruttivi (specialmente *Ransomware*), attacchi Ddos, campagne di disinformazione e *leak* di database.
In questo quadro, gruppi di hacker, di matrice statuale, hanno deciso di schierarsi a favore della Russia, altri con l'Ucraina, prendendo di fatto parte al conflitto nel c.d. "dominio cibernetico".

In riferimento a questo specifico scenario e ai rischi collegati al quadro internazionale in dinamica evoluzione, il Servizio Polizia Postale e delle Comunicazioni, Organo del Ministero dell'Interno per la sicurezza delle telecomunicazioni, ha condiviso, a tutti gli attori istituzionali dell'ecosistema della cyber sicurezza nazionale, le evidenze informative raccolte relative alle potenziali criticità in ambito cibernetico che depongono per il mantenimento del più elevato grado di allertamento nonostante.
In particolare, il Servizio ha implementato l'attività informativa e di monitoraggio ad ampio spettro, esteso anche al *dark web*, attivando canali di diretta interlocuzione dedicati allo scenario in atto, con Europol, oltre che con Interpol e FBI, con l'obiettivo di elevare il livello di attenzione con particolare riguardo al settore economico/finanziario, tradizionalmente oggetto di interesse da parte di compagini criminali con connotazione *state sponsored*.
Il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC), attraverso dedicati alert ha diffuso indicatori di compromissione e avvisi di informazione di sicurezza alle infrastrutture informatiche dicasteriali, alle infrastrutture critiche nazionali e ai potenziali target di azioni ostili, individuati attraverso la permanente attività informativa assicurata dal Centro.

In particolare, sono stati diramati oltre 70 alert alle infrastrutture critiche presenti sul territorio nazionale in ordine a minacce e vulnerabilità, connesse al conflitto in atto.
I dipendenti Compartimenti sono stati inoltre sensibilizzati all'innalzamento delle attività di competenza, attraverso un adeguato e precipuo coinvolgimento dei rispettivi Nuclei Operativi di Sicurezza Cibernetica (NOSC), e alla predisposizione di adeguati servizi di monitoraggio e analisi, significando l'esigenza di tempestiva condivisione di ogni evidenza utile in relazione al quadro internazionale in parola.
Alla stessa stregua le strutture territoriali della Specialità sono state interessate per l'intensificazione dell'attività informativa, con particolare riguardo alle realtà economiche nazionali individuate dal NCS, con proiezione operativa ed interessi in territorio ucraino.

Sul punto, il Servizio Polizia Postale e delle Comunicazioni ha già assunto diretti contatti con oltre 80 società collegate all'Ucraina, operanti anche nel territorio italiano in ambiti strategici, al fine di innalzare i livelli di sicurezza e stabilire un canale informativo rafforzato.

C.N.A.I.P.I.C. e N.O.S.C.	Primo Semestre 2021	Primo Semestre 2022	VARIAZIONE PERCENTUALE
Attacchi rilevati	**2980**	**5430**	**+82%**
Totale persone indagate	**98**	**240**	**+145%**
Alert diramati	54937	58429	+6%



Infrastrutture Critiche (IC) – Operatori Servizi Essenziali (OSE) – Piccole Amministrazioni Locali (PAL)

Recenti eventi di sicurezza

Sono state recentemente osservate le seguenti attività ostili, potenzialmente riconducibili all'attuale crisi internazionale:

- È divenuta sempre più importante la presenza in rete del gruppo hacker russo denominato "Conti". Lo stesso, attivo già dal 2020, risulta essere una *crew* fortemente organizzata, in grado di sfruttare il modello business del "Ransomware as a Service" per condurre attacchi informatici a scopo estorsivo a target di rilievo internazionale. Il gruppo sfrutterebbe una serie di campagne di *spear-phishing* e la compravendita di credenziali nel Dark Web per riuscire ad avere accesso diretto alle strutture informatiche ed inoculare malware distruttivi.

La recente cronaca ha puntato i riflettori sulla dichiarazione pubblica del gruppo "Conti" di sostenere le operazioni militari condotte dalla Federazione Russa, promuovendo azioni di *cyberwar* contro le infrastrutture critiche dei Paesi schierati a sostegno dell'Ucraina. Nell'ambito della dedicata attività di analisi e monitoraggio del Servizio Polizia Postale e delle Comunicazioni, si è appreso che tale schieramento, non condiviso da tutti i suoi membri, ha avuto come conseguenza la pubblicazione di un *data-leak* contenente una serie di conversazioni riservate della *crew* in parola, verosimilmente ad opera di attivisti informatici riferibili al c.d. "esercito cyber" ucraino, che ha come target siti, servizi e infrastrutture russi in risposta all'invasione del Cremlino.
I dati esfiltrati riferibili a *bitcoin wallet, email, hash, ip, c&c*, in uso alla "Conti Gang" sono oggetto di approfondita analisi per sviluppare ogni evidenza, da condividere, oltre che in sede di cooperazione internazionale di polizia, con le infrastrutture critiche per mitigare ogni minaccia.

- È stato rilevato un attacco informatico ai danni della società Viasat S.p.A., subfornitrice del Gruppo Telespazio partecipato dalla Leonardo S.p.A., leader europeo nel campo dei servizi satellitari, di geo informazione e sistemi di navigazione di rete, che ha determinato inizialmente l'indisponibilità in Ucraina dei servizi di connettività satellitare offerti attraverso la rete di collegamento KA-SAT e, successivamente, avrebbe interessato l'intero sistema operativo satellitare ad alta velocità di trasmissione dati.
  Nell'ambito dell'attività investigativa in corso per la ricostruzione della dinamica dell'attacco, sono stati attivati i canali di cooperazione internazionale con FBI ed Europol per acquisire ulteriori evidenze relative all'azione ostile.

- È in corso ad opera del CNAIPIC un'attività investigativa per riscontrare elementi informativi relativi ad azioni ostili in danno di risorse digitali appartenenti alla rete telematica italiana della *European Space Agency*.
  In particolare, una risorsa digitale ostile, riferibile per quanto appreso al gruppo statuale russo denominato convenzionalmente Snake/Turla, avrebbe avuto accesso ad informazioni relative al satellite Aeolus, utilizzato da ESA per il telerilevamento e la produzione di immagini satellitari.
  Dopo aver assunto contatti diretti con il personale ESA, si è appreso che l'attaccante avrebbe contattato diversi server attestati su una porzione isolata della rete informatica e sarebbe riuscito ad impossessarsi di informazioni destinate alla condivisione con la comunità scientifica accreditata per il progetto in parola.
  Sono in corso le verifiche tecniche volte ad appurare l'estensione della compromissione e il livello di riservatezza delle informazioni carpite, con particolare riferimento a quelle afferenti il comando e la gestione del satellite che, allo stato, non risultano essere state violate.

Oltre le sopradescritte indagini in essere, risultano in corso ulteriori attività investigative in ordine ad attacchi informatici di matrice criminale condotti ai danni delle infrastrutture critiche di Ferrovie dello Stato e, da ultimo, del Ministero della Transizione Ecologica.
In particolare, si è proceduto ad attivare un dedicato canale di collaborazione internazionale anche con Europol, finalizzato al confronto circa le evidenze fin ora raccolte.

Minaccia "Killnet"

A partire dal 19 maggio u.s., l'Italia - al pari di altri Paesi con posizioni di sostegno all'Ucraina - è stata interessata da una vasta mole di attacchi informatici, operati da gruppi di dichiarata matrice filorussa, diretti verso le infrastrutture critiche di numerosi paesi atlantisti. In Italia in particolare, tali attacchi si sono tradotti tra l'altro nella minaccia di danneggiamenti significativi a pubbliche amministrazioni (ivi inclusi i sistemi del Governo, del Ministero dell'Interno e della Difesa), primari Organi di stampa, Istituti bancari, Porti, Aeroporti, Logistica.
Una specifica campagna di attacchi informatici di tipo DDOS, è stata condotta ai danni dei siti internet dell'evento internazionale Eurovision Song Contest 2022 e degli obiettivi istituzionali e nazionali sopracitati, dal collettivo hacker "KillNet", associato ad ambienti filorussi, rivendicata attraverso i propri canali Telegram.
Gli attacchi, portati con tecnica c.d. "D-Dos", volta a dirigere ingenti quantità di connessioni e richieste verso siti internet allo scopo di determinarne il malfunzionamento o la paralisi, hanno progressivamente interessato diversi settori governativi e della pubblica amministrazione in generale, il settore dei trasporti, il settore della stampa ed il settore bancario/finanziario.
L'attività del CNAIPIC del Servizio Polizia Postale e delle Comunicazioni, oltre ai doverosi approfondimenti investigativi, si è tradotta nell'analisi tecnica della minaccia, volta alla elaborazione di informazioni di sicurezza preventiva, nonché nel supporto operativo alle infrastrutture attaccate, per il più rapido ripristino dei sistemi.
Le evidenze raccolte per la più ampia diffusione sono state altresì partecipate, per i profili di competenza, all'Agenzia per la Cybersicurezza Nazionale.
Le azioni poste in essere hanno consentito, allo stato, il ritorno alla piena operatività di tutti i sistemi informatici colpiti.
Nella serata del 21 maggio u.s., infine, il collettivo *hacker* ha pubblicato un messaggio con il quale ha preannunciato l'intenzione di dirigere i prossimi attacchi verso le risorse informatiche della Polonia.
A tal proposito, il Servizio Polizia Postale e delle Comunicazioni ha provveduto all'immediata attivazione dei canali di cooperazione internazionale di polizia, per la pronta veicolazione delle informazioni preventive di sicurezza.

Eurovision 2022 e 72° Festival della Canzone Italiana di Sanremo

Come in occasione di importanti eventi nazionali, personale del CNAIPIC del Servizio Polizia Postale e delle Comunicazioni ha garantito dedicati servizi di sicurezza informatica a

favore del Festival della Canzone Italiana di Sanremo e dell'*Eurovision Song Contest* 2022.
Il Servizio Polizia Postale e delle Comunicazioni ha assicurato un complessivo supporto alla struttura di sicurezza cibernetica della RAI, infrastruttura critica convenzionata con il CNAIPIC, al fine di garantire il regolare svolgimento delle iniziative.
In particolare, presso le location degli eventi in parola, sono state allestite sale operative, attive h24, con la presenza di tecnici specializzati per la diretta tutela dei sistemi e dei servizi informatici nonché per la neutralizzazione di minacce cibernetiche.
Durante l'attività svolta, il personale tecnico della Specialità ivi impiegato ha individuato e segnalato numerose vulnerabilità, consentendo così ai referenti informatici RAI di approntare le opportune e tempestive attività di rimedio, al fine di evitare possibili attacchi informatici.
La sala operativa del CNAIPIC ha altresì svolto più di 1000 ore di monitoraggio con oltre 100 specialisti della Polizia Postale, monitorando l'intera rete e analizzando dati informatici provenienti anche dalle diverse piattaforme social.
È stato inoltre assicurato un monitoraggio costante degli account social (Twitter, Facebook ed Instagram) attivati per le due manifestazioni, esteso anche al sistema di tv *streaming* presente su www.raiplay.it, al fine di rilevare e neutralizzare in tempo reale minacce e interferenze ostili.

Financial Cybercrime

Nel primo semestre del corrente anno si mantiene la tendenza, già evidenziata nel 2021, in base alla quale il *financial cybercrime* si conferma sempre più come una delle forme predominanti e preminenti del crimine informatico.
Tale tendenza permane sia a livello nazionale che globale: poiché questa tipologia di reati pone il vantaggio per la criminalità di ricevere dalle attività delittuose un immediato e corposo riscontro economico.
Sono pertanto molteplici ed in continua evoluzione le tecniche utilizzate dalle organizzazioni criminali, che indiscriminatamente incidono sia sui semplici cittadini che sulle piccole e medie imprese che costituiscono il tessuto economico portante del nostro Paese.

I *modus operandi* mediante i quali vengono perpetrati i crimini finanziari sono prevalentemente quelli che afferiscono al c.d. *"Man in the middle"*; e del "Phishing" che consente il furto dei dati sensibili per l'accesso ai sistemi di *home banking*.

Quest'ultima tipologia assume svariate forme che vengono qualificate, in relazione al mezzo utilizzato quindi non solo tramite mail, ma anche mediante sms, "Smishing" o attraverso un contatto diretto a voce, "Vishing".
Lo scopo di tali tecniche di attacco è quello di entrare in possesso delle credenziali finanziarie delle vittime, per poter poi operare dai conti correnti online; con le carte di credito/debito con prelievi; con bonifici; con l'acquisto di beni online.

Per quanto riguarda la tecnica criminale c.d. del "Man in the middle", il BEC *(Business e-mail compromised)* e il *Chef Executive Officer fraud* (CEO *Fraud*) rappresentano a tutt'oggi le tipologie di frode maggiormente diffuse e che vanno a colpire fondamentalmente le aziende.

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

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

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

La tecnica cosiddetta del "Sim Swap" è una costola diretta del *phishing* e delle sue varianti che si è sviluppata con l'innalzamento della sicurezza da parte delle Banche e la doppia verifica sul telefono del titolare. Sussistendo, infatti, la necessità di acquisire i codici autorizzativi, i criminali riescono ad ottenere dai gestori un duplicato della SIM della vittima (con la scusa di averla smarrita o che gli è stata rubata) ove ricevono i codici autorizzativi per le operazioni fraudolente.

L'attività di questa Specialità nel settore del *Financial Cybercrime* è svolta a 360°, sia in ambito informativo, con campagne mirate di informazione rivolte sia alle Law Enforcement (reparti non specializzati in materia di Cyber) che al pubblico, anche attraverso i *social* ufficiali, sia particolarmente in ambito investigativo.

Per tale attività di *intelligence*, oltre alla tempestività adottata su tutto il territorio nazionale, ci si avvale anche della collaborazione internazionale sia in ambito europeo che extraeuropeo. Nei casi di prontezza di reazione delle vittime e, quindi, nell'immediatezza dei fatti, la Polizia Postale e delle Comunicazioni riesce a conseguire buoni risultati ai fini del recupero delle somme distratte ed all'identificazione degli autori.

Tale protocollo operativo risulta di più difficile attuazione quando ci si trova a dover collaborare con alcuni Paesi extraeuropei.
Fondamentale è l'apporto della piattaforma OF2CEN *(On Line Fraud Cyber Centre and Expert Network)*, realizzata appositamente al fine di prevenire e contrastare le aggressioni criminali ai servizi di home banking e monetica, con la quale viene svolta un'accurata analisi delle frodi in esame. Tale struttura informatica è frutto di specifiche convenzioni con le principali banche, con **ABI** e con gran parte del mondo bancario e quindi consente di intervenire in tempi ristretti sulle segnalazioni.

È da segnalare la partecipazione, fra i vari tavoli di lavoro internazionali, a quello denominato EMMA (European Money Mule Action), giunto oramai alla sua settima edizione.
Aderiscono, unitamente a questa Specialità, altri 26 Stati Europei e l'Agenzia Europol, che in un periodo di tempo concertato lavorano in sinergia, svolgendo indagini congiunte, effettuando provvedimenti dell'Autorità Giudiziaria, identificando i titolari dei conti correnti, collaborando in tempo reale con gli altri Paesi coinvolti nell'operazione, con risultati investigativi di notevole rilievo.
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 **7.000 transazioni bancarie fraudolente**, sono state avviate oltre **2.500 autonome indagini**, riuscendo a prevenire frodi per un **danno stimato in 67,5 milioni di euro**. **Più di 18.000 i muli individuati, 324 organizzatori e coordinatori di muli identificati.**

I risultati possono essere riassunti come nella tabella riportata di seguito:

TIPO	1° Sem.2021	1° Sem.2022	Variazione %
Numero di Frodi di interesse internazionale in danno di grandi e medie imprese investigate dalla Polizia Postale e delle Comunicazioni con l'ausilio della piattaforma F.I.S.A. – Financial Investigation Smart Analysis	44	86	+95%
Casi trattati sul territorio nazionale	7329	4734	-35%
Persone Indagate nel territorio nazionale	437	438	+0,2%

Di seguito, un dettaglio delle **operazioni più significative** portate a termine dalla Specialità nell'azione di contrasto ai richiamati fenomeni delittuosi nel primo semestre del 2022.

Operazione "BOLTON"

Sotto la direzione e il coordinamento della Procura della Repubblica di Cagliari, personale della Specialità della Polizia Postale e delle Comunicazioni e della Guardia di Finanza ha dato esecuzione a misure cautelari personali e patrimoniali disposte dal Giudice per le indagini preliminari del Tribunale di Cagliari nei confronti di sei persone gravemente indiziate, unitamente ad altri quattro indagati denunciati a piede libero, per i delitti di associazione per delinquere finalizzata all'abusivismo finanziario, alla truffa, al riciclaggio ed autoriciclaggio, per aver costituito un reticolo di società finanziarie, anche di diritto estero strumentali al procacciamento di clienti.

Proprio grazie alle predette società, gli indagati hanno infatti esercitato, in assenza delle prescritte autorizzazioni, un'attività finanziaria promuovendo la compravendita di strumenti finanziari dietro la promessa di profitti elevati, pari al 5% lordo mensile, indi ripagando gli incauti investitori, idealmente rassicurati da rendimenti particolarmente favorevoli in tempi molto brevi, con fondi raccolti presso nuovi clienti applicando in sequenza il noto "schema Ponzi"; ciò, finché non è "crollata" la catena di raccolta del denaro.

Alla prima scadenza annuale dell'investimento, infatti, solo alcuni investitori sono rientrati in possesso di parte delle somme investite e la maggior parte di essi non ha ottenuto alcun rendimento, né la restituzione dei capitali raccolti sull'intero territorio nazionale, per circa 5 milioni di euro, ai danni degli ignari risparmiatori.

Il sodalizio criminale investigato, strutturato in modo piramidale, vedeva al suo vertice il *dominus* delle società, un uomo di anni 51, ritenuto promotore ed organizzatore del sistema illecito, e ad un livello inferiore, i suoi più stretti collaboratori: il fratello, di anni 41 e la sorella, di anni 46, tutti residenti in provincia di Cagliari. Della compagine associativa sono risultati appartenere anche una donna, di anni 51, residente in provincia di Varese, responsabile del "marketing"; un uomo, di anni 47, residente a Como, quale cofondatore e comproprietario di alcune società offerenti gli investimenti finanziari abusivi; un altro uomo di nazionalità saudita, di anni 48, residente in Svizzera e che ha amministrato il flusso di denaro proveniente dall'abusiva raccolta del risparmio, ed un uomo di anni 39 residente ad Olbia, che ha ideato il progetto iniziale d'investimento, in qualità di formale proprietario di una società slovena.

Sono risultati coinvolti, inoltre, tre promotori finanziari, due uomini ed una donna, rispettivamente di anni 39, 35 e 33, residenti nell'oristanese e nel sud Sardegna.

L'attività investigativa svolta dal Compartimento della Polizia Postale e delle Comunicazioni di Cagliari nasce proprio a seguito delle denunce di truffa sporte da diversi cittadini cagliaritani. Il Pubblico Ministero inquirente, conseguentemente, ha delegato, allo stesso Compartimento, lo sviluppo delle denunce delle vittime nonché il rintraccio delle ulteriori centinaia di investitori truffati, sparsi su tutto il territorio nazionale, l'audizione di testimoni, l'esecuzione di innumerevoli attività di intercettazioni telefoniche e telematiche volte a ricostruire lo schema illecito utilizzato e la rete posta in essere dagli indagati.

