Exprivia Threat Intelligence Report

Italia – 3Q2022

future. perfect. simple.

Sommario

Indice delle figure

Introduzione

La CyberSecurity si distingue da molte altre scienze in quanto i reali competitor non sono coloro che forniscono soluzioni migliori, ma gli attaccanti che ogni giorno sviluppano tecniche e metodologie per compromettere i servizi utilizzati da coloro che si difendono per averne un beneficio. Exprivia crede nel valore della condivisione e mette a disposizione i dati rilevati su attacchi, incidenti e violazioni privacy dal suo Osservatorio a beneficio di chi lavora nel mondo della CyberSecurity.
L'Osservatorio colleziona informazioni pubbliche e non, anche se abbiamo deciso di condividere e creare statistiche solo utilizzando informazioni pubbliche. Questa decisione si basa sulla volontà di non compromettere in alcun modo la confidenzialità delle informazioni consegnateci dai nostri clienti e per avere un insieme di dati statisticamente validi e il più possibile solidi. Le statistiche vengono aggiornate modificando il numero di sorgenti. Nuove sorgenti vengono inserite solo e soltanto se i dati acquisti sono rilevanti dal punto di vista statistico e integrabili.
A ogni record inserito nel rapporto corrisponde una precisa informazione sulla sorgente da cui questo record è stato preso.
Al fine di ottenere e condividere dati statisticamente rilevanti, si è attuato un restringimento del perimetro all'Italia. I valori della ricerca hanno però valenza a livello globale in quanto indicatori di tendenze consolidate.
In caso di scostamenti da cosa è stato osservato a livello globale, questo scostamento verrà discusso e analizzato ulteriormente nel rapporto.
I record registrati relativamente ad attacchi, incidenti e violazioni privacy sono consolidati al 30/09/2022. Eventuali dati la cui evidenza è successiva a questa data possono non essere oggetto dell'analisi in questione.

Executive Summary

Da oramai quattro quarti (con una leggera flessione solo nel secondo quarto del 2022) eravamo abituati ad una crescita di attacchi ed incidenti ed una riduzione della forbice tra attacco e difesa. La buona notizia è che in questo quarto a fronte di un numero di violazioni della privacy che sono costanti nel tempo, notiamo che attacchi e incidenti diminuiscono e che anche la forbice tra attacco e difesa sembra leggermente riaprirsi. Le buone notizie finisco qui. Infatti, una diminuzione di attacchi lo si era registrato anche nel 3Q2021 anche se in maniera meno drastica per poi riprendere a crescere nel 4Q2021. Altra cattiva notizia è che malgrado si registra una sensibile riduzione del fenomeno rispetto al 2Q2022, il 3Q2022 è sensibilmente peggiorato sia in quantità di attacchi, che di incidenti di sicurezza, che di violazioni privacy che di forbice tra attacco e incidente. Insomma, a fronte di un miglioramento rispetto al quarto precedente, c'è un sensibile peggioramento rispetto all'anno precedente e su tutti i fronti. Alla luce della osservazione del fenomeno in tre anni, risulta evidente che la riduzione di attività commerciali durante l'estate abbia un peso sul fenomeno complessivo sul territorio italiano. Scompaiono quasi del tutto attacchi ed incidenti collegati al conflitto russo-ucraino. Cresce l'Investment Index in tutta Italia. Si ricorda che l'Investment Index è il rapporto tra servizi digitali analizzati e vulnerabilità identificate. Il miglioramento è più sensibile al nord mentre al sud, pur essendo un valore superiore al nord, risulta pressoché costante rispetto al quarto precedente. Lo stesso miglioramento lo abbiamo se l'osservazione la focalizziamo sui dispositivi IoT. Su tutto il territorio nazionale rileviamo un miglioramento dell'UII (Unsecurity IoT Index, rapporto tra dispositivi in rete e vulnerabilità identificate). In questo quarto abbiamo deciso di focalizzare anche la nostra attenzione sui dispositivi medicali che risultano meno a rischio di telecamere e stampanti. Si tratta di un quadro generale, pertanto, in cui tutti gli indicatori sono positivi, da quelli che suggeriscono adozioni di pratiche di security by design (II) all'IoT (UII), passando per riduzione di attacchi, di incidenti e della forbice tra attacco ed incidente. Pertanto, pur essendo uno scenario meno preoccupante del quarto precedente, abbiamo una situazione peggiore rispetto allo scorso anno e che se non si procede nella progressiva riduzione del rischio sul territorio nazionale, corriamo il rischio di dover fronteggiare nei primi mesi del 2023 uno tsunami difficilmente arginabile (se superiore a quello di quest'anno).