Si è trattato di un'attività d'indagine minuziosa, dettagliata e articolata, caratterizzata da approfondite e complesse analisi di numerosissime operazioni finanziarie, dall'ascolto e

trascrizione di conversazioni telefoniche e telematiche estrapolate dagli apparecchi cellulari e informatici sequestrati agli indagati.
Al Nucleo di Polizia Economico-Finanziaria della Guardia di Finanza di Cagliari sono state contestualmente delegate dal P.M. indagini finanziarie e patrimoniali, consistite nell'analisi delle movimentazioni di danaro transitato sui conti correnti dei soggetti e delle società coinvolti, le cui risultanze sono state incrociate con gli approfondimenti delle segnalazioni di operazioni sospette inoltrate dagli intermediari finanziari, arricchiti con le informazioni acquisite mediante i canali di cooperazione internazionale utili per reperire dalla rete delle Financial Intelligence Units estere, in attuazione della normativa nazionale e delle Direttive antiriciclaggio dell'Unione Europea, le informazioni occorrenti per contrastare, tra gli altri, i fenomeni di riciclaggio e reimpiego di proventi illeciti da parte delle organizzazioni criminali, reati presupposto a esso associati e finanziamento del terrorismo.
Tale forma di proficua collaborazione, caratterizzata anche dalla congiunta esecuzione di perquisizioni e sequestri, ha consentito agli Organi inquirenti di individuare i rapporti finanziari sui quali sono transitati i risparmi sottratti alle vittime, nonché di individuare ulteriori società estere, amministrate da prestanome e utilizzate per occultare l'origine dei capitali illecitamente raccolti ed impedirne la tracciabilità.
A conclusione dell'attuale fase delle indagini, dunque, la Polizia Postale e delle Comunicazioni ha dato esecuzione a sei provvedimenti cautelari personali (una custodia in carcere, una misura degli arresti domiciliari e quattro di sottoposizione degli indagati all'obbligo di dimora presso il comune di residenza), mentre le Fiamme Gialle hanno eseguito il sequestro preventivo, finalizzato alla confisca anche per equivalente, di beni e disponibilità finanziarie per un importo complessivo di oltre 4.500.000 euro nei confronti del *dominus* dell'organizzazione, per i reati di riciclaggio e autoriciclaggio.
Tra i beni sequestrati vi sono disponibilità finanziarie, quote societarie ed una struttura alberghiera ubicata nell'*hinterland* cagliaritano, del valore stimato di circa 1.500.000 euro, la cui acquisizione da parte del *dominus* dell'associazione criminale è avvenuta mediante il coinvolgimento di un prestanome.

Operazione "Moscow Mule 2"

La Polizia di Stato ha arrestato una cittadina russa appartenente ad un'organizzazione criminale transnazionale dedita alle frodi informatiche di ultima generazione, alla ricettazione ed al riciclaggio.
Gli investigatori del Compartimento Polizia Postale e delle Comunicazioni di Genova, coordinati dalla locale Procura della Repubblica, hanno ottenuto l'aggravamento degli arresti domiciliari e hanno arrestato nuovamente M.N., 40enne cittadina russa.
La donna era già stata arrestata nel capoluogo ligure nel mese di ottobre 2021. Nella vita di tutti i giorni si nascondeva dietro alla parvenza di una tranquilla madre di famiglia, in realtà si trattava di un'avvenente esperta *hacker*: un ingegnere informatico con la passione per il crimine e le cryptovalute.
Il Tribunale di Genova, nel mese di marzo 2022, aveva concesso alla donna gli arresti

domiciliari presso un'associazione di volontariato del centro genovese impegnata nel recupero dei detenuti.
Le particolari attitudini e l'alto profilo criminale hanno indotto gli investigatori della Polizia Postale a pianificare stretti contatti con la struttura presso la quale "l'ingegnere" era stata posta agli arresti domiciliari. Le continue richieste della donna di poter utilizzare un telefono o un computer avevano, infatti, ulteriormente insospettito gli investigatori, inducendoli a predisporre delle attività tecniche di intercettazione ambientali e telematiche.
Da queste si è potuta avere la certezza che la donna, nonostante fosse agli arresti domiciliari avesse da subito cercato di riorganizzarsi, iniziando nuovamente a intessere rapporti con altri appartenenti al sodalizio criminale risiedenti all'estero e con questi a commettere frodi informatiche a danno di ignari cittadini.
L'*hacker* ha oltremodo dimostrato la propria capacità criminale avvedendosi dell'intercettazione telematica e procedendo ripetutamente in continui tentativi di eludere le investigazioni e di cancellare le prove a suo carico.
Nel corso della perquisizione domiciliare, gli esperti della Sezione Financial Cybercrime della Polizia Postale hanno sequestrato numeroso materiale, tra l'altro reperito dalla donna durante la detenzione domiciliare, che è tuttora sottoposto ad esame per ulteriori risvolti investigativi.

Operazione "Perugia"

Questa Specialità unitamente ai Carabinieri ha dato esecuzione a un Provvedimento emesso dal Tribunale di Perugia che ha disposto le misure cautelari nei confronti di undici soggetti per frodi informatiche, indebiti utilizzi di carte di credito e truffe finanziarie. Sono state complessivamente eseguite 4 misure cautelari in carcere, 4 arresti domiciliari e per altri 3 è stato disposto l'obbligo di presentazione alla polizia giudiziaria.
Le indagini hanno svelato ruoli e compiti di ogni singolo componente il *cui modus operandi* era sostanzialmente il seguente: le truffe venivano realizzate mediante l'utilizzo di sistemi informatici o telematici (phishing); i componenti dell'associazione -mediante l'invio di SMS (smishing) o tramite delle chiamate telefoniche (vishing) - dopo aver "agganciato" l'ignara vittima e spacciandosi per operatori bancari si facevano consegnare í codici autorizzativi ed eseguivano operazioni di prelievo veicolando la somma fraudolentemente incassata in uno dei vari sportelli ATM dislocati sul territorio.
Successivamente gli indagati, al fine di garantirsi l'anonimato e rendere al contempo più difficile il loro rintraccio, per mezzo di intermediari (Money Mules) - che operavano con la prospettiva di ottenere una commissione -, tramite sportelli ATM, trasferivano il denaro fraudolentemente acquisito su altri conti "dedicati" e gestiti dagli stessi componenti dell'associazione.
L'articolata e complessa attività d'indagine ha avuto inizio da una denuncia per estorsione. Dai successivi accertamenti, è emerso che in realtà si trattava di una frode informatica che, mediante sofisticate tecniche di raggiro, inducevano la vittima designata a credere di interfacciarsi con siti istituzionali e, per tale motivo, a fornire le proprie credenziali di accesso ai dati bancari.

Tale sodalizio criminale - dotato di molteplici utenze e apparati telefonici ed informatici - si avvaleva di numerosi gregari, di volta in volta reclutati con il ruolo di intermediari, per procedere all'incasso e alla ripartizione dei proventi economici derivanti dalle attività illecite poste in essere.
Determinante e strategico era - all'interno dell'associazione - il ruolo proprio degli intermediari: a questi era deputato il compito di aprire i rapporti finanziari a loro nome sui quali venivano fatti confluire i proventi delle attività illecite che venivano messi successivamente a disposizione degli altri membri del sodalizio.
Sempre agli intermediari era deputato il compito di sottoscrivere finanziamenti (con istituti di credito o finanziarie), poi destinati a rimanere insoluti atteso l'utilizzo anche di falsi documenti. L'attività delittuosa descritta, nel solo mese di maggio 2021, ha fruttato al gruppo criminale un illecito profitto di oltre euro 100 mila a cui si sono aggiunti circa 130 mila euro di proventi derivanti dalle cosiddette truffe "finanziarie" (acquisto di auto tramite finanziamenti e richieste prestiti).
Le indagini - che hanno richiesto una conoscenza tecnica nel settore dei reati informatici da parte degli investigatori di entrambe le Forze di Polizia - hanno consentito di ricostruire una molteplicità di episodi delittuosi utili a richiedere ed ottenere il provvedimento cautelare eseguito nella giornata odierna.
L'acquisizione dei gravi indizi di colpevolezza è stato possibile anche grazie alla fattiva collaborazione di diversi Uffici del territorio della Specialità della Polizia Postale e delle Comunicazioni, nonché dei diversi Comandi Stazione dell'Arma dei Carabinieri competenti sul territorio.
Nel corso dell'esecuzione delle misure, uno degli indagati - sottoposto all'obbligo di presentazione alla polizia giudiziaria - trovato in possesso di alcuni documenti di identità falsi, è stato tratto in arresto in flagranza di reato.

Nell'ambito della prevenzione e contrasto della diffusione di contenuti terroristici online, il costantemente monitoraggio del web effettuato dalla Polizia Postale e delle Comunicazioni ha permesso di riscontrare il continuo e vertiginoso incremento dell'utilizzo delle piattaforme di comunicazione online, social network e di applicazioni di messaggistica istantanea, ed il conseguente allarmante incremento della diffusione di contenuti propagandistici riconducibili al terrorismo, ad una platea pressoché illimitata, sia di matrice islamista (jihadista, ISIS, Al Qaeda, Al Shabaab ed altre articolazioni locali), sia di formazioni di estrema destra (neonazismo, neofascismo, tifoserie strutturate, suprematismo), nonché di estrema sinistra (movimenti di lotta armata, anarchici, insurrezionalisti, antagonisti).
In tale ambito, la Polizia Postale garantisce sia l'esecuzione di una costante attività di monitoraggio investigativo della rete e dei canali di messaggistica istantanea, per l'identificazione e il deferimento all'Autorità Giudiziaria dei responsabili della diffusione dei contenuti illeciti, sia un costante scambio informativo con la Direzione Centrale della Polizia di Prevenzione e con le Agenzie di Intelligence, competenti in materia di contrasto al terrorismo.

		Eversione Internazionale Politico Religiosa Eversione Nazionale Politica - Attività in circostanze di emergenza			
		Casi trattati	**Persone indagate**	**Spazi Virtuali Monitorati**	**Spazi Virtuali con contenuti illeciti rilevati**
2021	**Dal 01/01/2021 al 30/06/2021**	622	25	51.914	738
2022	**Dal 01/01/2022 al 30/06/2022**	881	32	79.601	700
	Variazione %	+33%	+28%	+53%	-5%

Trattandosi, in particolare, di un fenomeno di carattere transnazionale, sia per la natura internazionale del fenomeno, che per la stessa connaturata struttura della rete, risulta imprescindibile l'attivazione efficiente degli strumenti della cooperazione sovranazionale, soprattutto per la condivisione di informazioni che, collegate a situazioni peculiari interne, riescono ad apportare un indiscusso valore aggiunto alle attività di prevenzione messe in atto dalle diverse forze di polizia nazionali.
In ambito europeo, proprio al fine di garantire la cooperazione internazionale, il Servizio Polizia Postale e delle Comunicazioni rappresenta il punto di contatto nazionale dell'Internet Referral Unit (IRU) di Europol, Unità preposta a ricevere dai Paesi Membri le segnalazioni relative ai contenuti terroristici diffusi in rete e di orientarne l'attività.
In tale ambito, l'attività di monitoraggio del web effettuata dalla Specialità ha permesso di riscontrare in primis come la diffusione di messaggi propagandistici jihadisti, nel corso del tempo, abbia subito un sensibile peggioramento qualitativo, determinato sia dal ridimensionamento del Califfato sul territorio, sia dalle perdite di tecnici e social media manager cui era devoluto l'incarico di gestire la propaganda.
Diversamente, nel caso della propaganda online legata all'estremismo razzista e xenofobo, il trend di forum e discussioni dedicate all'argomento risulta in costante aumento.
In particolare, è stata riscontrata la presenza di numerose board – diverse dai principali social network, come, ad esempio, 4Chan, 8Chan, DioChan, Gab, Reddit – destinate alla diffusione di opinioni xenofobe e razziste e/o di commenti e "meme" connotati da hate speech.
In seguito a tale evidente innalzamento del rischio, si è assistito ad un parallelo incremento del livello di attenzione anche nei tavoli di lavoro internazionali, e, proprio in seno all'E.U. Internet Forum, personale di questo Servizio Polizia Postale e delle Comunicazioni ha contribuito – con la partecipazione dei rappresentanti degli Stati Membri e di Europol, nonché di alcuni delegati delle maggiori compagnie fornitrici di servizi internet (tra le quali Facebook, Google, Microsoft, Telegram, Twitter, Snap, JustPaste.it e Dropbox) – all'elaborazione di

un protocollo di crisi dell'Unione Europea finalizzato al contrasto ed al contenimento della rapida diffusione virale di contenuti terroristici e di estremismo violento online.
Ed ancora, sebbene i decreti governativi di contenimento dell'emergenza socio-sanitaria determinata dalla pandemia negli ultimi mesi abbiano disposto sempre meno restrizioni, la Polizia Postale è stata chiamata a garantire una rilevante attività di monitoraggio dei canali e gruppi, all'interno delle varie piattaforme di comunicazione online, nelle quali sono stati pubblicati numerosi commenti con l'obiettivo di organizzare vere e proprie azioni di piazza non consentite, anche violente.
Nell'ambito del contenimento e del contrasto della minaccia ibrida, la Polizia Postale sta svolgendo dedicati approfondimenti info-investigativi sul tema della disinformazione e del ruolo delle *fake news* anche con riferimento all'attuale scenario di crisi internazionale.
In tale contesto informativo, il monitoraggio è volto ad individuare tempestivamente la diffusione di *fake news* sul conflitto bellico in atto che possano assumere il carattere della viralità, determinando un rischio per l'ordine e la sicurezza pubblica.
In particolare, è stato possibile riscontrare come, già dalle prime ore dall'inizio del conflitto, sebbene diverse piattaforme abbiano dichiarato di aver inibito la diffusione degli spot politici russi a pagamento, all'interno di numerosi social network con *policy* meno stringenti, è stata riscontrata la presenza di numerosi gruppi gestiti e frequentati da contestatori e cospirazionisti "anti-sistema", fino a pochi giorni prima noti per le posizioni "NoVax". In tale contesto, è emerso come i negazionisti dell'emergenza sanitaria da Covid-19, ora, abbiano assunto posizioni filorusse ed un ruolo attivo nella diffusione della propaganda.
Giova sottolineare, infine, come l'attuale scenario bellico abbia determinato un costante e tempestivo scambio informativo con la Direzione Centrale della Polizia di Prevenzione e con le agenzie di intelligence in merito alla diffusione, all'interno di numerose piattaforme di comunicazione online prevalentemente frequentati da soggetti provenienti da vari Stati europei, di messaggi in cui si esorta il reclutamento di volontari, a sostegno dei combattenti del "Battaglione Azov", sia attraverso donazioni in denaro corrente/cripto, sia mediante l'indicazione di informazioni logistiche utili a raggiunger il fronte ucraino.
Proprio in tale contesto informativo, sono stati identificati alcuni internauti riconducibili al territorio nazionale che hanno espresso la volontà di recarsi in Ucraina e prendere parte al conflitto in corso, nei cui confronti sono in corso dedicate attività di monitoraggio, in raccordo con gli Uffici di Prevenzione.
Infine, appare opportuno evidenziare come la Polizia Postale stia analizzando con attenzione l'evoluzione dell'utilizzo dell'intelligenza artificiale, anche nell'ambito circoscritto alla diffusione della propaganda terroristica online.
L'I.A., infatti, negli ultimi anni ha contribuito ad un innalzamento vertiginoso di effetti destabilizzanti sull'opinione pubblica che, a riscontro di quanto già emerso, si sono vissuti già nel periodo dell'emergenza pandemica, proseguendo anche con riferimento alla tematica della guerra tra Russa e Ucraina, per inserirsi anche nella recente campagna elettorale italiana.

L'allarme di tale fenomeno, invero, è stato lanciato dagli stessi gestori delle piattaforme social, i quali hanno reso noto come attraverso l'uso di "profili falsi" e "bot", fonti esterne non meglio identificate abbiano alimentato, in taluni casi sfiducia verso le istituzioni politiche, sanitarie e sociali, in altri la promozione di pubblicità online di contenuti politici tendenziosi.
Di fondamentale importanza, legata all'utilizzo d'identità fittizie, è risultato l'utilizzo del "GAN" (Generative Adversarial Networks) - tecnica d'intelligenza artificiale il cui obiettivo è generare immagini indistinguibili da quelle reali - impiegata generalmente per la creazioni di video deep-fake, che ha consentito una maggiore diffusione dei contenuti subdolamente creati ed ha permesso di costituire una rete di utenti fake che hanno aumentato, in tale modo, la loro credibilità sul mondo smisurato del cyberspazio.
L'intelligenza artificiale tecnologicamente avanzata, sfruttata dagli stessi social network, riesce a distinguere le tendenze più basilari – tramite comandi semplici come il *like* – da quelle dai contenuti più complessi. Questi sofisticati algoritmi in grado di razionalizzare le azioni in rete hanno imparato a riconoscere i gusti e le preferenze dei singoli utenti, suggerendo contenuti ed oscurandone altri, opprimendo di fatto il processo di democratizzazione tanto celebrato nell'era e negli ambienti social.

Commissariato di P.S. Online

L'uso crescente delle nuove tecnologie ha reso necessario lo sviluppo e il potenziamento di nuovi strumenti di comunicazione che consentisse alla Polizia di Stato di mettersi in contatto diretto con gli utenti del *web*.
In tale ottica il portale del Commissariato di PS online ha permesso al cittadino, abituato ormai a utilizzare la rete internet per svolgere le principali attività quotidiane, di rivolgersi agli agenti della Polizia Postale in qualsiasi momento e ovunque si trovi. Attraverso il computer l'utente può esprimere il proprio disagio per un torto subito, segnalare comportamenti che giudica illeciti e chiedere aiuto per superare difficoltà e problematiche, anche nei casi in cui potrebbe essere fonte di disagio rappresentarle di persona.
La facilità con cui il cittadino riesce ad interagire con la piattaforma dedicata rende possibile raccogliere le segnalazioni di quegli utenti che, mossi da spirito altruistico e di collaborazione, si rivolgono alla Polizia Postale e delle Comunicazioni in un'ottica di sicurezza partecipata - nella sua declinazione online - fornendo utili evidenze su fenomeni emergenti potenzialmente lesivi, così contribuendo, in termini di efficace prevenzione, ad evitare che altri internauti possano cadere nelle trappole della Rete: grazie al servizio online dedicato all'inoltro di segnalazioni e alla richiesta di informazioni accessibile dal portale, infatti, gli operatori della Specialità, possono orientare l'analisi rispetto a condotte delittuose anche emergenti ed elaborare idonee strategie di contrasto.
L'analisi delle 57.397 segnalazioni ricevute dal sito del Commissariato di PS online nel primo semestre 2022, numero in aumento rispetto all'analogo periodo dell'anno precedente, ha evidenziato che in molti casi gli internauti non adottano quelle piccole e necessarie accortezze di igiene informatica che consentirebbero di prevenire e limitare la maggior parte

degli attacchi informatici e il perpetrarsi di attività delittuose. Per questo motivo, è stata introdotta sul sito una specifica sezione dedicata alla c.d. "*cyber hygiene*" con cui vengono veicolate al cittadino pillole di sicurezza informatica funzionali a ridurre al minimo i rischi legati all'uso di dispositivi informatici.
L'esigenza di innalzare al massimo i livelli dell'azione preventiva ha imposto di introdurre una nuova sezione, dedicata agli *alert*, dove vengono raccolti e pubblicati gli "avvisi agli utenti" che, proprio perché costantemente aggiornati e facilmente raggiungibili, costituiscono un efficace strumento di autotutela messo a disposizione del cittadino. Tra i fenomeni riscontrati con maggior frequenza in questo primo semestre annoveriamo, a titolo esemplificativo, i furti di *account social*, le estorsioni a sfondo sessuale, il *phishing* ai danni di correntisti di istituti bancari, i falsi investimenti online, nonché falsi siti di vendita di quei prodotti che, in un determinato contesto temporale, risultano essere maggiormente richiesti sul mercato.

Campagne preventive di sensibilizzazione

Nell'ambito dell'attività di prevenzione svolta dalla Specialità, oltre al monitoraggio continuo del *web*, 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.
Le opportunità di incontro con i giovani internauti, principalmente nel mondo della scuola, portate avanti anche in videoconferenza, hanno riscosso consensi e partecipazione da parte di alunni, genitori e insegnanti, consentendo 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 li vedono spesso protagonisti.
Tra le iniziative più significative si inserisce "Una vita da Social", la campagna itinerante attraverso la quale la Polizia Postale e delle Comunicazioni incontra, in collaborazione con gli istituti scolastici, studenti, docenti e genitori. Con il ritorno nell'anno scolastico appena concluso dei ragazzi in aula, è stato possibile organizzare, per la 9^ edizione, nuovamente incontri *de visu* con la platea scolastica, ripristinando - dopo il periodo interessato dalle misure di contenimento per la pandemia da Covid - la caratteristica di campagna itinerante del progetto. A bordo del *truck* che contraddistingue l'iniziativa, che si trasforma in una vera e propria aula multimediale, sono state accolte dagli operatori della Specialità le numerose scolaresche interessate, alle quali sono state illustrate le possibili insidie della Rete e forniti utili strumenti per un corretto utilizzo del *web*.
L'azione preventiva attuata si rivolge ormai da anni, 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 fornite agli spettatori informazioni utili alla corretta navigazione in rete, volte anche a stimolare nei ragazzi una sempre maggiore consapevolezza della gravità delle azioni prodotte online, in relazione all'impatto prodotto nella vita dei loro coetanei. Per l'anno 2022, la 6^ edizione della citata manifestazione è stata realizzata in data 8 febbraio, in occasione del *safer internet day*, giornata mondiale per la sicurezza in rete, con un grande evento online, durante il quale la Polizia Postale e delle Comunicazioni si è collegata, attraverso una piattaforma dedicata, con oltre 270 mila studenti.
L'impegno profuso dagli specialisti della Polizia Postale e delle Comunicazioni nell'azione di sensibilizzazione e informazione ha consentito, da settembre 2021 ad oggi di realizzare incontri, ai quali hanno preso parte anche docenti e genitori, con oltre 2.300 istituti scolastici coinvolti e di veicolare contenuti educativi a più di 750.000 studenti.
Il 17 marzo u.s., inoltre, è stato presentato, presso l'Auditorium parco della musica di Roma, alla presenza del capo della Polizia, Prefetto Lamberto Giannini, il docufilm "Haters e piccoli eroi", con protagonista Valerio Catoia, ragazzo con la sindrome di down nominato "Alfiere della Repubblica" e "Poliziotto ad honorem". Il video è stato realizzato dalla Polizia di Stato in collaborazione con l'istituto di cinematografia "Roberto Rossellini" di Roma e narra la storia di questo ragazzo speciale, raccontata da ragazzi come lui, attraverso il linguaggio degli adolescenti, per combattere il cyberbullismo. Valerio è un campione dei Gruppi sportivi paralimpici italiani e, a soli 17 anni, ha salvato da sicuro annegamento una bambina di 10 anni travolta dalle onde del mare. Nonostante il gesto eroico e i riconoscimenti istituzionali conseguiti, è stato oggetto di ripetuti insulti sui canali social. Grazie anche al sostegno della famiglia e all'intervento della Polizia Postale e delle Comunicazioni, Valerio ha trovato la forza di reagire a questa situazione ed oggi è diventato il *testimonial* della campagna della Polizia Postale e delle Comunicazioni per prevenire il fenomeno del cyberbullismo tra gli adolescenti. All'evento hanno assistito oltre 1000 studenti delle scuole di Roma.

Geopolitica e Cybersecurity

[A cura di Carlo Mauceli, Microsoft]

La guerra informatica a supporto della guerra convenzionale e delle strategie politiche dei singoli Stati

Il 23 febbraio 2022, il mondo della cybersecurity è entrato, definitivamente, in una nuova era; l'era della guerra ibrida. Quel giorno, diverse ore prima che la Russia lanciasse i primi missili contro l'Ucraina e i carri armati ne attraversassero i confini, alcuni "attori" russi cominciarono un massiccio attacco informatico contro le infrastrutture tecnologiche e finanziarie dello stato ucraino.

Il 18 luglio 2022, il governo albanese ha denunciato di aver subito un "massiccio attacco cibernetico, mai avvenuto prima", costringendo la chiusura temporanea di tutti i siti governativi e fermando i servizi pubblici online, ovvero il 90% dei servizi offerti dall'amministrazione pubblica.

Nel mese di giugno del 2022, un attacco informatico ha temporaneamente messo fuori uso i siti web pubblici e privati in Norvegia. L'attacco DDOS (Distributed Denial-of-Service) aveva preso di mira una rete di dati nazionale considerata sicura costringendo la sospensione temporanea dei servizi online per diverse ore dopo l'incidente.

Un paio di giorni prima era stata la volta della Lituania i cui siti web pubblici e privati erano stati messi fuori uso da un gruppo di hacker vicini a Mosca che avrebbe, a sua volta, rivendicato la responsabilità dell'attacco.

In questo scenario, la Nato ha più volte ribadito che "**un attacco cyber rivolto ad una nazione è un'aggressione a tutti i paesi membri**". L'articolo 5 dell'Alleanza atlantica che sancisce il diritto alla difesa collettiva, scatterebbe immediatamente poiché la Nato considera lo spazio cibernetico una nuova dimensione degli scontri armati al pari di terra, cielo, aria e spazio.

Ai nostri giorni, la guerra aperta è possibile solo in scenari periferici e a condizione che gli eserciti delle maggiori potenze non si confrontino direttamente sul campo. La recente storia dimostra che azioni di guerra possono essere condotte solo come guerra indiretta attraverso il confronto fra soggetti minori, protetti ciascuno da una grande potenza, oppure sotto forma di guerra coperta o, meglio ancora, catalitica, dove un soggetto scatena una guerra fra due suoi concorrenti, restando nell'ombra.

L'uso di forme di guerra coperta deve accompagnarsi ad altre forme di guerra non militare, come, ad esempio, la destabilizzazione politica, la guerra economica, i sabotaggi, le sanzioni, ecc. e deve avere una certa flessibilità, così da modularsi secondo le esigenze, momento per momento.

È in tale contesto che la cyber war viene ad assumere un ruolo centrale e strategico sovvertendo però, per certi versi, le tradizionali gerarchie di potere.

Ci troviamo di fronte a quello che viene, comunemente definito, **Sharp Power** finalizzato a:

- influenzare l'opinione pubblica attraverso la propaganda e la manipolazione dell'informazione. Ad esempio, la Russia ha sostenuto la sua guerra con operazioni di propaganda per influenzare le opinioni nella stessa Russia, in Ucraina ed anche a livello globale;
- penetrare nell'economia del Paese agendo sul sistema di import/export e sui principali nodi logistici commerciali;
- incidere sulle scelte politiche dello stato in questione non esitando a ricorrere a pratiche ricattatorie.

A guidare tale sistema di conflitto non possono che essere i servizi di intelligence dei vari paesi.
Mentre l'intelligence della seconda metà del Novecento era, in massima parte, ideologica, quella attuale si muove in una prospettiva geopolitica e geoeconomica. Mentre le strategie precedenti avevano al centro l'obiettivo del controllo territoriale, quella attuale ragiona in termini di reti di connessione.
L'enorme raccolta di dati impone tecniche di integrazione, verifica, trattamento e analisi per i quali i servizi si sono dotati di sofisticati sistemi basati su algoritmi e, a volte, i risultati sono rivenduti a imprese industriali e finanziarie. Si tratta di una ricaduta di quella guerra senza limiti che è già cominciata e che porrà problemi drammatici soprattutto ai sistemi democratici. Buona parte della battaglia si svolgerà proprio sul campo della cyber war.
Lo spionaggio esiste da sempre ma ciò che è cambiato, in modo radicale, è la tecnologia che fornisce a quasi tutte le organizzazioni capacità di intelligence innovative. Con la crescente dipendenza dalla tecnologia, lo spionaggio informatico provoca il caos e ostacola lo sviluppo del business sfruttando il cyber spazio per ottenere informazioni riservate appartenenti ad un governo, a un'organizzazione o a specifici individui.
Lo scopo è quello di produrre guadagni netti, per quanto, chiaramente, si tratti di pratiche illegali. Le tecnologie utilizzate per le intrusioni informatiche segrete sono sia avanzate ma, molto spesso, già utilizzate in passato perché consolidate.

Chi sono queste organizzazioni? Di chi stiamo parlando? Da chi vengono sponsorizzate?
Un'organizzazione State Sponsored è un gruppo sponsorizzato dal governo che attacca con forza e ottiene l'accesso illecito alle reti di altri governi o a gruppi industriali per rubare, danneggiare o modificare le informazioni.
Microsoft identifica questi attori con i nomi degli elementi chimici e ha definito questa mappa che ben inquadra il conflitto attuale in cui gli attaccanti appartengono all'emisfero orientale.

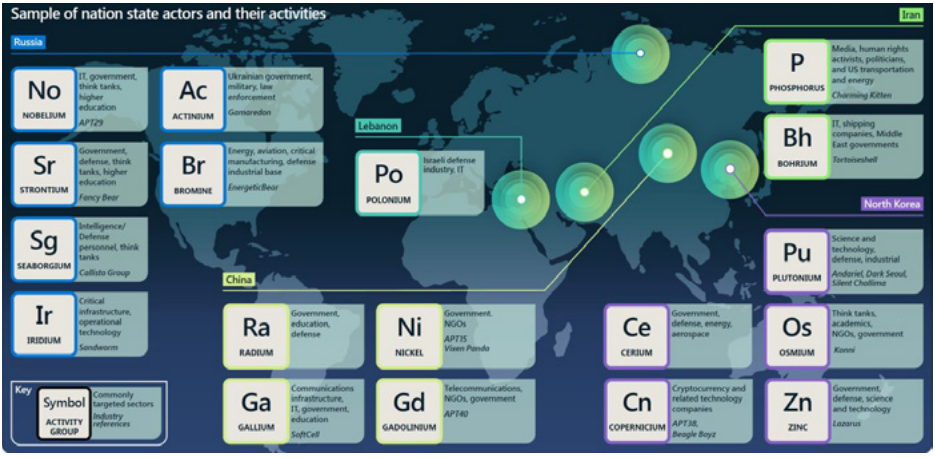


Figura 1 - *Mappa degli State Actor*

Il conflitto russo ucraino ha insegnato moltissimo. In primo luogo, in un mondo che è dominato dall'ideologia del sovranismo, la sicurezza delle operazioni e dei dati digitali può e deve essere migliorata, sia nel cyberspazio che nello spazio fisico, grazie all'utilizzo dei servizi cloud. Non è un caso che i primi attacchi russi hanno preso di mira i servizi on-premise con l'utilizzo di un malware wiper mentre, contestualmente, i missili venivano lanciati sui Datacenter fisici. L'Ucraina ha risposto spostando rapidamente i servizi e i dati su cloud hyperscale ospitati nei datacenter al di fuori del Paese.
In secondo luogo, i progressi nell'ambito della Cyber Threat intelligence e della protezione degli endpoint, alimentate dall'artificial intelligence e dal Machine Learning, tipici dei servizi cloud, hanno aiutato l'Ucraina a difendersi contro gli attacchi informatici russi.
Altrove, gli state actor sono aumentati e attraverso l'utilizzo di tecnologie sempre più innovative, hanno cominciato ad attaccare un insieme sempre più ampio di obiettivi sfruttando la debolezza della supply chain.
Il patching, la protezione dell'identità, l'hardening dei sistemi e la messa in sicurezza delle reti diventano sempre più importanti in uno scenario in cui le tecniche di attacco migliorano e si modificano utilizzando, spesso, software opensource o anche legittimo.
Oriente e Occidente sono riferimenti quasi risibili in termini informatici dal momento che nello spazio cibernetico regna oggi il caos di un conflitto di tutti contro tutti, pieno di nemici da cui difendersi e con pochi alleati di cui diffidare. Dall'Iran all'Albania, dagli USA alla Russia passando per l'Ucraina, la Finlandia, Israele e chissà chi altro partono attacchi e contrattacchi informatici a sistemi energetici, produttivi, militari ed economici. Un contesto nel quale si confondono interessi nazionali, strategici e criminali.

È, comunque, un dato di fatto che gli attori principali sono Russia, Cina, Nord Corea e Iran che operano secondo una distribuzione che ha visto USA e UK come i target principali. Ma anche Germania, India, Canada, Svizzera ed Israele sono stati degli obiettivi significativi nel 2022 per non parlare di Paesi più piccoli che hanno rappresentato il target preferito dalla Cina.

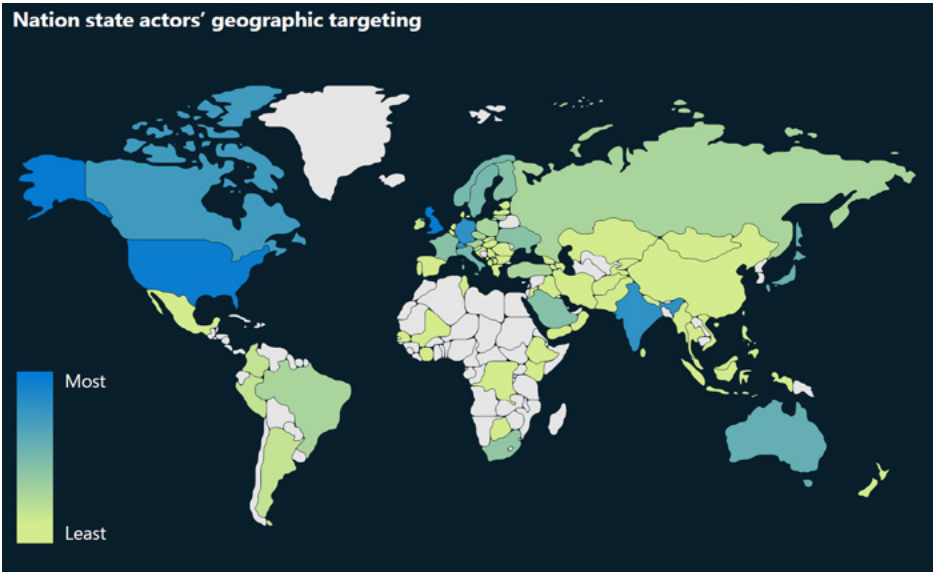


Figura 2 - *Geografia degli obiettivi degli State Actor*

In uno scenario simile, è necessario avere un quadro globale coerente che dia priorità ai diritti umani e che protegga le persone perché è chiaro che non si tratta soltanto di attacchi alle aziende bensì di compromissione e di attacco all'intera società. Tutte le nazioni devono lavorare per attuare norme e regole concordate.
Le infrastrutture critiche sono sempre più oggetto di attacchi con un incremento significativo negli ultimi tre anni tanto che se prima dell'invasione dell'Ucraina i governi pensavano che i dati dovessero rimanere all'interno di un Paese per essere sicuri, dopo l'invasione, la migrazione dei dati nel cloud e il loro spostamento al di fuori dei confini territoriali è diventata la pratica maggiormente adottata per garantire la resilienza dei servizi ed una maggiore sicurezza.

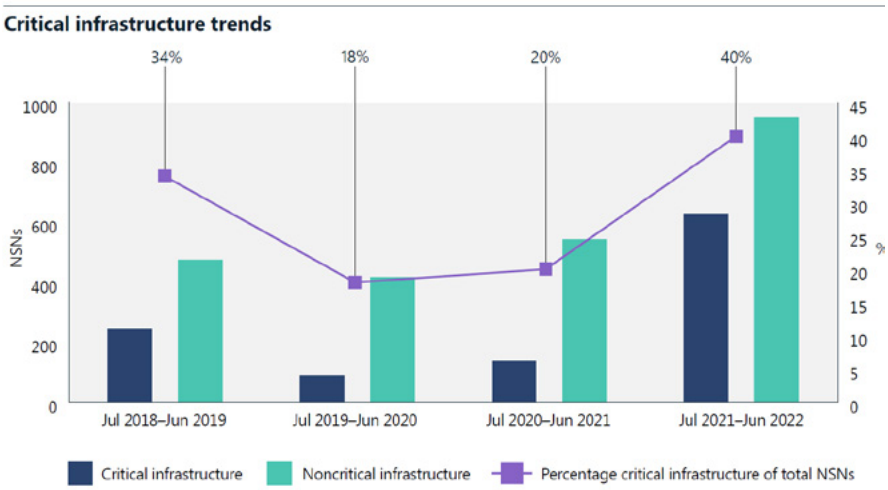


Figura 3 - *Trend degli attacchi alle Infrastrutture Critiche*

Facciamo, allora, un approfondimento di due dei Paesi più attivi sul fronte cyber: Russia e Cina.

Russia

Non si può parlare degli state actor russi senza fare riferimento al conflitto in essere dallo scorso febbraio. Non bisogna, altresì, dimenticarsi che questi criminali informatici sono gli stessi che hanno attaccato aziende private sparse in tutto il mondo.
È chiaro che la parte del leone la fa il supporto che hanno dato alla guerra convenzionale in Ucraina utilizzando, però, le stesse tecniche e le medesime tattiche che li hanno resi famosi. Se è vero che negli occhi di tutti rimane impressa l'attività rivolta a danneggiare le infrastrutture critiche dell'Ucraina (IRIDIUM ha distribuito il malware Industroyer2 per cercare di colpire le centrali energetiche dell'Ucraina) è altrettanto vero che, al di fuori dell'Ucraina, BROMINE ha condotto operazioni contro organizzazioni dell'ambito manufatturiero e del controllo industriale.
Gruppi affiliati alla Russia come ACTINIUM, NOBELIUM, STRONTIUM, DEV-0257, SEABORGIUM e, appunto, IRIDIUM hanno utilizzato campagne di phishing per compromettere account con i quali ottenere l'accesso alle reti delle varie organizzazioni presenti in diversi Paesi come potete osservare nella seguente immagine:

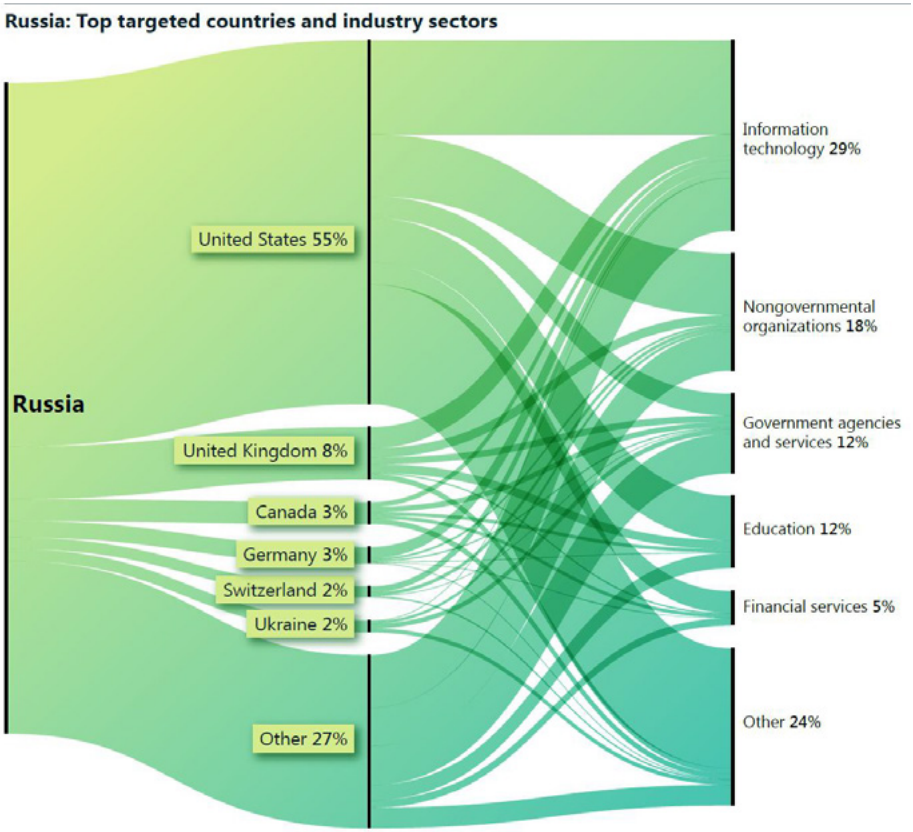


Figura 4 - *Top Target degli State Actor Russi*

NOBELIUM ha utilizzato account compromessi di diplomatici per inviare e-mail di phishing, mascherate da comunicazioni diplomatiche, a ministri appartenenti a Paesi di tutto il mondo.
STRONTIUM ha creato falsi account basandosi su quelli disponibili pubblicamente e titolari di conti correnti negli Stati Uniti per inviare messaggi di phishing così da ottenere l'accesso a questi conti. SEABORGIUM ha sviluppato campagne di phishing utilizzando esche relative a reportage sul conflitto ucraino per ottenere accesso a conti relativi ad affaristi internazionali che si occupavano della vendita di carri.
In tutto il mondo, ma soprattutto negli Stati Uniti e nell'Europa occidentale, NOBELIUM ha preso di mira i fornitori di servizi IT per ottenere l'accesso alle reti governative sfruttando la debolezza delle supply chain.