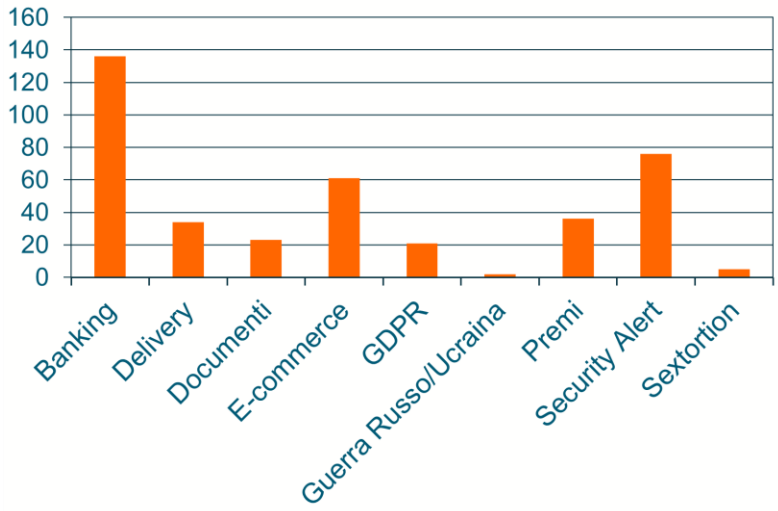

Figura 1 - Tematiche riscontrate di attacchi, incidenti e violazioni privacy nel 3Q2022 in Italia

Attacchi, incidenti e violazioni privacy

Nei rapporti è necessario identificare con dettaglio gli oggetti delle statistiche. Il presente rapporto include dati che fanno riferimento a diversi elementi.

- **Attacchi**: insieme di azioni intraprese per compromettere un servizio. In presenza di una campagna di phishing indirizzata a molti target, verrà contabilizzata la campagna come un attacco. Il rapporto include campagne criminali intese a sfruttare vulnerabilità di servizi ampiamente utilizzati in Italia, anche se non ci sono prove esplicite che la campagna abbia compromesso clienti italiani.
- **Incidenti**: un attacco che ha avuto successo. Nel caso di un attacco che abbia avuto successo su diverse entità, verranno contabilizzate tutte le istanze di incidenti nei confronti delle varie vittime.
- **Violazioni privacy**: vengono contate non solo le violazioni segnalate dalle istituzioni (ad esempio GDPR), ma anche quelle pubbliche quando queste ultime dovessero essere eclatanti. Ovviamente manterremo il riserbo e non esporremo la vittima, anche se la violazione dovrà essere descritta in una sorgente aperta, ma il dato riteniamo che abbia rilevanza statistica, al pari di incidenti e attacchi.

La ricerca degli eventi riprende tutto il primo semestre del 2022 evidenziando un andamento costante degli attacchi, degli incidenti e delle violazioni privacy, registrando dei picchi a marzo e maggio 2022. Marzo è infatti il mese peggiore in termini di casi registrati, ben 386. Questo aumento è da associare ad un'evoluzione della sofisticatezza degli attacchi, degli incidenti e delle violazioni privacy, infatti, attraverso l'utilizzo di tecniche sempre più complesse, continua ad essere sempre più difficile identificare in maniera efficace i cybercriminali.
I mesi di marzo e maggio 2022, dunque, segnano un periodo tragico per gli operatori della sicurezza informatica (rispettivamente 386 e 362 casi analizzati). Il 3Q2022 si caratterizza per una netta diminuzione dei fenomeni osservati (160 nel mese di luglio, 145 agosto, 176 settembre). Tuttavia, il 2022 continua ad essere indubbiamente l'anno più complesso in termini di sicurezza.

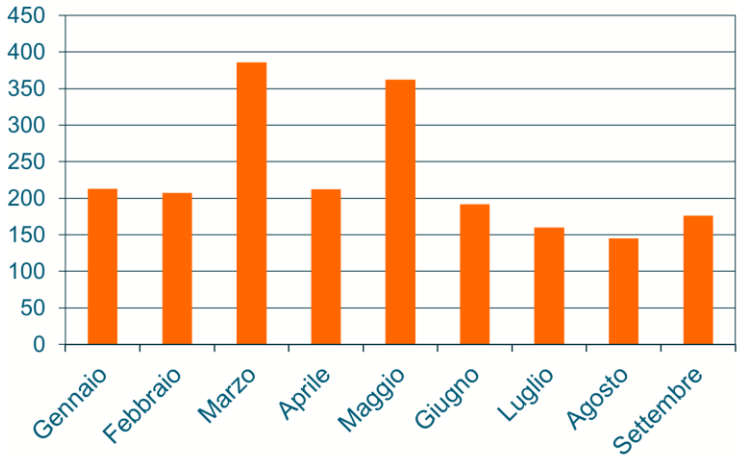

Figura 2 - Numero di attacchi, incidenti e violazioni privacy suddivisi in mesi in Italia