Cina

Nel complesso clima geopolitico di oggi, lo Stato cinese e i gruppi di criminali informatici ad esso affiliati hanno condotto operazioni mirate a rafforzare la propria posizione sempre più dominante sia in ambito militare che economico. Nell'ultimo anno, si è osservato una diffusa minaccia cinese rivolta ai paesi di tutto il mondo come evidenziato nella seguente immagine:

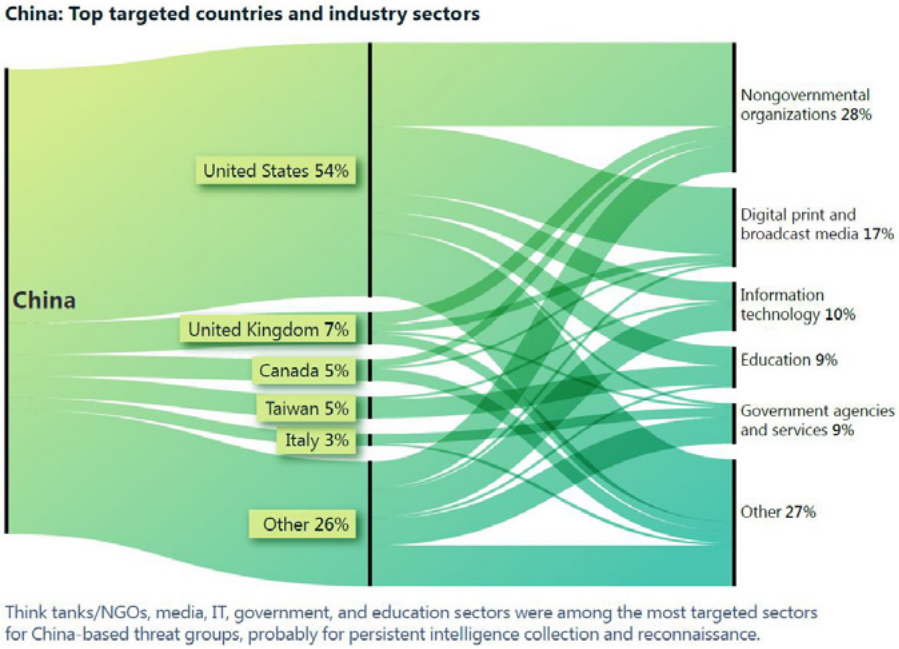


Figura 5 - *Top Target degli State Actor Cinesi*

Dalla metà del 2021, la Cina ha operato per garantirsi la stabilità economica e finanziaria dopo l'ondata di COVID-19 che l'aveva pesantemente colpita negli ultimi due anni. La Cina ha continuato a destreggiarsi per trovare un equilibrio nello scenario internazionale che da un lato bilanciasse il partenariato "illimitato" con la Russia e dall'altro gli permettesse di mantenere la propria posizione "dominante" sulla scena mondiale. Inoltre, la posizione della Cina contro gli Stati Uniti e i suoi alleati in merito alla vicenda riguardante Taiwan ha continuato a mettere a dura prova le relazioni estere con molti paesi.

La Cina ha, altresì, continuato ad espandere la propria influenza economica a livello globale attraverso accordi stabiliti precedentemente quali "Belt and Road Initiatives" (BRI), tentando di rilanciare un nuovo framework per gli investimenti con l'UE e di negoziare un nuovo accordo commerciale con i paesi della zona asiatica del Pacifico, noto come Regional Comprehensive Economic Partnership.

Tutto ciò è avvenuto e continuerà ad avvenire utilizzando le armi della Threat Intelligence e dello spionaggio cyber in modo da acquisire informazioni che consentano di supportare la strategia politica, economica e militare del Paese.
La particolarità della Cina sta negli obiettivi che, a differenza di altri Paesi, sono rappresentati da nazioni più piccole, cosa che evidenzia come la Cina stia, probabilmente, usando lo spionaggio informatico come componente della propria economia globale e influenza militare.
La portata degli obiettivi ha incluso paesi in Africa, nei Caraibi, in Medio Oriente, in Oceania e in Asia meridionale con una particolare attenzione ai paesi del sud-est asiatico e alle isole del Pacifico.
In linea con la strategia BRI della Cina, gli state actor hanno preso di mira entità in Afghanistan, Kazakistan, Mauritius, Namibia e Trinidad e Tobago. Ad esempio, Trinidad e Tobago è stato il primo paese caraibico ad appoggiare la strategia BRI nel 2018 e la Cina lo considera un Partner molto importante.
Tra i gruppi principali che hanno operato lo scorso anno troviamo: NICKEL e RADIUM.
Nel gennaio 2022, RADIUM si è reso protagonista di una serie di attacchi ad aziende associate ai governi di Vietnam ed Indonesia. Queste azioni sono state effettuate in assoluta sintonia con gli obiettivi strategici di espansione della Cina nel mare del Sud della Cina.
Tra la fine di febbraio e l'inizio di marzo, GALLIUM ha compromesso oltre 100 accounts di una organizzazione intergovernativa nella regione del Sudest asiatico. Il timing non fu casuale perché in quel periodo era previsto un congresso tra esponenti del governo degli Stati Uniti e i leader degli Stati di quella regione. L'obiettivo era quello di fare attività di intelligence.
L'espansione della Cina nelle Isole del Pacifico è stata accompagnata dalle attività cyber di questi gruppi.

In aprile, la Cina e le isole Solomon hanno siglato un accordo al fine di, si legge, *"promote peace and security"*. L'accordo permette, potenzialmente, alla Cina di vendere armi in quei Paesi. **In questo mondo, purtroppo, una delle contraddizioni più evidenti è che per ottenere la pace, bisogna usare le armi!**
Un mese dopo, i sistemi governativi delle Isole Solomon vengono colpiti da un malware noto come GADOLIUM e contemporaneamente, RADIUM fa girare codice malevolo sui sistemi delle compagnie di telecomunicazioni della Nuova Guinea. Entrambe le attività sono da annoverarsi tra quelle di intelligence per ottenere informazioni a supporto della strategia politica cinese.

Anche NICKEL ha preso di mira parecchie agenzie governative compromettendone cinque tra la fine di marzo e l'inizio di maggio 2022; agenzie che erano già state compromesse in passato. Questo fatto ha dimostrato la capacità di persistenza di questi attori, garantita da ulteriori entry points in queste entità e da canali di command & control che non erano stati, evidentemente, rimossi dagli attacchi precedenti.

In sintesi, in uno scenario di enorme tensione politica come quello che stiamo vivendo, va ricordato che questi attori usano le stesse tecniche e tattiche utilizzate per colpire le singole organizzazioni industriali il che fa capire come, ancora una volta, sia fondamentale per le organizzazioni avere una chiara strategia di difesa e per i governi la necessità di investire nella cyber e nel digitale.
Non ci si può permettere di non aggiornare i sistemi, di non avere soluzioni anti-phishing, di non formare le persone e di mantenere applicazioni che creano lock-in a livello di sistema operativo. Chi lo fa sa che, prima o poi, ne subirà le conseguenze, purtroppo.
Per uno "state actor" non fa differenza che la vittima sia uno Stato, un'infrastruttura critica o una pubblica organizzazione. Il movente è sempre lo stesso e si chiama denaro oppure potere politico.

Bibliografia

Digital Defense Report

Profili Cyber ultra-specializzati e nuovi trend del mercato del lavoro

(Ultra-specializzazioni, RAL crescenti e strategie di attraction e retention delle aziende)

[A cura di Yuri Riccardo Perseu, Experis]

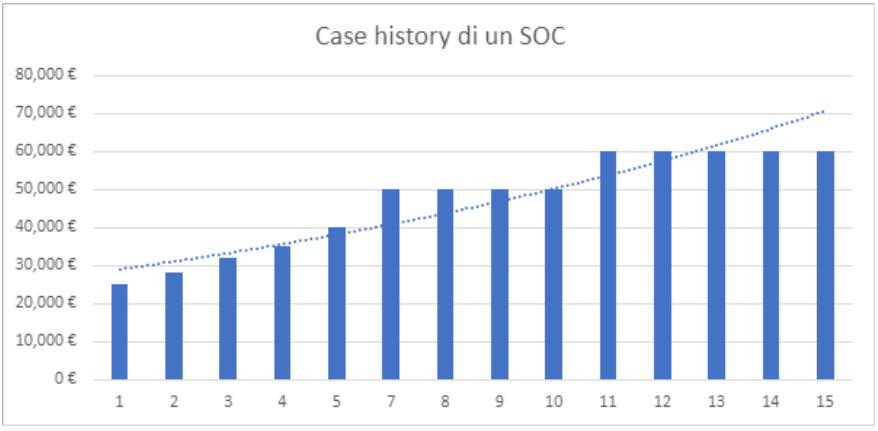
Negli ultimi anni abbiamo visto susseguirsi diversi *trend* di mercato in ambito *innovation*, dalla "febbre degli sviluppatori" alla vorace ricerca di esperti del mondo Data.
Il settore informatico ha, tuttora, una forte necessità di queste figure: non ci sono infatti, oggettivamente, aree tecnologiche sature, dove la richiesta del mercato è adeguatamente coperta dal corretto numero di professionisti.
Secondo l'indagine MEOS – ManpowerGroup Employment Outlook Survey – per l'ultimo trimestre del 2022, i datori di lavoro italiani prevedono assunzioni in crescita registrando una previsione netta di occupazione (NEO) del +13%, al netto degli aggiustamenti stagionali. Uno dei mercati del lavoro più favorevoli è proprio il settore IT, Tech, Telecomunicazioni e Media, dove le prospettive occupazionali nette sono salgono al +14%.
I ruoli digitali continuano a guidare la maggior parte della domanda a livello globale, con il maggior bisogno di talenti con competenze tecnologiche. A livello globale il settore IT registra in assoluto la maggiore prospettiva di assunzioni. Le organizzazioni del settore IT riportano le prospettive più ottimistiche (+42%).
Con il PNRR, i processi di digitalizzazione sono diventati *task* fondamentali - e trasversali a tutte le *Industry* - per la ripresa economica e l'adeguamento degli standard ai livelli internazionali. Uno dei principali *trend* emergenti che osserviamo è rappresentato dalle aziende del mondo industriale concentrate sempre di più sulle tematiche informatiche che prima, invece, non riscontravano la stessa risonanza.
L'esigenza di innovare, adeguare le soluzioni di *Cyber Security* e raggiungere la sovranità digitale, sotto la spinta del PNRR, porta le aziende a investire sulle persone, puntando sulla valorizzazione delle competenze e sulle collaborazioni con Enti nazionali e internazionali, Università e Centri di Ricerca Scientifica.
Secondo i dati di Experis Italia, brand di ManpowerGroup e *provider* IT di soluzioni applicative, consulenza, resourcing e formazione, ad oggi la domanda di professionisti *Cyber* sta esplodendo rispetto figure con hard skills in ambito informatico e *security* per la parte *Operation*, ovvero profili con competenze nel campo riconosciuto universalmente con la sigla OT. Oltre ai profili classici appartenenti al mondo *Cyber, quindi*, sono ricercati professionisti specializzati e con esperienza all'interno di aziende del comparto produttivo. Di recente, infatti, un settore molto attivo nella ricerca di figure professionali esperte nella sicurezza informativa è quello dell'*Automotive*. Sul mercato i *job title* di tendenza sono il *Cyber Security Engineer*, l'*OT Security Expert* e il *Security Governance Specialist*.
Osserviamo sempre più aziende occupate nella ricerca di figure professionali specializzate nella gestione di infrastrutture complesse, come quelle dei *plant* produttivi o delle macchine di produzione, o con competenze in ambito *governance* per la gestione dei *framework* e dei requisiti relativi alle ISO di riferimento. Si tratta di profili molto rari, in quanto specia-

lizzati in una determinata *Industry* che diventa poi il perimetro della loro carriera, creando così delle vere e proprie "nicchie di competenze". Un professionista che ha costruito le sue competenze sulle normative di riferimento del settore *Automotive,* ad esempio, dopo aver consolidato il suo percorso in questo comparto, probabilmente non andrà a lavorare in *un'Industry* diversa, ad esempio nella GDO.
In sintesi, un bacino di profili ICT ultra-specializzati particolarmente ristretto comporta una spendibilità delle competenze limitata e una contrazione molto forte, che ostacola i piani di crescita delle aziende di tutto il Paese.

La crescita esponenziale della RAL dei profili Cyber: case history di un SOC

Secondo quanto rilevato da ManpowerGroup, oggi il 72% delle aziende italiane riscontra difficoltà nel trovare i talenti adeguati alle proprie esigenze. Le competenze più difficili da trovare secondo i datori italiani sono IT e Data (27%). I profili legati al mondo digital più difficili da trovare sono: ingegneri robotici, specialisti fintech, di digital marketing e strategia, professioni sanitarie, risorse umane, esperti di *Cyber Security*, *Process Automation*, *Digital Transformation* e sviluppatori di App.
Per questi professionisti del mondo tecnologico, il tema dei livelli retributivi è diventato un elemento di notevole rilevanza, per affrontare sfide importanti di carriera o per dedicarsi allo sviluppo di alcune particolari competenze. Questo argomento è di estrema importanza anche per chi si occupa di sviluppo aziendale e strategie di *retention* dei talenti.
Oggi il settore *Tech* è condizionato da un *trend* indubbiamente complesso da calmierare e razionalizzare, quello della curva crescente delle retribuzioni di tutti i professionisti appartenenti al mondo IT e, in particolar modo, di coloro che si sono specializzati nell'ambito della *Cyber Security*.
Come evidenziato anche dal *Report* di Experis **Tech Cities** (prima edizione, 2022), un laureato in Informatica e specializzato in *Cyber Security*, anche senza alcuna esperienza professionale alle spalle (profilo *junior*), riceve offerte di lavoro che superano abbondantemente la soglia dei 25.000 € come prima retribuzione. Per i profili che, invece, non hanno completato un percorso di studi universitari, ma hanno iniziato subito a lavorare nel settore IT come Help Desk, Sistemisti o Specialisti di Rete junior, e si sono specializzati successivamente in ambito Security, questa soglia viene raggiunta entro un anno dall'assunzione.
Secondo gli *insight* di Experis, il dato più evidente, e che sicuramente incuriosisce di più, è che dal primo giorno lavorativo fino al sesto anno di lavoro la RAL (retribuzione annua lorda) tenderà a salire in maniera vertiginosa, superando facilmente i 50.000 €, per poi frenare la crescita nei successivi 6 anni, raggiungendo una RAL media di 65.000 – 70.000 €.
Di seguito un esempio pratico che prende in considerazione un contesto tecnologico di riferimento come quello del *Security Operation Center* (SOC) e una delle sue figure più ricercate sul mercato, quella dell'analista.
Ipotizziamo che un profilo *junior*, che ha completato un percorso di laurea o un corso di specializzazione, con competenze tecniche minimamente sviluppate, una conoscenza base

della lingua inglese e *soft skills* già sviluppate, inizi a lavorare in un'azienda di consulenza di medie dimensioni come SOC Analyst di primo livello, con una RAL intorno ai 25.000 €. Dopo un paio di anni, grazie all'esperienza maturata sul campo e dopo il conseguimento di certificazioni in ambito *security*, siano essa relative a un prodotto o a un determinato *framework,* riceverà dalla sua azienda un *increase* che valorizza le sue competenze, raggiungendo una RAL anche di 28.000 €. Oggi, un profilo come quello appena descritto si colloca tra i "*most wanted*" dei *Recruiter IT*, pronti a concretizzare il proprio interesse con un'offerta di lavoro che prevede un contesto migliore, progetti più interessanti e maggiori opportunità di crescita. Il nostro SOC Analyst - ora diventato un profilo *middle* - riceverà in poco tempo una proposta economica che comprende un aumento del 15% e dei bonus, conquistando così, dopo appena tre anni di lavoro, una RAL di 32.000 €. Cambiare azienda significa, anche per un SOC Analyst, partecipare a corsi di formazione, prendere nuove certificazioni, dedicarsi a *task* e attività con maggiori responsabilità, ampliando il perimetro di lavoro e le proprie competenze e uscendo dalla *routine* tipica dei professionisti *junior*. Nel caso del SOC, si può ipotizzare la fine del lavoro di monitoraggio su turnazione in favore della gestione degli *incident*. Raggiunta la qualifica di *Incident Responder,* dopo un paio di anni, il mercato del lavoro avanzerà certamente una nuova offerta. Il nostro profilo *middle*, che grazie alle competenze sviluppate, adesso ha una RAL variabile tra 32.000 e i 35.000 €, può ambire a un'offerta economica di 40.000 – 42.000 €. Come si evince anche dal grafico, dopo circa 5 anni di esperienza, un esperto di sicurezza informatica può raggiungere tranquillamente una retribuzione di 42.000 €.



Se avessimo voluto rendere l'esempio ancor più reale avremmo dovuto illustrare uno schema composto non solo da offerte, ma anche da controfferte. Si conta, infatti, che un candidato svolga almeno un iter di selezione all'anno e che possa ricevere almeno una controf-

ferta ogni anno e mezzo. In questo scenario, il nostro SOC Analyst avrebbe raggiunto anche prima la RAL di 42.000 €.
Continuando il nostro esempio senza *boost* di carriera particolari, un professionista in ambito *Cyber Security*, dopo 5 anni, ha mediamente una retribuzione prossima al livello manageriale, è già responsabile di un team ed ha un ruolo centrale all'interno delle logiche aziendali. Al settimo anno di lavoro, potenzialmente, potrebbe ricoprire un ruolo di Team Leader con una RAL media che si attesta sui 50.000€. Dopo 10 anni d'esperienza, il nostro esperto di sicurezza è pronto a farsi carico della responsabilità dell'intera struttura e quindi prendere il comando del SOC, arrivando a guadagnare una somma che va dai 60.000 ai 70.000€. Attraverso questo esempio, volutamente semplificato, possiamo chiaramente vedere come nell'arco di 7 anni la RAL di un esperto *Cyber* raddoppi repentinamente, ma superati questi primi anni fatichi a crescere, salvo non arrivare a ricoprire ruoli Dirigenziali.
Nello schema appena descritto, gioca un ruolo fondamentale il numero di professionisti con competenze tecniche spendibili in un mercato in forte crescita, che in ambito *Cyber Security* è molto basso. Questo gioco frenetico di offerte e controfferte, agevolato dall'atteggiamento dinamico dei *Millennials* – tipicamente propensi al cambiamento, non solo per ragioni economiche ma anche per motivi di crescita professionale - è sicuramente più evidente che nelle generazioni precedenti.

Turnover aziendale: strategie per attraction e retention dei talenti dell'innovazione

La scarsità di talenti in ambito *Cyber* da un lato e l'interesse di interi comparti verso le medesime aree tecniche dall'altro, ha generato una fortissima competizione tra le aziende, da cui ne deriva sia la perdita - rapida e ciclica - di personale, che l'impiego di molto tempo e notevoli sforzi per riacquisirlo.
L'attenzione da parte delle aziende alla *talent acquisition* e *retention* sono trend che stanno caratterizzando trasversalmente tutti i settori, anche se la tematica è particolarmente sentita nel mondo STEM, quindi anche nel settore della *Cyber Security,* dove a causa della trasformazione digitale lo *skills gap* è particolarmente evidente e difficile da colmare.
Nel comparto della *Cyber Security* si registra un turnover molto elevato all'interno delle aziende medio-piccole, dove i candidati sono soliti iniziare l'esperienza professionale a fronte di una formazione specializzante. Poi entrano in gioco le big company che, con uno sforzo economico relativamente piccolo, riescono a ingaggiare candidati già formati ed inserirli *"plug and play"* su progetti tecnici, evitando tempi di formazione troppo lunghi.
Tendenzialmente, le imprese medio-piccole non hanno la forza economica per rispondere alle offerte dei *competitor* o per garantire una crescita professionale al pari di un contesto internazionale, comportando flussi di uscite ciclici di talenti. Ciononostante, anche le aziende più grandi hanno difficoltà nel trattenere i talenti, sia per i diversi *driver* delle nuove generazioni, sia per i *trend* di mercato prima citati.
Secondo Experis, le soluzioni per la *talent attraction* e *retention* in ambito ICT possono essere diverse: in fase di attrazione del talento, una leva ad alto valore aggiunto è ad esempio

la formazione professionale *on the job* "blindata", che garantisce la permanenza in azienda per un periodo prestabilito e piani di crescita strutturati, anticipando le offerte del mercato da parte di aziende *competitor*. Durante la carriera, anche al fine di trattenere i talenti, risultano vincenti i percorsi di *upskilling* verticali come quelli offerti da Experis Academy, il Training Provider di Experis specializzato nella formazione tecnica sul segmento IT & Technology.

Altre soluzioni, puramente HR, riguardano lo sviluppo della filosofia e del contesto aziendale, che prevedono, ad esempio, investimenti nella costruzione di un ambiente di lavoro positivo, che aiuti il professionista a sviluppare un senso di appartenenza e fedeltà verso l'azienda e il suo *team*. La creazione di un'identità collettiva è sicuramente una modalità di *retention* vincente per l'azienda. Durante le fasi di un processo di selezione, infatti, si fa sempre molta attenzione alla capacità di lavorare in squadra e all'atteggiamento positivo di una persona all'interno di un contesto lavorativo, anche se spesso se ne perde traccia a discapito del ruolo operativo del singolo. Senza dubbio si tratta di una soluzione complessa, che comporta azioni quotidiane da far perdurare nel tempo e la condivisione della *mission* a tutti i livelli aziendali, ma sicuramente è la soluzione meno impattante a livello di *budget* e la più sostenibile nel lungo periodo, giovando fortemente sulla *reputation* aziendale.

Un'ultima pratica, non condivisibile ma che sta trovando riscontro nel mercato del lavoro ICT, è quella della *retention* attraverso penali economiche. Garantirsi la permanenza di una risorsa con la forza non è mai positiva e, soprattutto, non garantisce che una *big company* non si aggiudichi il candidato poiché i limiti non vessatori sono sempre inferiori alla capacità economica che determinate realtà aziendali possono utilizzare per le assunzioni. Inoltre, mette in cattiva luce le aziende sia nel breve che nel lungo periodo.

Pertanto, è sempre bene analizzare il settore di riferimento, valutare i *competitor* e i loro approcci per costruire una politica aziendale che permetta alle persone di inserirsi in una *comfort zone* reale e di adottare un *mindset* che le aiuti a guardare al loro percorso in azienda a lungo termine.

Conoscere il mercato è sicuramente il punto di partenza per la gestione di *trend* e criticità di un settore complicato ma entusiasmante come quello dell'Informatica, e ancor di più della *Cyber Security*.

Operation Technology Security – Ultima chiamata

(A cura di Aldo Di Mattia, Fortinet)

Non si può più attendere. Non si può più rimandare. La sicurezza OT deve essere al centro dei piani strategici di ogni nazione. Teoricamente in Italia è tra le priorità, ma questo non è più il momento della teoria, siamo già in ritardo di anni, ora dobbiamo agire e dobbiamo farlo adesso. Se in ambito IT il divario che divide i cybercriminali e i nuclei di cybersecurity delle varie aziende è spesso troppo ampio, a favore degli attaccanti ovviamente, in ambito OT è disarmante.

L'Italia, come Stato membro EU, ha il compito di adottare la direttiva sulla sicurezza delle reti e dell'informazione (NIS), il primo atto legislativo a livello europeo sulla cybersecurity, con l'obiettivo di raggiungere un elevato livello comune di sicurezza informatica per le infrastrutture critiche. La direttiva ha un obiettivo condivisibile e imprescindibile, ma la sua attuazione si è rivelata complessa e frammentata. Per affrontare in modo più strutturato il problema, la Commissione Europea ha presentato una proposta per sostituire la direttiva NIS, rafforzando ulteriormente i requisiti di sicurezza. Novità fondamentale è quella di introdurre misure di vigilanza più rigorose e requisiti di applicazione più stringenti, tra cui sanzioni armonizzate in tutta l'UE. Inoltre, c'è la proposta di ampliare l'ambito di applicazione della NIS2, obbligando di fatto un maggior numero di entità e settori industriali ad adottare le misure, così da aumentare ancora di più il livello di sicurezza informatica nell'Unione Europea. All'interno del Parlamento europeo, si è raggiunto un accordo provvisorio sul testo il 13 maggio 2022, ma prima di essere adottato formalmente dovrà passare al vaglio del voto nei prossimi mesi. Un altro regolamento EU in fase di bozza, che sta introducendo innumerevoli cambiamenti per il tema della cyber security OT, è la direttiva macchine che permette ai produttori di macchinari di automazione di ricevere il marchio CE. Proprio in questo mercato, dove l'Italia risulta essere tra i leader Europei, ci sarà il bisogno da parte

degli OEM (Original Equipment Manufacturer) e degli utilizzatori finali di attuare soluzioni di tracciamento delle connessioni da remoto e gestire in modo adeguato i dati "IN/OUT" dei macchinari, per assicurare il corretto funzionamento in termini di sicurezza informatica e operativa.
Siamo in ritardo però, come già anticipato da Fortinet più di un anno fa, nello studio condotto **dalla global intelligence dei FortiGuard Labs di Fortinet,** i cybercriminali utilizzano sempre più ransomware in ambito OT per paralizzare le infrastrutture critiche nazionali, al fine di chiederne poi un riscatto (probabilmente questo è il caso migliore), oppure creare caos e instabilità (caso forse peggiore e sempre più attuale in uno scenario geopolitico estremamente complesso). Attualmente le infrastrutture OT italiane non hanno soluzioni di sicurezza state-of-art attive, beneficiano al più di Next Generation Firewall nel punto di contatto tra IT e OT e, molto più raramente, utilizzano sonde basate su intelligenza artificiale per il monitoraggio dei flussi OT.
Per raggiungere una architettura di sicurezza state-of-art bisognerebbe avere anche Next Generation Firewall all'interno dei flussi L3 e L2 (della pila ISO OSI) delle infrastrutture OT con signature specifiche, switch capaci di isolare apparati all'interno della stessa vlan (senza cambiare gli indirizzi IP ovviamente), sistemi OT esca gestiti da soluzioni di deception, sistemi di sandboxing capaci di verificare la presenza di minacce sconosciute in ambito OT, oltre che SIEM, SOAR e altro ancora (maggiori dettagli nel prossimo paragrafo).

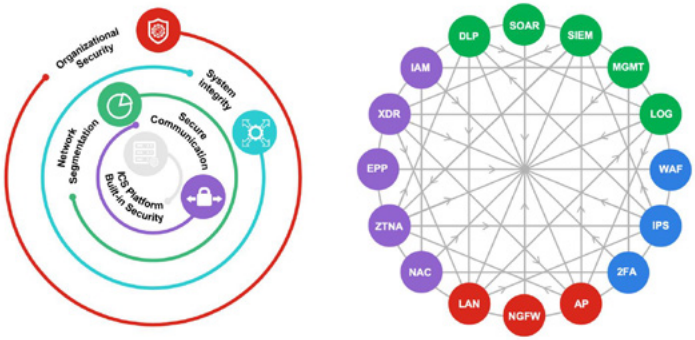
Il divario tra le attuali architetture OT italiane e quelle state-of-art è abissale ma per questa disparità non vanno colpevolizzate le strutture di progettazione delle varie organizzazioni pubbliche e private, così come non bisogna puntare il dito su eventuali carenze di budget e investimenti (vedi piano PNRR).

Questo scenario nefasto è generato da diversi fattori:

- I sistemi OT hanno avuto una notevole evoluzione negli ultimi anni: siamo passati da uno scenario con impianti air-gapped (cioè non connessi) e tecnologie proprietarie a uno scenario dove i produttori utilizzano tecnologie off-the-shelf (sistemi operativi commerciali e protocolli TCP/IP) e reti connesse al mondo IT per traguardare la digitalizzazione degli impianti (vedi Industry 4.0).
- Le applicazioni, i protocolli e i Firmware dei device OT non sono stati concepiti per offrire sicurezza e integrità dei dati, ma solo velocità e resilienza, tralasciando quindi sistemi di autenticazione e cifratura del traffico comunemente usati nel modo IT.
- L'evoluzione descritta, ai punti precedenti, è stata più veloce della diffusione della consapevolezza dei possibili rischi legati alle minacce cyber.
- I sistemi OT vengono acquistati dalle aziende in rack o contenitori chiusi e certificati dal produttore/integratore stesso di sistemi OT. Nessun cliente può decidere autonomamente di aggiungere elementi di sicurezza all'interno di queste black box senza invalidare le garanzie offerte dal produttore/integratore.

Come si esce da questa impasse? I clienti e lo stato dovrebbero pretendere dei rack/contenitori certificati e già provvisti al proprio interno dei sistemi di sicurezza citati e i nuovi bandi dovrebbero rendere queste architetture obbligatorie, pena esclusione. Dall'altra parte, i vendor OT rispondono alle esigenze del cliente, la sicurezza OT ha un onere non trascurabile e questi costi extra possono essere inseriti solo se il cliente include le soluzioni di cybersecurity tra i requisiti obbligatori.

Uno strumento a supporto degli operatori degli impianti OT è lo standard IEC62443 "Security of Industrial Automation and Control Systems", che descrive un approccio metodologico per l'implementazione della cybersecurity nel mondo dei sistemi di controllo e automazione industriale. I benefici di un approccio su base standard IEC62443, comprendono la riduzione delle probabilità di un cyber attacco mediante l'utilizzo di un insieme di requisiti comuni tra tutti gli stakeholders di un impianto OT (clienti, fornitori, manutentori, etc.).



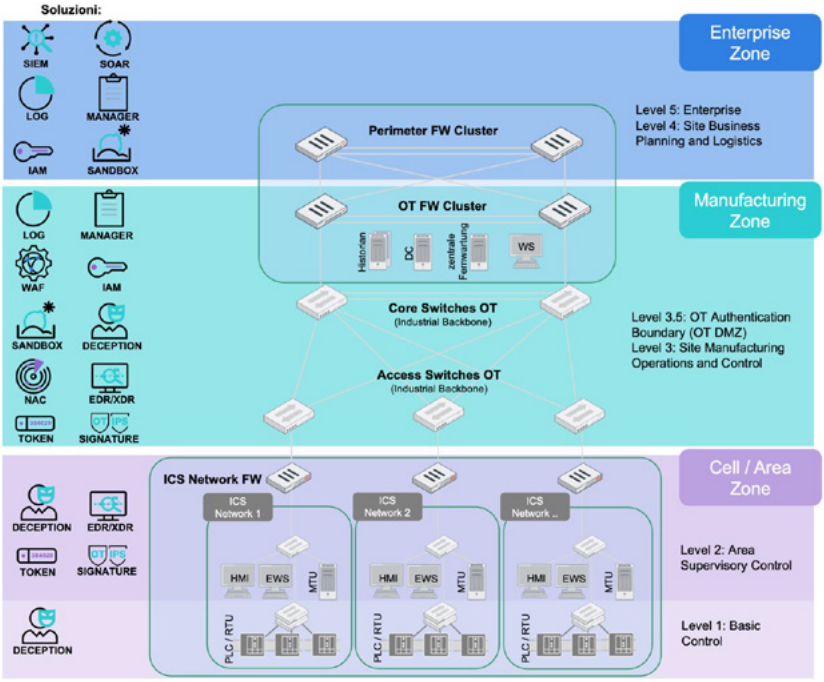
Defense in depth (IEC 62443) con un esempio di Security Mesh Architecture (Security Fabric)

Mediante un risk assessment, il gestore dell'impianto va a definire un target security level (SL-T) per ogni parte dell'impianto OT, con l'obbiettivo di andare ad annullare o mitigare i rischi identificati.
Una volta definiti i fattori di rischio e di sicurezza mediante un risk assesment, è necessario sviluppare contromisure per portare il security level (SL-T) a un livello di rischio che l'azienda sia disposta ad accettare. Questo comprende diverse fasi e tecniche, come l'approccio "Defense in Depth" e la creazione di zone e per fornire diversi livelli di protezione. Il "Defense in Depth" è un concetto militare che fornisce diversi livelli o strati di protezione contro un potenziale attaccante o intruso che cerca di violare il SL-T. Sebbene sia strettamente legata alla tecnologia, la difesa in profondità considera parte integrante della sua implementazione anche altri fattori, come le persone e i processi. Il risk assesment può essere suddiviso in più fasi (tipicamente high level e low level) mediante la scomposizione dell'impianto con il modello "zone and conduit", in modo tale da definire rischi specifici (e di conseguenza requisiti specifici) per ogni parte dell'impianto. Ovviamente si andrà a definire livelli di sicurezza più alti dove i rischi saranno più alti e livelli di sicurezza più bassi ove i rischi saranno ridotti. Lo standard definisce quattro security level (SL) e per ognuno una lista di requisiti tecnici specifici che un progetto OT deve rispettare. La definizione dei requisiti è molto dettagliata, si tenga conto che un impianto SL4 (Security Level 4, il massimo livello definito) deve soddisfare più di cento requisiti tecnici.
Ecco che allora il gestore di un sistema OT, una volta definito un SL-T, può richiedere ai propri fornitori quale sia la capacità in termini di requisiti soddisfatti secondo lo standard IEC62443 dei prodotti e delle soluzioni proposte. Il SL richiesto potrà essere definito in base ai livelli di rischio calcolati dal gestore, che saranno opportunamente indirizzati per ogni sezione dell'impianto. Questo approccio basato su IEC62443 permette di raggiungere in modo efficiente alti livelli di sicurezza, con un approccio metodologico riconosciuto da tutti i vendor del mercato.

Infrastruttura di sicurezza OT State-of-Art

Sono sempre più frequenti le minacce che hanno come obbiettivo la compromissione di sistemi OT critici. Nei 10 anni trascorsi, da quando l'attacco Stuxnet ha interrotto il programma nucleare iraniano, abbiamo assistito ad un aumento della sofisticazione e della quantità di attacchi informatici alle infrastrutture OT. L'OT è particolarmente vulnerabile, poiché le minacce che in passato richiedevano una presenza fisica attraverso il trasferimento di file via connettori locali USB (o simili) ora sfruttano la potenza dell'interconnessione con le reti IT.
Per implementare un'infrastruttura di sicurezza OT adeguata occorre fare lo stesso cambiamento compiuto negli ultimi anni nella sicurezza IT, cioè passare da prodotti specifici isolati a un approccio di tipo Security Mesh. Bisogna pertanto creare un'unica soluzione di sicurezza OT, che sfrutti l'integrazione nativa di molteplici prodotti di sicurezza mediante interfacce API (Application Programming Interface), con una gestione integrata dell'intera infrastruttura in un unico punto (single-pane-of-glass). Queste soluzioni possono essere

calate nel tradizionale modello Purdue che resta il riferimento architetturale per eccellenza dei sistemi OT.



Purdue model

Un'architettura state-of-art deve comprendere almeno le seguenti componenti:

- Accesso: Next Generation Firewall (NGFW), secure switch, access point (AP) Wi-fi. Tutti questi dispositivi devono essere disponibili in versione "rugged", cioè ingegnerizzati per l'installazione in ambienti industriali complessi ed estremi in termini di temperatura, umidità, vibrazioni, elettromagnetismo e altro ancora. Questi sistemi possono essere utilizzati per costruire le reti di supervisione e controllo (livello 2), le reti di stabilimento (livello 3), le reti DMZ locali (livello 3.5) fino all'interconnessione con le reti IT (livello 4).
- Reti Wi-Fi sicure: le reti Wi-Fi entrano sempre più negli impianti OT, sia per la connessione di oggetti IIoT (Industrial Internet of Things) che per la digitalizzazione dei processi di gestione e manutenzione degli impianti. Queste devono essere configurate implementando le best practices riguardo l'hardening delle reti: autenticazione WPA3-enterprise, Wireless Intrusion Detection tra cui la gestione dei Rogue AP, policy di esclusione degli utenti malevoli e molto altro ancora. L'interconnessione delle reti Wireless con il resto dell'impianto deve essere realizzata mediante NGFW a livello 3.

- Analisi del traffico: effettuare una deep-inspection dei flussi di traffico di automazione o SCADA per poter identificare manomissioni o tentativi di intrusione e un'analisi comportamentale del traffico in grado di identificare eventuali anomalie dei flussi applicativi OT.
- Autenticazione: NAC (network access control), autenticazione a più fattori (MFA), Single Sign-on, VPN e Zero Trust Network Access (ZTNA). I sistemi di autenticazione possono operare su tutti gli apparati dell'impianto, queste soluzioni prevedono normalmente una gestione centralizzata a livello 3.
- Protezione avanzata: End Point Detection and Response (EDR), soluzioni di Deception OT e soluzioni di Sandboxing OT. Anche questi sistemi possono operare su tutti i livelli dell'impianto e prevedono una gestione centralizzata a livello 3.
- Gestione: SIEM e SOAR. Questi sistemi monitorano e raccolgono i log di tutti gli apparati dell'impianto (tutti i livelli) e hanno una consolle centralizzata che può essere installata a livello 3 o livello 4 per una gestione entreprise.