Si conferma la crescita di attacchi, incidenti e violazioni privacy sia nel trimestre oggetto di analisi che per l'intero anno in corso rispetto ai corrispettivi periodi del 2021.
Un'analisi comparativa dei casi registrati nel 3Q2022, pari a 481, rispetto allo stesso periodo dell'anno precedente 3Q2021, pari a 273, evidenzia una percentuale di crescita di circa il 76%. Se ampliamo l'intervallo di riferimento ai dati per l'anno in corso, dal 1Q2022 al 3Q2022, si osserva una totalità di 2053

fenomeni di sicurezza. Nell'analogo periodo dell'anno appena trascorso, dal 1Q2021 al 3Q2021, sono stati registrati 902 casi con un incremento percentuale di ben 128%.

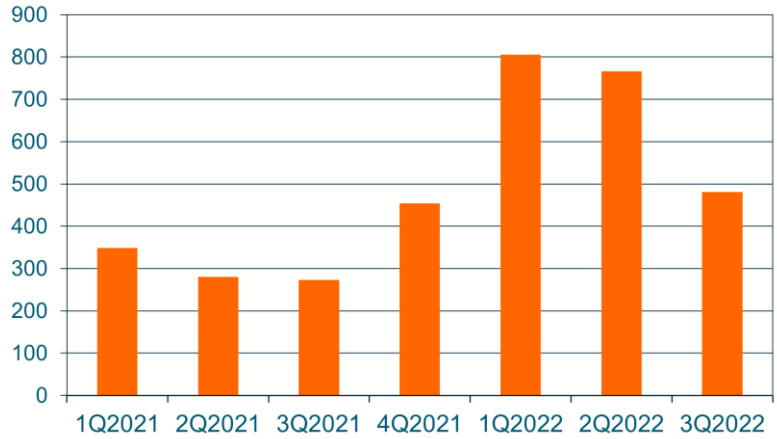

Figura 3 - Numero di attacchi, incidenti e violazioni privacy nel 2021, 1Q2022, 2Q2022 e 3Q2022 in Italia

Nel corso del 3Q2022 sono stati registrati precisamente 251 attacchi, 203 incidenti di sicurezza e 27 violazioni privacy.
Rispetto al 2Q2022 per attacchi e incidenti si registra un decremento significativo (-34% attacchi e -43 % incidenti), mentre per le violazioni della privacy non risulta alcuna variazione significativa.

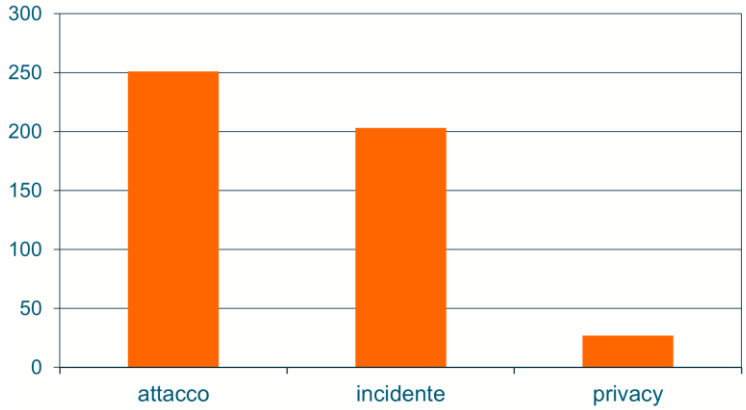

Figura 4 - Numero di attacchi, incidenti e violazioni privacy nel 3Q2022 in Italia

I dati raccolti relativi nel 3Q2022 fanno ben sperare, in quanto, come è evidente dal grafico, sembra che i fenomeni di sicurezza stiano diminuendo, si è registrato un calo del 37% nella loro totalità. Nonostante questa inversione di tendenza, rispetto ai primi sei mesi del 2022, non sono dati da sottovalutare, infatti se confrontati con le rilevazioni del terzo quarto del precedente anno sono comunque di valori maggiori del 76%. Nello specifico, le rilevazioni prese in considerazione se confrontate con quelle del terzo quarter del 2021, evidenziano un aumento del 51% degli attacchi perpetrati, un aumento del 118% degli incidenti di sicurezza ed un aumento del 93% relativi alle violazioni della privacy.