Le soluzioni indicate sono indispensabili per raggiungere i seguenti obiettivi:
- Segregazione delle reti, per il traffico in direzione nord/sud mediante il controllo del traffico con NGFW, switch e AP per implementare il concetto di "zone and layer segmentation".
- Abilitazione delle funzionalità di Application Control per riconoscere il traffico industriale e bloccare i flussi non autorizzati e applicazione di Virtual Patching per proteggere sistemi difficilmente aggiornabili, da attacchi già riconosciuti e classificati.
- Analisi comportamentale dei flussi applicativi mediante l'utilizzo di sonde che hanno il compito di studiare il traffico delle reti OT e tracciare delle "baseline", così da identificare asset collegati in rete e rispettivi flussi applicativi, al fine di individuare eventuali difformità dalle "baseline" apprese.
- Micro segmentazione delle reti, per il traffico in direzione est/ovest all'interno delle stesse reti e mediante NGFW a layer 2 (ISO/OSI).
- Controllo degli accessi, mediante NAC per l'identificazione degli oggetti connessi in rete e la conseguente profilazione.
- Autenticazione degli utenti tramite protocolli standard cifrati e abilitazione di multi-factor authentication.
- Protezione degli host da minacce di tipo zero-day (compresi spyware e ransomware).
- Individuazione di minacce interne e lateral movement.
- Gestione dei log, degli incidenti e automazione delle risposte alle minacce.

Come già precisato, tutto questo si può ottenere solo se i distinti prodotti (NGFW, NAC, Sonde OT, EDR/XDR, Deception, Sandbox, SIEM, SOAR, ecc.) sono integrati nativamente tra loro e compongono un'unica soluzione, un'architettura basata su automatismi e cooperazione è infatti indispensabile, altrimenti la complessità prende il posto di ogni beneficio.

Dati FortiGuard Labs OT

Nel corso della prima metà del 2022 i FortiGuards Labs di Fortinet hanno individuato diversi attacchi SCADA diretti a infrastrutture critiche italiane e mondiali. Purtroppo, questo dato è inferiore rispetto al numero dei reali attacchi prodotti dai cyber criminali, il ritardo generale descritto precedentemente nell'attuazione di contromisure idonee, impedisce di individuare e dunque conteggiare, tutti gli attacchi sferrati. A livello mondiale Fortinet ha riscontrato i seguenti attacchi.

Indicatros of Comprmise (IoC)	Count
CirCarLife.Scada.HTTP.Credential.Information.Disclosure	255950
LAquis.SCADA.Web.Server.Directory.Traversal	121674
mySCADA.myDESIGNER.Import.ZIP.Directory.Traversal	39832
Schneider.Electric.ClearSCADA.Remote.Authentication.Bypass	5640
KingScada.KxClientDownload.ActiveX.Remote.Code.Execution	2304
Schneider.Electric.Interactive.Graphical.SCADA.Buffer.Overflow	1728
LAquis.SCADA.Web.Server.relatorioindividual.Command.Injection	1720
LAquis.SCADA.Web.Server.relatorionome.Command.Injection	1372
Advantech.WebAccess.SCADA.Password.Parameter.Buffer.Overflow	1000
Rockwell.FactoryTalk.View.SE.SCADA.Remote.Code.Upload	864
7-Technologies.IGSS.SCADA.System.Directory.Traversal	760
7-Technologies.IGSS.SCADA.System.Memory.Corruption	624
CoDeSys.Scada.Webserver.Stack.Buffer.Overflow	576
Measuresoft.ScadaPro.XF.Function.Remote.Command.Execution	494
RealFlex.RealWin.SCADA.Packet.Pasring.Buffer.Overflow	312
Advantech.WebAccess.SCADA.webvact.AccessCode2.Buffer.Overflow	300
DATAC.RealWin.SCADA.Parsing.Buffer.Overflow	252
ABB.MicroSCADA.Wserver.Command.Execution	240
SCADA.Engine.BACnet.OPC.Client.Overflow	208
CitectSCADA.ODBC.Server.Buffer.Overflow	102
Advantech.WebAccess.SCADA.ProjectName.Parameter.Buffer.Overflow	100
Intellicom.Netbiter.webSCADA.Read.CGI.Information.Disclosure	82
Total	**436194**

Tabella delle signature OT maggiormente individuate nel mondo

In Italia l'attacco più identificato è mySCADA.myDESIGNER.Import.ZIP.Directory.Traversal, che a livello mondiale si colloca al terzo posto.

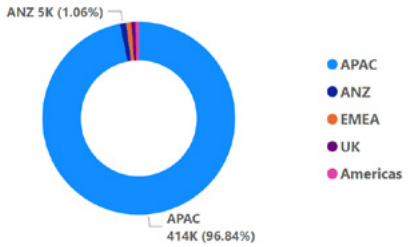
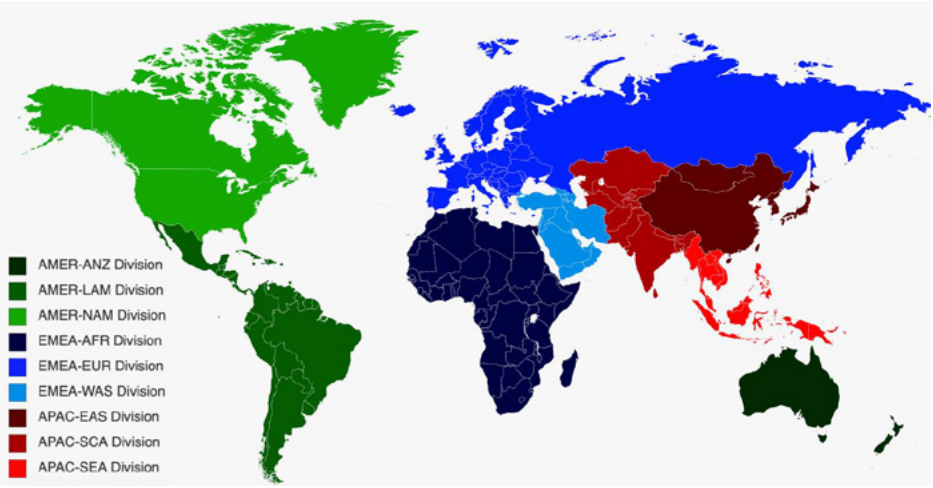


Grafico delle aree che hanno individuato più attacchi a livello mondiale

Dal punto di vista della distribuzione, l'area APAC (Asia Pacifica) è quella maggiormente bersagliata, seguita da sud America ed EMEA (Europa, medio-est, Africa). In queste classifiche bisogna considerare le percentuali riportate sempre da due punti di vista distinti e opposti: una percentuale elevata indica un numero di attacchi cospicui tentati da parte dei cyber criminali, ma allo stesso modo una presenza consolidata di soluzioni di OT security. Infatti, solo chi sta costruendo un'infrastruttura di sicurezza state-of-art ha la capacità di individuare attacchi e bloccarli, quindi di conteggiarli.



Mavcro-aree mondiali

All'interno di queste aree vengono di seguito indicati i paesi che hanno identificato il maggior numero di attacchi SCADA.

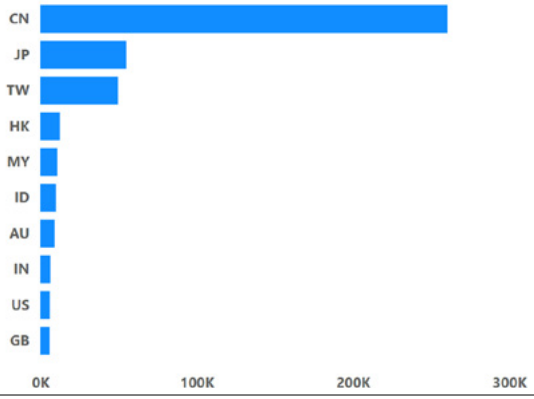


Grafico dei paesi che hanno individuato più attacchi a livello mondiale

Analizziamo in dettaglio i tre attacchi più individuati al mondo per capire cosa comportano. Partiamo dalla terza posizione, anche in considerazione del fatto che mySCADA.myDESIGNER.Import.ZIP.Directory.Traversal è l'attacco con più riscontri in Italia, con un picco importante nel mese di Giugno.

Indicatros of Comprmise (IoC)	Count
CirCarLife.Scada.HTTP.Credential.Information.Disclosure	255950
LAquis.SCADA.Web.Server.Directory.Traversal	121674
mySCADA.myDESIGNER.Import.ZIP.Directory.Traversal	39832

Tabella delle prime tre signature OT maggiormente individuate nel mondo

Signature: mySCADA.myDESIGNER.Import.ZIP.Directory.Traversal

Descrizione

Attacco che mira a sfruttare una Directory Traversal Vulnerability in mySCADA myDESIGNER. La vulnerabilità è dovuta all'assenza di un'opportuna validazione dell'input nell'elaborazione dei file di progetto durante l'operazione di importazione. Un attaccante remoto può sfruttare questa vulnerabilità inducendo un utente target ad aprire un file di progetto opportunamente costruito. Lo sfruttamento della vulnerabilità può comportare l'esecuzione di codice arbitrario da remoto nel contesto di sicurezza dell'utente target.

Prodotti affetti

mySCADA myDESIGNER 8.20.0 e precedenti

Impatto

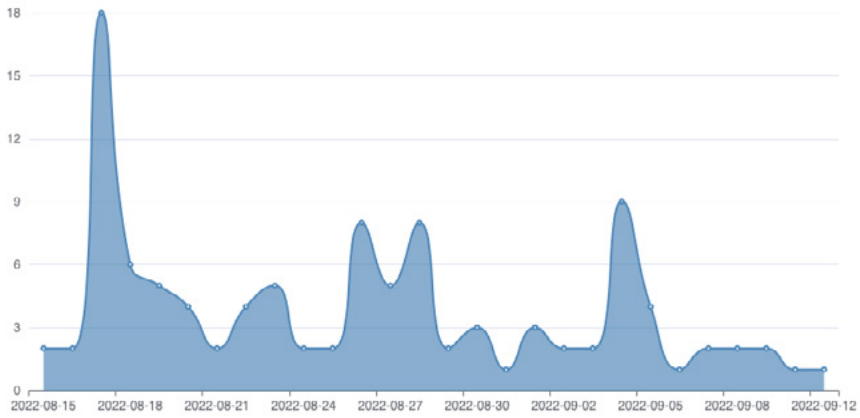
System Compromise: Attaccanti remoti possono prendere il controllo dei sistemi vulnerabili.

Azioni raccomandate

Applicare il più recente upgrade disponibile o la patch fornita dal vendor.
https://www.myscada.org/version-8-22-0-released-security-update/
CVE References: CVE-2021-43555

Telemetria

Numero di intercettazioni a livello mondiale dell'attacco nell'ultimo periodo in cui sono stati estratti i dati.



Signature: LAquis.SCADA.Web.Server.Directory.Traversal

Descrizione

Attacco che mira a sfruttare una Directory Traversal Vulnerability in LAquis SCADA. Remotamente un attaccante non autenticato può sfruttare questa vulnerabilità mandando una richiesta opportunamente forgiata ad un server target. Lo sfruttamento con successo della stessa può comportare condizioni di unrestricted directory traversal e information disclosure.

Prodotti affetti

LAquis SCADA precedenti a 4.1.0.4150

Impatto

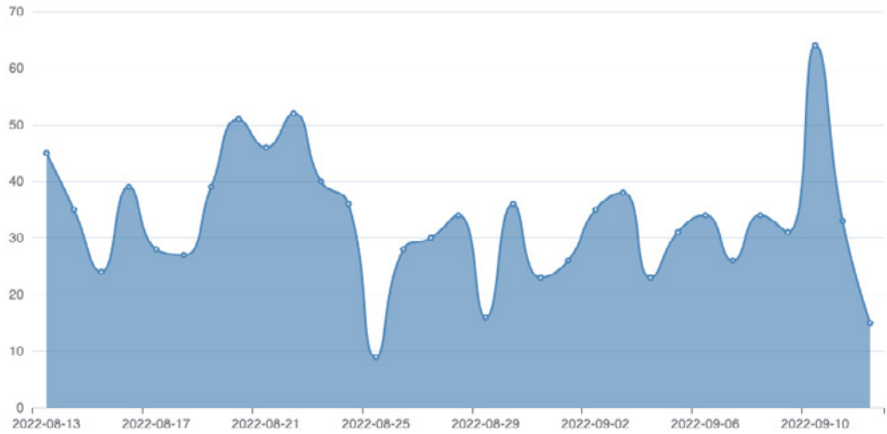
Information Disclosure: un attaccante remoto può ottenere informazioni sensibili dai sistemi vulnerabili.

Azioni raccomandate

Applicare il più recente upgrade disponibile o la patch fornita dal vendor.
https://laquisscada.com/
CVE References: CVE-2018-18990

Telemetria

Numero di intercettazioni a livello mondiale dell'attacco nell'ultimo periodo in cui sono stati estratti i dati.



Signature: CirCarLife.Scada.HTTP.Credential.Information.Disclosure

Descrizione

Attacco che mira a sfruttare una Information Disclosure Vulnerability in CirCarLife Scada. La vulnerabilità è dovuta ad un errore nell'applicazione vulnerabile durante la gestione di una richiesta malevola. Un utente malintenzionato può sfruttare la vulnerabilità per accedere a file arbitrari sulla macchina interessata tramite una richiesta opportunamente forgiata.

Prodotti affetti

CirCarLife Scada before version 4.3

Impatto

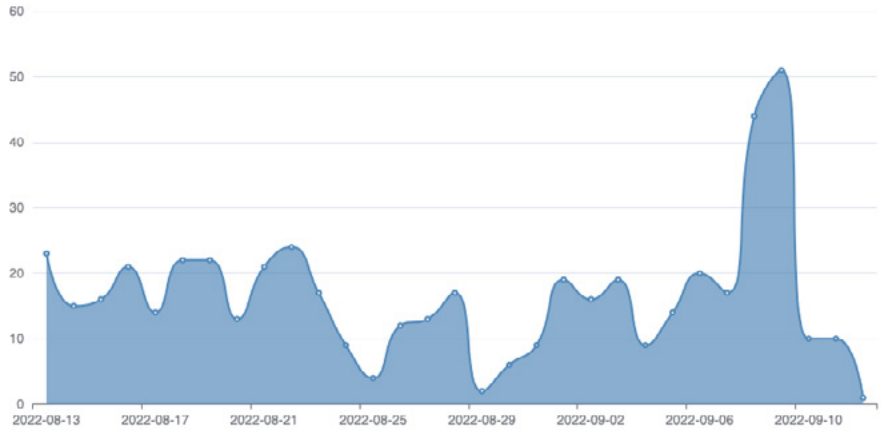
Information Disclosure: un attaccante remoto può ottenere informazioni sensibili dai sistemi vulnerabili.

Azioni raccomandate

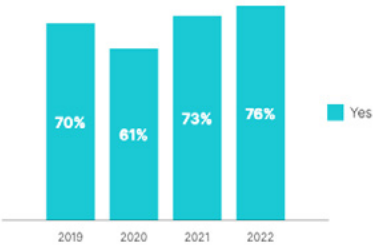
Attualmente non siamo a conoscenza di upgrade o patch messi a disposizione del vendor.
CVE References: CVE-2018-16669 CVE-2018-12634

Telemetria

Numero di intercettazioni a livello mondiale dell'attacco nell'ultimo periodo in cui sono stati estratti i dati.

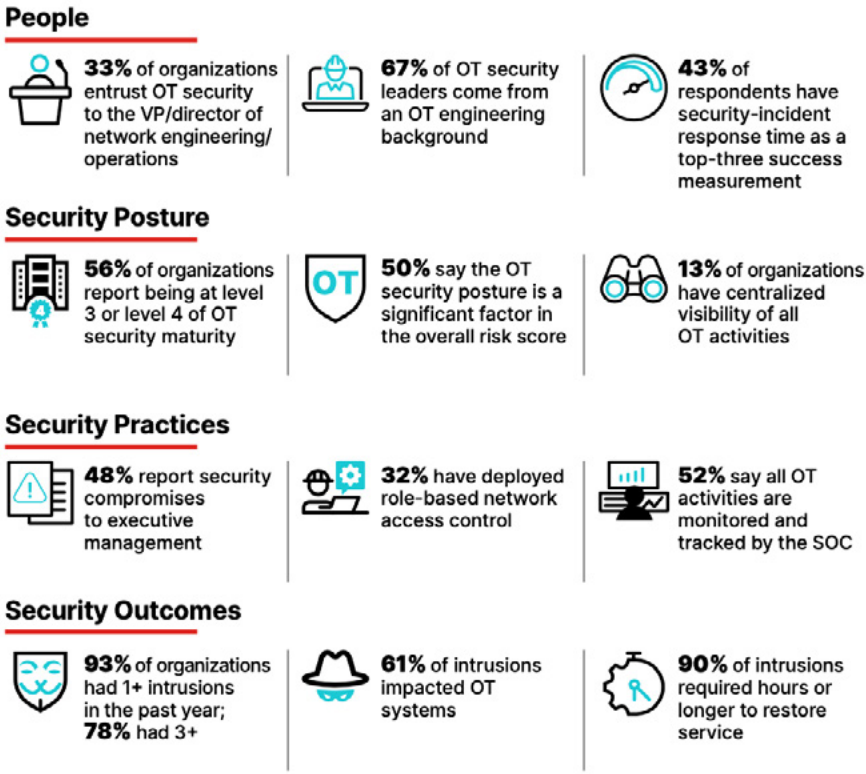


Indagine sullo stato di Operational Technology e Cybersecurity



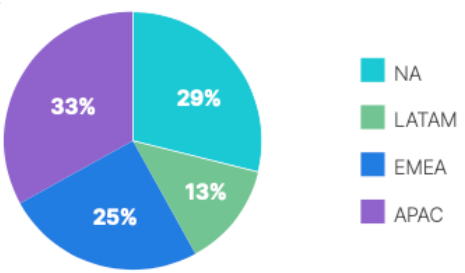
Percentuale di intervistati che giudica necessaria la gestione di OT Sec da parte dei CISO entro un anno

Sulla base di un'indagine globale condotta su oltre 500 professionisti della sicurezza OT, il rapporto Fortinet 2022 rileva che, sebbene la sicurezza OT abbia l'attenzione dei leader dell'organizzazione, continua ad essere indirizzata senza la presenza dei CISO.
Per molti degli intervistati la sicurezza è parte della valutazione del proprio lavoro, anche se molti sono valutati maggiormente su logiche di efficienza e produttività. Di seguito i punti chiave emersi dal sondaggio:

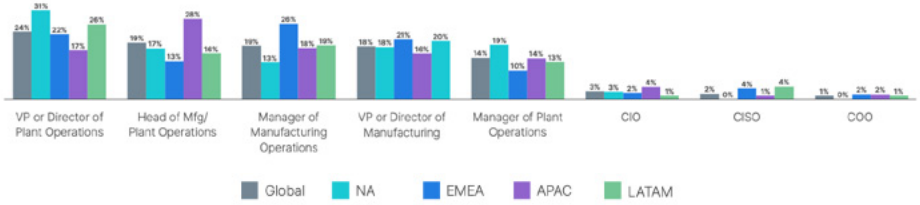


Punti chiave emersi nell'indagine Fortinet OT 2022

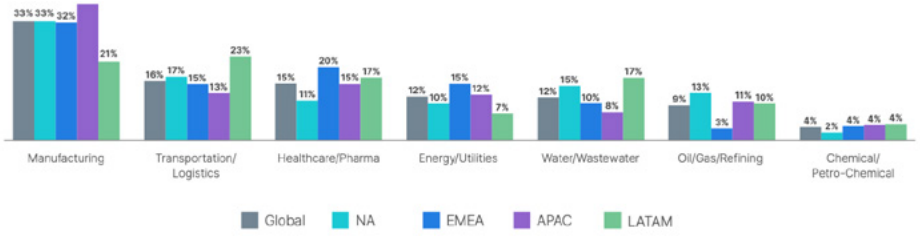
L'indagine è stata condotta a livello globale, nello specifico sono state intervistati esperti di settore secondo le seguenti percentuali.



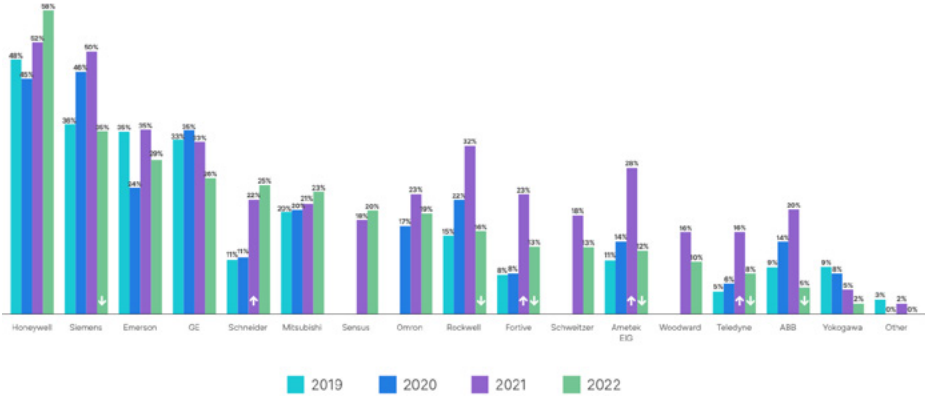
Percentuale dei professionisti coinvolti nelle distinti macro regioni mondiali



Percentuale dei professionisti coinvolti in base al ruolo aziendale



Percentuale dei professionisti coinvolti in base al titolo e al mercato di appartenenza



Percentuale dei vendor OT utilizzati

"Effetti della guerra sulla sicurezza delle Infrastrutture Critiche"

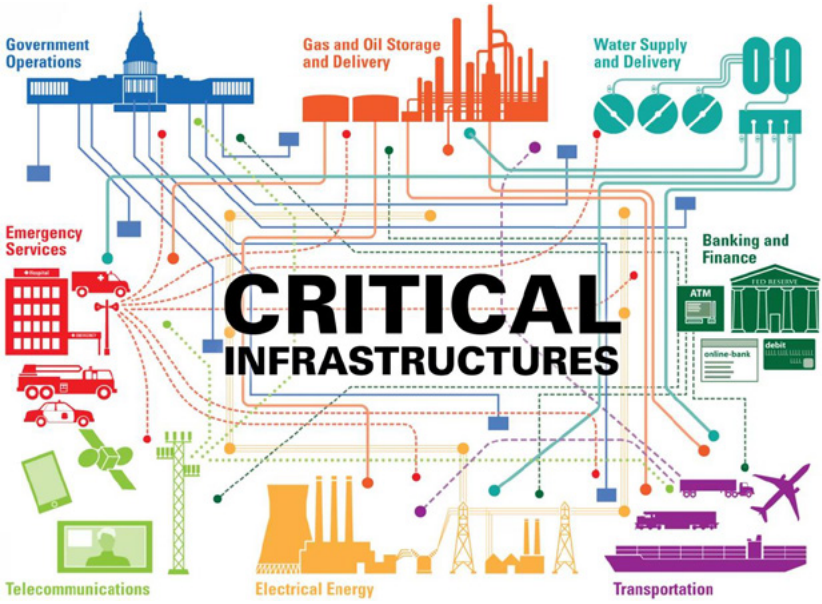
Una questione di cyber resilience quale calibrata sintesi di risk management, business continuity & cybersecurity

[A cura di Federica Maria Rita Livelli]

Scenario

L'attuale conflitto sta evidenziando la necessità di un approccio concreto e operativo al tema della cybersecurity, soprattutto in relazione alle Infrastrutture Critiche dei paesi dichiarati ostili da Mosca, tra cui l'Italia.

Ricordiamo che lo sviluppo, la sicurezza e la qualità della vita nei paesi industrializzati dipendono dal funzionamento continuo e coordinato di un insieme di infrastrutture che, per la loro importanza e strategicità, sono definite "Infrastrutture Critiche".
Il ministero degli Interni del nostro Paese definisce le Infrastrutture Critiche come "le risorse materiali, i servizi, i sistemi di tecnologia dell'informazione, le reti e i beni infrastrutturali che, se danneggiati o distrutti, causerebbero gravi ripercussioni alle funzioni cruciali della società, tra cui la catena di approvvigionamenti, la salute, la sicurezza e il benessere economico o sociale dello Stato e della popolazione". Rientrano in tale tipologia:



Fonte immagine: *https://privacy108.com.au/insights/new-security-obligations-critical-infrastructure-providers/*

- Gli impianti e le reti energetiche;
- Sistemi di comunicazione e tecnologia dell'informazione e le reti informatiche;
- La finanza;
- Il sistema sanitario;
- L'approvvigionamento alimentare e idrico;
- I trasporti;
- La produzione, lo stoccaggio e il trasporto di sostanze pericolose;
- L'amministrazione pubblica soprattutto nell'erogazione dei servizi pubblici essenziali.

Al fine di fronteggiare i sofisticati attacchi informatici odierni è necessario poter disporre di tecnologie avanzate, infrastrutture sicure e maggiore cooperazione operativa, unitamente a un approccio comune su parametri di cybersecurity per prodotti e servizi anche a livello europeo.

Di fatto, le infrastrutture critiche sono sempre più controllate e monitorate da Sistemi di Controllo Industriale (*Industrial Control System - ICS*), inclusi i sistemi SCADA (*Supervisory Control and Data Acquisition*).
Inoltre, è doveroso ricordare che i prodotti ICS si basano principalmente su piattaforme di *embedded standard system* e spesso utilizzano software commerciali standard che, se da un lato facilitano una riduzione dei costi e una maggiore facilità d'uso, dall'altro lato aumentano l'esposizione agli attacchi basati su reti di computer rendendo indispensabile la implementazione di misure di sicurezza.

Infrastrutture Critiche - Normative principali

Il Programma Europeo per la Protezione delle Infrastrutture Critiche (*European Program of Critical Infrastructure Protection - EPCIP*), presentato dalla Commissione Europea nel 2006, ha delineato una serie di principi, processi e strumenti proposti per la sua implementazione. Successivamente è stato anche definito un piano d'azione complementare *Critical Information Infrastructure Protection* (CIIP), costruito su cinque pilastri: preparazione e prevenzione, rilevamento e risposta, mitigazione e ripristino, cooperazione internazionale e criteri per le infrastrutture critiche europee.

La Direttiva 2008/114/CE - sull'identificazione e la designazione delle Infrastrutture Critiche europee – ha, invece, l'obiettivo di istituire sia una "procedura per l'identificazione e la designazione delle Infrastrutture Critiche europee (*European Critical Infrastructure - ECI*) sia un approccio comune alla valutazione della necessità di migliorare la protezione delle tali infrastrutture al fine di contribuire alla protezione delle persone. Allo stesso tempo, l'Agenzia dell'Unione Europea per la Sicurezza delle Reti e dell'informazione (*European Network Security Agency - ENISA*) si propone di attuare le misure CIIP.

Sempre in un'ottica di adeguamento allo scenario in continua evoluzione, è in fase di approvazione la direttiva *NIS2 (Network and Information Security- versione 2)*, che contiene norme più dettagliate e maggiori sanzioni per aziende ed enti pubblici relativamente agli incidenti informatici. Inoltre, in termini di Direttiva ECI la NIS2 richiede agli Stati membri di identificare le Infrastrutture Critiche nei loro territori e di designarle come ECI. A seguito di questa designazione, i proprietari/operatori di ECI sono tenuti a creare piani di sicurezza dell'operatore (Operator Security Plans - OSP), che dovrebbero stabilire soluzioni di sicurezza pertinenti per la loro protezione. Senza dimenticare le varie linee guida di ENISA riferite alle Critical Information Infrastructure assets and services unitamente a misure e risorse per il rafforzamento delle capacità di cybersecurity.

Oltre Oceano, il *National Institute of Standards and Technology (NIST)* ha pubblicato nel febbraio 2014 il Framework for Improving Critical Infrastructure Cybersecurity, che fornisce una linea guida generica su come le aziende e le istituzioni responsabili delle Infrastrutture Critiche possono organizzare, migliorare, mitigare e riprendersi da un attacco informatico.

Scenario Geopolitico vs. Infrastrutture Critiche

Sappiamo da anni che, almeno da marzo 2016, *i cyber hacktivist* del governo russo hanno preso di mira diversi settori delle Infrastrutture Critiche degli Stati Uniti, tra cui l'energia, il nucleare, le strutture commerciali, l'acqua, l'aviazione e i settori manifatturieri critici.

Negli anni successivi, con l'accelerazione della trasformazione digitale, i criminali informatici e gli attori *state-nation* hanno concentrato maggiormente i loro sforzi su questi settori considerando che, se da un lato la convergenza di asset fisici e digitali crea un vantaggio competitivo, dall'altro lato comporta rischi inevitabili.
Alla fine di marzo, diversi gruppi di *hacktivist,* come i Cyber Partisans bielorussi, Anonymous, il gruppo KillNet, AgainstTheWest, il gruppo KelvinSecurity, UNC1151/Ghostwriter/TA445 e Network Battalion 65' (NB65), hanno iniziato a far sentire la loro presenza. Inoltre, vi sono gruppi di criminali informatici come Conti, Xenotime, Dymalloy e Allanite che continuano a prendere di mira le Infrastrutture Critiche.

Di fatto, le Infrastrutture Critiche rientrano sempre più nel campo di battaglia del conflitto Russia-Ucraina in atto; ricordiamo che all'inizio di aprile 2022, le sottostazioni elettriche ad alta tensione gestite da un fornitore di energia in Ucraina sono state prese di mira dal malware Industroyer2, con l'intento di causare danni manipolando i sistemi di controllo industriale.

È doveroso ricordare che un attacco cyber segue i principi della guerra asimmetrica: non c'è un fronte ben definito, gli attacchi possono raggiungere qualunque punto ed in qualunque momento e creare danni sostanziali.

Di fatto, l'uso del cyber come arma offensiva all'interno di un conflitto geopolitico potrebbe essere considerato una strategia militare in quanto consente interruzioni pur mantenendo la negazione, o almeno, non provocando un'escalation immediata. Ovvero: dal momento che non abbiamo una visibilità perfetta in tutte le reti di Infrastrutture Critiche, è difficile rilevare in modo affidabile i primi segnali di tali azioni coordinate e attribuirli in modo accurato. Pertanto, a fronte di questa escalation di attacchi perpetrati ai danni delle Infrastrutture Critiche, è sempre più necessario prendere misure proattive in termini di protezione/prevenzione che deve essere diffusa, aggiornata e strutturata secondo criteri solidi, validati e condivisi.

RAPPORTO IBM –Infrastrutture Critiche

Secondo il recente report di *IBM - Cost of a Data Breach 2022* continuano ad aumentare le preoccupazioni relative a possibili attacchi cyber ai danni delle Infrastrutture Critiche.
Il rapporto di IBM rivela che il ransomware e gli attacchi distruttivi hanno rappresentato il 28% delle violazioni tra le organizzazioni di Infrastrutture Critiche studiate, evidenziando come gli attori delle minacce stiano cercando di colpire le catene di approvvigionamento globali che fanno affidamento su queste organizzazioni. Ciò include, tra le altre, società di servizi finanziari, industriali, di trasporto e sanitarie.

Inoltre, lo studio rivela che quasi l'80% delle organizzazioni di Infrastrutture Critiche studiate non adotta strategie zero trust e di conseguenza il costo medio delle violazioni è aumentato a 5,4 milioni di dollari, i.e. un aumento di 1,17 milioni di dollari vs. le organizzazioni che adottano tale strategia.

Le violazioni nelle organizzazioni di Infrastrutture Critiche sono dovute principalmente a:
- 28% - ransomware o attacchi dirompenti s
- 17% -partner commerciale inizialmente compromesso.

Thales Data Threat Report 2022 Critical Infrastructure Edition

Il rapporto scaturisce dall'intervista/sondaggio a 300 professionisti della sicurezza di organizzazioni di Infrastrutture Critiche in tutto il mondo e rivela che, nonostante una elevata consapevolezza dell'evoluzione dei rischi delle Infrastrutture Critiche non si è stato un miglioramento della gestione.

Il report evidenzia che la perdita di dati da violazioni continua ad essere problematica a causa dei bassi tassi di crittografia e delle pratiche di gestione delle chiavi di accesso eccessivamente complicate, che tendono a essere in contrasto tra loro.

Inoltre, in termini di attacchi, il rapporto rivela che il 55% degli intervistati ha classificato il malware come la principale fonte di maggiori attacchi alla sicurezza, seguito da vicino dal ransomware (53%).

È interessante notare che le società di trasporto hanno riportato aumenti di malware più elevati rispetto alla media (+65%) e un minor numero di casi di ransomware (+45%). Il settore dell'autotrasporto e delle spedizioni hanno riportato casi di malware notevolmente inferiori (+32%) e subito attacchi ransomware molto più elevati (+64%).
Inoltre, risulta che il 19% degli intervistati di Infrastrutture Critiche ha subito un attacco ransomware vs. 20% del sondaggio complessivo, mentre il settore dei trasporti e dell'energia/servizi pubblici hanno invece riportato attacchi ransomware inferiori (+17%).

In termini di strategie di mitigazione, il *Multi Factor Authentication (MFA)* risulta implementato solo dal 58% delle Infrastrutture Critiche intervistate, mentre l'approccio Zero trust continua a guadagnare slancio, in particolare, negli ambienti di accesso remoto e cloud. È doveroso sottolineare che una vera strategia Zero trust dovrebbe essere ugualmente applicabile a tutti gli utenti e dispositivi, indipendentemente dalla posizione, in modo da garantire una strutturata cyber resilience.

Resilienza delle Infrastrutture Critiche: una calibrata sintesi di Risk Management, Business Continuity & Cybersecurity

È doveroso ricordare che la resilienza informatica si riferisce alla capacità di un'organizzazione di prepararsi, difendersi e riprendersi da minacce/attacchi informatici in modo da limitare le violazioni e garantire la continuità del business senza alcuna interruzione.
Ne consegue che ogni Paese deve essere in grado di far fronte a qualsiasi tipo di minaccia e progettare le strategie per rimanere resiliente considerando che le Infrastrutture Critiche sono sempre più digitalizzate e dipendenti da terze parti e, di conseguenza, maggiormente vulnerabili agli attacchi informatici su più vettori. Pertanto, urge garantire un approccio strutturato scaturito dalla calibrata sintesi dei principi di Risk Management, Business Continuity & Cybersecurity.

Di fatto, le organizzazioni delle Infrastrutture Critiche devono capire a che punto sono oggi, al fine di fissare obiettivi per il futuro. Ovvero, non si può gestire ciò che non si conosce e, facendo rimando alla vecchia massima aristotelica *gnòthi seautòn* - i.e. conosci te stesso – esse devono acquisire la consapevolezza di sé e dei punti di cedimento che le caratterizzano. Pertanto, in un'ottica di approccio risk-based e resilience-based, le Infrastrutture Critiche dovranno implementare i principi di risk management, business continuity e cyber security in modo tale da:

- **Analizzare i rischi** –Si tratta di stabilire un inventario delle risorse dell'Infrastruttura critica in termini di hardware e software, nonché in termini di informazioni/dati in modo da identificate le diverse minacce sia interne sia esterne, sia di tipo intenzionali o accidentali. I rischi identificati dovranno essere successivamente mitigati attraverso strategie di protezione, controlli e misure di sicurezza.
- **Stabilire una governance della sicurezza -** Le risorse tecnologiche devono essere allineate con il business dell'organizzazione; ne consegue che è necessario stabilire un

quadro per la governance delle tecnologie dell'informazione in modo da progettare la strategia e la pianificazione delle tecnologie tenendo in considerazione i principi di info-cybersecurity e di risk management in modo appropriato. Ovvero si tratta di progettare un sistema di gestione della sicurezza delle informazioni (ISMS) allineato con il business.

- **Progettare la Operational Resilience -** Si tratta di identificare le operazioni necessarie per il business, la loro automazione e monitoraggio, in modo da rispondere agli incidenti e garantire il ripristino in caso di crisi, incidenti o eventi dirompenti secondo i principi di business continuity e cybersecurity. Si dovranno definire, altresì, le procedure di aggiornamento delle applicazioni (DevOps), identificare le strategie di protezione (i.e. il software necessario antivirus, sistema operativo, database, ecc.) e, soprattutto, come garantire la business continuity attraverso una puntuale analisi degli impatti, progettazione di piani di disaster recovery, incident management, crisis communication, ecc.
- **Definire l'architettura di Operation security -** Si tratta di: progettare la rete, insieme ai dispositivi di protezione perimetrale necessari; definire la gestione degli accessi e delle identità in base alle operazioni da svolgere, garantendo la sicurezza delle comunicazioni.
- **Garantire la sicurezza del software di base -** È necessario stabilire procedure e attività propedeutiche a mantenere aggiornati sia gli antivirus sia i diversi server applicativi, la email., il web, i sistemi operativi e i sistemi di gestione dei database.
- **Controllare adeguatamente l'accesso ai sistemi -** Urge garantire la sicurezza fisica dei diversi asset, sia dall'esterno delle strutture sia dall'interno di esse. Altrettanto importante è definire e gestire le procedure di accesso ai sistemi da parte del personale, in base al loro ruolo e attività, prestando particolare attenzione nei casi di cambio di mansione o risoluzione del contratto.
- **Misurare la sicurezza in modo continuo -** Si tratta di valutare in modo permanente che i controlli e le procedure funzionino in base alle esigenze dell'organizzazione e alle operazioni che vengono eseguite.
- **Formazione, esercitazioni e consapevolezza –** È quanto mai necessario garantire una formazione continua al personale e svolgere esercitazioni periodiche per aumentare la cultura della cybersecurity in termini di social engineering, phishing, errori comuni, dato che avere personale qualificato permettere di essere maggiormente proattivi nel rilevare e rispondere agli incidenti.

Ovvero, si tratta di garantire la cyber resilience delle Infrastrutture Critiche secondo un approccio di:

- **Cybersecurity Predittiva -** attività di Domain Threat Intelligence, Cyber Threat Intelligence, Early Warning Threat Intelligence, Technology Monitoring, Social Threat Intelligence, Supply Chain Cyber Risk, ecc.
- **Cybersecurity Preventiva -** attività di Vulnerability Assessment, Network Scan, Penetration Test, Code Review, Phishing Attack, Smishing Attack, Security Management, Cyber Security Framework Check-up, Ransomware Attack Simulation, Security Operation Center (SOC) Performance Simulation, Zero Day Attack Simulation, ecc.

- **Cybersecurity Proattiva –** dotazione di un SOC e un Incident Response Team, continuo training del personale e periodiche esercitazioni.

Conclusione

Indubbiamente, non esiste una pozione magica che permetta di preservare completamente le Infrastrutture Critiche dagli attacchi informatici,
La cyber resilience delle Infrastrutture Critiche scaturisce dalla implementazione dei principi di Risk Management, Business Continuity, unite ad una visione globale della Cybersecurity.

Le Infrastrutture Critiche dovranno sempre più garantire il governo della sicurezza con una visione strategica molto ben definita e coerente con i servizi e i prodotti che devono essere salvaguardati. Pertanto, sarà sempre più fondamentale essere consapevoli che:

- **La sicurezza informatica deve essere intesa come un processo continuo -** Le Infrastrutture Critiche necessiteranno sempre di protezione contro attori malintenzionati. La gestione del rischio deve essere al centro di qualsiasi approccio che adottiamo.
- **Il settore della cybersecurity non è ancora sufficientemente maturo -** La tecnologia continua ad evolversi e anche gli aggressori stanno innovando le loro tecniche. La sicurezza informatica è un campo in rapido adattamento ed è probabile che rimanga tale per qualche tempo. Pertanto, occorre continuare a lavorare sulle buone pratiche e migliorare i quadri normativi in modo coerente.

- **È necessaria un'armonizzazione degli approcci**. Gli attacchi informatici possono avere effetti intersettoriali agendo in un contesto sempre più interconnesso. Pertanto, è necessaria un'armonizzazione sia delle *good practices* sia degli approcci normativi.
- **La distribuzione delle responsabilità deve essere chiara -** Le responsabilità in materia di sicurezza informatica sono distribuite tra molti attori regionali, nazionali e industriali. Spesso queste entità non parlano al di fuori del loro settore o paese. Tuttavia, gli aggressori non si preoccupano di questi confini, quindi, abbiamo bisogno di un più esteso e capillare scambio di informazioni in relazione a buone pratiche, attacchi informatici e azioni difensive correlate.
- **L'ecosistema della sicurezza informatica deve essere basato sulla fiducia**. I *Computer Emergency Response (Or Readiness) Team (CERT)*, gli *Information Sharing and Analysis Center (ISAC)* e le autorità nazionali competenti che si occupano di cybersecurity avranno probabilmente maggiori responsabilità nei prossimi anni. Per garantire il loro successo, risulterà fondamentale creare un ambiente di collaborazione, fiducia e scambio di informazioni tra attori pubblici e privati.
- **Lo sviluppo delle capacità di cybersecurity deve fondarsi su collaborazione e la costruzione della fiducia**. C'è un chiaro divario di competenze in materia di sicurezza informatica ed è assolutamente necessario un maggiore sviluppo di tali capacità.
- **Le norme internazionali esistenti in materia di cybersecurity devono essere implementate –** Un gran numero di governi nel 2015 ha concordato una serie di norme internazionali sulla sicurezza informatica presso le Nazioni Unite e queste devono essere implementate. Nonostante alcuni paesi abbiano già iniziato a recepirle, ci vorrà ancora del tempo per acquisire un buon livello di efficienza.
- **Il diritto internazionale va adeguato alla natura del cyberspazio -** Recenti discussioni in seno alle Nazioni Unite hanno chiarito che il diritto internazionale si applica al cyberspazio nella sua interezza. Tuttavia, si tratta di un settore emergente del diritto e sono necessari ulteriori lavori per raggiungere un accordo comune sulle modalità di applicazione del diritto internazionale al ciberspazio.
- **Gli hacker dovranno essere sanzionati/puniti -** Attaccare istituzioni e servizi critici è ancora relativamente privo di rischi rispetto ad altri atti criminali. Gli aggressori oggi sono raramente identificati e puniti. Urge un cambio di approccio a livello sia nazionale sia internazionale.

Non si sfuggirà al caos nel cyberuniverso e al ritorno al passato, se non sarà attuata – e praticata con costanza e da tutti – questa semplice, anche se ardua, "tavola delle leggi", per la sua sopravvivenza come forma di civiltà.

Bibliografia

Thales - Data Threat Report 2022 Critical Infrastructure Edition
IBM - Cost of a Data Breach 2022

Le interviste con i partner istituzionali

Inauguriamo con questa edizione del Rapporto una nuova sezione, dedicata agli attori istituzionali (Autority, Agenzie, Forze dell'Ordine e Centri di Competenza) con cui il Clusit ha stretto accordi operativi per:diffondere la cultura della sicurezza informatica presso le Aziende, la Pubblica Amministrazione e i cittadini. Il format utilizzato per questa sezione **è quello dell'intervista.**

Iniziamo quindi con un'intervista al **Prof. Leonardo Querzoni, presidente del Centro di Competenza Italiano sulla Cybersecurity CYBER 4.0**

Cos'è il Centro di Competenza CYBER 4.0?

CYBER 4.0 è una realtà giovane, formalmente nata nel 2020 e pienamente operativa a partire dalla fine del 2021, su spinta del Ministero dello Sviluppo Economico che ne co-finanzia le attività di natura istituzionale. Avviato insieme ad altri sette centri di competenza ad alta specializzazione nel contesto del piano Industria 4.0, CYBER 4.0 è stato scelto nell'ambito della procedura di selezione pubblica bandita nel 2018 sulla base di un programma fortemente incentrato sui temi della cyber security. Il centro è un partenariato pubblico-privato costituitosi nella forma di una associazione non profit, che ha il mandato di svolgere attività di orientamento e formazione a imprese su tematiche relativa alla transizione digitale e all'adozione sicura di tecnologie innovative, anche promuovendo iniziative di ricerca. Ma non solo: oggi CYBER 4.0 intrattiene collaborazioni con la pubblica amministrazione italiana, così come relazioni internazionali con i principali attori europei che gravitano nell'area della cyber security. Il centro oggi conta 45 soci di natura e dimensioni molto diverse: grandi aziende che operano nel settore della cybersecurity (Leonardo, TIM, Almaviva, Engineering, Cy4Gate, etc.), università (Sapienza Università di Roma, LUISS, Tor Vergata, Roma 3, Campus Biomedico, Università dell'Aquila, della Tuscia e di Cassino), aziende di dimensione media e piccola che erogano servizi altamente specializzati o che producono soluzioni di sicurezza, associazioni di settore.

Quali sono i principali campi di attività del Centro?

CYBER 4.0 agisce su tre principali linee di attività. Una prima linea, prettamente istituzionale, riguarda il finanziamento di progetti di innovazione, ricerca industriale e sviluppo sperimentale presentati da imprese. Il finanziamento proviene direttamente dal Ministero e viene erogato integralmente verso le imprese che si vedono riconosciuti parte dei costi di progetto. Ad oggi CYBER 4.0 ha erogato 2,2M di euro di fondi su questa linea attraverso due bandi competitivi. Sono stati finanziati 15 progetti, con un massimo di 200k€a progetto, per un totale di circa 50 tra imprese e centri di ricerca destinatari del finanziamento. I progetti sono attualmente in corso, i primi risultati saranno disponibili nella prima metà del 2023. Sono progetti a TRL molto elevato, il cui obiettivo è di portare in produzione soluzioni innovative già prototipate in laboratorio, per scaricare a terra il valore della tanta innovazione prodotta dalla ricerca industriale italiana.

Una seconda linea di azione, derivante anche questa direttamente dal mandato del Ministero, riguarda lo sviluppo di iniziative volte alla formazione ed orientamento delle piccole e medie imprese sui temi della cyber security. In questo ambito CYBER 4.0 ha avviato diverse attività. Da diversi mesi svolgiamo procedure di assesment della sicurezza per le piccole e medie imprese in collaborazione con il sistema dei Digital Innovation Hub di Confindustria, attraverso una metodologia sviluppata internamente con il contributo delle università e basata sul Framework Nazionale di Cyber Security e protezione dei dati personali. Le aziende che decidono di intraprendere questo percorso ricevono indicazioni dettagliate sui possibili ambiti di intervento, sulle azioni prioritarie da considerare e sulle eventuali soluzioni applicabili per migliorare la propria postura rispetto ai rischi cyber.
Ad inizio ottobre, in occasione del Mese Europeo della Cyber Security, abbiamo anche lanciato il Roadshow CYBER 4.0, una serie di appuntamenti, uno per ogni regione del paese, in cui gli esperti di Cyber 4.0, in collaborazione con le sedi regionali di Confindustria, incontrano le PMI del territorio. In ogni incontro vengono illustrati i rischi più comuni a cui le imprese vanno incontro, vengono fornite indicazioni operative su come evitare questi rischi e ridurre il loro potenziale impatto, il tutto con una serie di attività che mirano a coinvolgere attivamente il pubblico partecipante. Tutti gli incontri sono gratuiti previa registrazione. Dopo il primo incontro svoltosi a Roma, i prossimi appuntamenti sono previsti in Umbria a novembre ed in Abruzzo a dicembre. Le date precise sono disponibili attraverso i canali di comunicazione di CYBER 4.0.
Sempre considerando i rischi legati alle PMI, CYBER 4.0 sta lavorando in questi giorni alla redazione di un *vademecum per le PMI* contenente i passi fondamentali per mettere in sicurezza una realtà aziendale di piccole e medie dimensioni. Il documento rappresenterà una guida semplice ed efficace per indicare i passi fondamentali che le PMI devono affrontare per migliorare il proprio livello di sicurezza. Il vademecum è frutto della stretta collaborazione tra CYBER 4.0 e Unindustria, ed è supportato attivamente da ENISA.
Oltre alle attività istituzionali, CYBER 4.0 ha sviluppato poi nell'ultimo anno numerose collaborazioni. Mi fa piacere in proposito citare lo stretto rapporto di collaborazione con ENISA, con ACN e con la Regione Lazio. Specificamente con Regione Lazio e ACN, CYBER 4.0 ha supportato la strutturazione delle attività dell'Accademia di Cybersicurezza Lazio (ACL), lanciata a Settembre e in corso di avvio operativo nel mese di Novembre. Confidiamo che il modello di formazione implementato in ACL possa essere esportato per iniziative analoghe anche in altre realtà.

Perché oggi è importante un focus sulle PMI?

Le PMI sono diventate da qualche anno uno degli obiettivi principali di gang criminali che vedono in loro un obiettivo facile da colpire e sufficientemente remunerativo. L'Eurobarometro segnala che nel 2021 il 28% delle PMI europee ha subito almeno un episodio legato al crimine informatico. In Italia questa cifra sale fino a toccare il 37%: più di una PMI su tre è stata vittima di un crimine informatico! All'interno dello stesso gruppo di imprese, il 32% ammette che i propri dipendenti hanno un livello informativo limitato

rispetto ai rischi informatici e bel l'85% non ha fatto nulla in proposito nell'anno precedente. Questi dati ci restituiscono la fotografia di un gruppo di imprese, molto ampio, che chiaramente non è preparato ai rischi che gli si parano di fronte. Questo problema è ulteriormente esacerbato per quelle realtà che più recentemente hanno abbracciato la trasformazione digitale accedendo a grandi opportunità a fronte di nuovi rischi.
Come preparare questa massa enorme di imprese? La formazione del personale per incrementare la consapevolezza del rischio e la preparazione necessaria per ridurlo è la chiave per limitare l'impatto degli incidenti. Nell'ultimo anno ENISA ha investito molto per fornire alle PMI degli strumenti e dei consigli pratici per contrastare le minacce. Ma questo non basta. È necessario operare a livello nazionale, e anche più in profondità, direttamente sul territorio, per raggiungere tutte quelle piccole realtà che sono focalizzate totalmente sul proprio business ed hanno bisogno di soluzioni rapide ed efficaci da poter mettere in pratica. Come centro di competenza, CYBER 4.0 sta cercando di indirizzare esattamente questo tipo di interventi.

Il nostro paese si è recentemente dotato di una strategia nazionale per la cybersecurity. Come si pone il centro di competenza rispetto alle sfide poste dalla strategia?

La strategia è una importante novità, attesa da molto tempo: finalmente anche l'Italia ha un piano di ampio respiro che tocca tutti gli aspetti più rilevanti nell'ambito della cybersecurity e fornisce un piano di implementazione chiaro e ben delineato fino al 2026. I punti di interesse all'interno della strategia sono molti, ed il centro di competenza è già impegnato con le proprie attività su molti di questi, in particolare negli ambiti della formazione e orientamento. Un ambito che trovo particolarmente importante e stimolante è quello legato allo scambio informativo relativo alle minacce. La strategia cita, tra le altre cose, la possibilità di favorire la nascita di ISAC (Information Sharing and Analysis Center) settoriali anche basati su partnership pubblico-private. In un recente webinar organizzato da CYBER 4.0 dedicato al tema dell'Information sharing pubblico-privato, tra i diversi elementi di discussione è emersa in particolare l'idea di creare un ISAC che sia specificatamente dedicato alle PMI. Un ISAC di questo genere consentirebbe di avere un punto di riferimento comune per aziende che spesso condividono problematiche più legate alla propria dimensione che al settore specifico di appartenenza e servirebbe da punto di aggregazione per la condivisione di esperienze di risposta ad incidenti e per un innalzamento collettivo del livello di consapevolezza su minacce in corso o prospettiche. In considerazione della natura pubblico-privata della sua constituency, e del mandato istituzionale di supporto alle PMI conferitogli dal Ministero dello Sviluppo Economico, nonché delle competenze che può mettere a disposizione per la gestione delle iniziative correlate e delle comunicazioni da e verso l'Agenzia Nazionale di Cybersecurity, Cyber 4.0 rappresenta certamente un contesto operativo importante in cui avviare un ragionamento sull'opportunità di creare un ISAC per le PMI.

Il CLUSIT ha recentemente aderito a CYBER 4.0. Quali scenari e opportunità apre questa collaborazione?

L'adesione del CLUSIT è per CYBER 4.0 certamente una grande opportunità. CLUSIT nei suoi 22 anni di vita ha costruito un importante network di competenze che spazia dall'ambito pubblico a quello privato. Questo network complementa la compagine sociale di CYBER 4.0, fornendo al centro di competenza un serie di competenze, specialmente nell'ambito degli studi di settore, particolarmente importante. In queste prime settimane dall'ingresso di CLUSIT abbiamo iniziato a delineare alcune attività da svolgere in collaborazione e sono certo che dopo queste esperienze iniziale il livello di collaborazione continuerà a crescere.

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 - Edizione di metà anno, ottobre 2022

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.

Aldo Di Mattia, è entrato in Fortinet nel 2012 con il titolo di System Engineer per poi diventare nel 2018 Principal System Engineer & team leader, nel 2020 Manager Systems Engineering e nel 2022 Senior Manager Systems Engineering. Oggi è il responsabile di un team di sistemisti che coprono il territorio del centro/sud Italia e Malta nei settori: Telco e MSSP; PAC, Defense, Finance e Insurance; PAL e Industry; Energy e 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 2004 e il 2012 per due tra i più importanti System Integrator italiani nella sicurezza informatica in qualità di Systems Engineer, Security Consultant, Sr. Systems Engineer and Team Leader. In questi anni di lavoro ha maturato 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 quattro brevetti con Fortinet presso USPTO (United States Patent and Trademark Office's) contenti innovazioni tecnologiche nella cybersecurity in relazione a: Security API Cooperation; End-point protection and smart working; Deception; SD-WAN.

Gabriele Faggioli, legale, è amministratore delegato di Digital360 e di Partners4Innovation, Presidente del Clusit e Responsabile Scientifico dell'Osservatorio Cybersecurity & Data Protection del Politecnico di Milano. Gabriele è inoltre Adjunct Professor del MIP – Politecnico di Milano ed è stato membro del Gruppo di Esperti sui contratti di cloud computing della Commissione Europea. 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.

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

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 a 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. È Partner di C.I.S.C.A. (Critical Infrastructures Security Consultants & Analysts) a Ginevra.

Federica Maria Rita Livelli, Consulente di Business Continuity & Risk Management, svolge attività di diffusione e di sviluppo della cultura della resilienza presso varie istituzioni ed università oltre ad essere Tutor di corsi di Business Continuity propedeutici al conseguimento della certificazione CBCP presso il DRI Italy. Board Member del BCI Italy Chapter, del CLUSIT Scientific Committe e di diverse Commissioni tecniche CLUSIT ed UNI. E' Socia AIPSA ed (ISC)2 Italy Chapter. Docente di moduli ISO 22301, ISO 31000, ISO 27001 e Crisis Management presso diverse università (SUPSI Lugano, POLIMI–BOCCONI, Verona, Cagliari, Padova, Statale di Milano, Università Genova e LIUC Castellanza). Relatrice e moderatrice in seminari, conferenze nazionali ed internazionali. Autrice di articoli su numerose riviste online italiane ed internazionali. Ha partecipato, in qualità di co-autrice, a: Edizioni 2020, 2021 e 2022 del Rapporto Clusit - Cyber Security; Libri tematici CLUSIT rif. Intelligenza Artificiale (2020) e Rischio Cyber (2021); Libro "Lo Stato in Crisi" ed. Angeli

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

Yuri Riccardo Perseu, Classe 1994, Laureato Magistrale in Marketing presso l'Università LUISS Guido Carli di Roma, inizia la sua carriera nell'Head Hunting nel 2018. La sua prima esperienza è all'interno del settore Accounting & Finance, successivamente diventa Consultant per la Divisione Procurement e Logistics e Sales & Marketing. Da sempre curioso ed appassionato d'informatica sviluppa la sua carriera nel settore, prima nella divisione Technology e poi contribuendo alla nascita del team di ricerca e selezione specializzato nella Cybersecurity di Experis. Attualmente in ManpowerGroup come Team Manager per la Divisione National IT & Cybersecurity di Experis.

Leonardo Querzoni, è professore associato presso la Sapienza Università di Roma e presidente del centro di competenza italiano sulla cybersecurity CYBER 4.0. Ha conseguito il dottorato di ricerca nel 2007 con una tesi sui sistemi middleware basati su eventi. I suoi interessi di ricerca spaziano dalla sicurezza informatica ai sistemi distribuiti e si concentrano, in particolare, su argomenti che includono l'analisi del codice binario, l'elaborazione di stream di dati, l'affidabilità e la sicurezza nei sistemi distribuiti. È autore di oltre 90 articoli pubblicati su alcune delle più prestigiose riviste scientifiche e simposi internazionali. È co-autore del Framework Nazionale per la Cyber Security e la Data protection. Dal 2020 è membro dello steering committee dell'ACM International Conference on Distributed and Event-Based Systems. Dal 2022 è coordinatore del dottorato di ricerca in Cybersecurity organizzato congiuntamente dalle Università Sapienza e LUISS.

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.

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 internazionale in materia di Cyber Defense. E' 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 18a 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, sulla 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.

Il ruolo istituzionale

In ambito nazionale, Clusit opera in collaborazione con: Presidenza del Consiglio, numerosi ministeri, Banca d'Italia, Polizia Postale e delle Comunicazioni, Arma dei Carabinieri e Guardia di Finanza, Autorità Garante per la tutela dei dati personali, Cyber 4.0 - il Centro di Competenza nazionale ad alta specializzazione per la cybersecurity, 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

Il Security Summit del 2022 si chiude con una edizione tutta in streaming il 9 e 10 novembre. Per il **2023** è prevista una edizione tutta in presenza, dal 14 al 16 marzo, seguita da una tappa a Napoli. Nella seconda parte dell'anno si terrà il Security Summit di Verona, in ottobre, e in chiusura un'edizione in streaming, in novembre. Continueranno gli **Atelier della Security Summit Academy**, che si terranno tutto l'anno, e gli **Eventi Verticali**, programmati in maggio (Energy & Utilities), giugno /Health Care) e ottobre (Manufacturing).

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: http://www.securitysummit.it/

In collaborazione con

CROWDSTRIKE

FORTINET

Microsoft

SECURITY SUMMIT

www.securitysummit.it