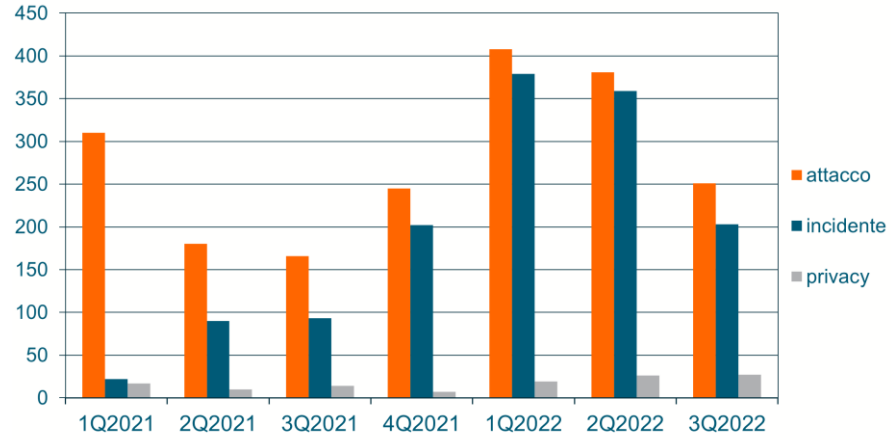

Figura 5 - Numero di attacchi, incidenti e violazioni privacy nel 2021, 1Q2022, 2Q2022 e 3Q2022 in Italia

Motivazione degli attaccanti

Per il 3Q2022 su di un totale di 481 casi, le analisi dei dati rilevano che l'87% di questi casi è attribuibile ad attività legate al crimine informatico, in leggero calo rispetto ai precedenti due quarti.
Tuttavia, resta un valore che se paragonato allo stesso periodo del 2021, in cui si rilevarono 242 eventi, risulta aumentato di oltre il 72%.
A seguire con il 7,6 % del totale dei fenomeni le motivazioni legate ad hacktivism, ed il 5,6 % legate al data breach, infine resta l'1% con 5 fenomeni legati alla guerra cibernetica, in forte calo rispetto ai casi rilevati nei quarti precedenti.

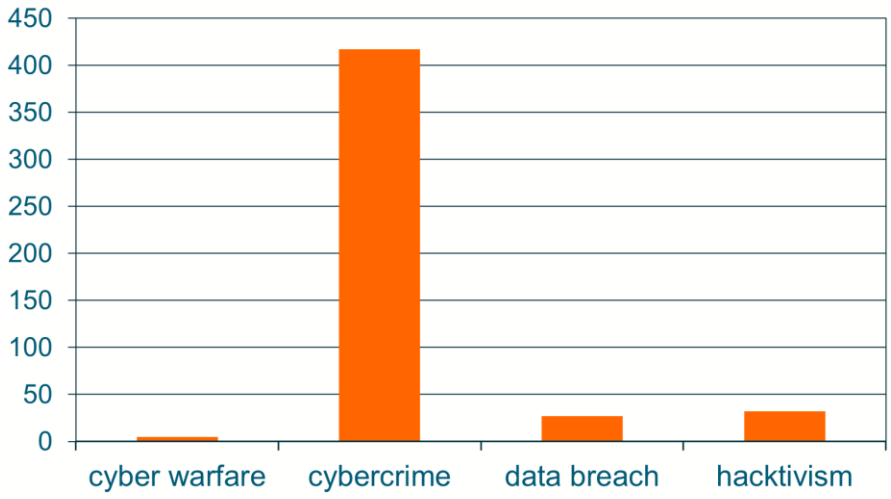

Figura 6 - Conteggio motivazione attacchi, incidenti e violazioni privacy per tipologia nel 3Q2022 in Italia

Come si può notare dal grafico sottostante, negli ultimi sette trimestri è stato il Cybercrime a costituire la maggioranza delle motivazioni dietro gli attacchi informatici, gli incidenti e le violazioni della privacy il cui trend è aumentato significativamente nel primo e nel secondo trimestre del 2022. Nello specifico, rispetto all'ultimo trimestre del 2021 (durante il quale il numero di attività legate al Cybercrime è stato il più alto di tutto il 2021) si è registrato un incremento del 50% nel primo trimestre del 2022, in seguito diminuito del 3% nel secondo trimestre del 2022 rispetto al 1Q2022, diminuito ulteriormente del 29% nel terzo trimestre del 2022 rispetto al 2Q2022.
A partire dal 2022, a seguito del nuovo conflitto bellico del quale la Russia si è fatta protagonista, si è aggiunto alla lista delle motivazioni il cyber warfare, che ha visto un incremento del 436% nel secondo trimestre del 2022 rispetto al precedente, mentre nel 3Q2022, rispetto al trimestre precedente, è diminuito del 96%.
A seguire si osserva che il data breach, l'hacktivism e l'espionage/sabotage si sono alternate nelle ultime tre posizioni in classifica.

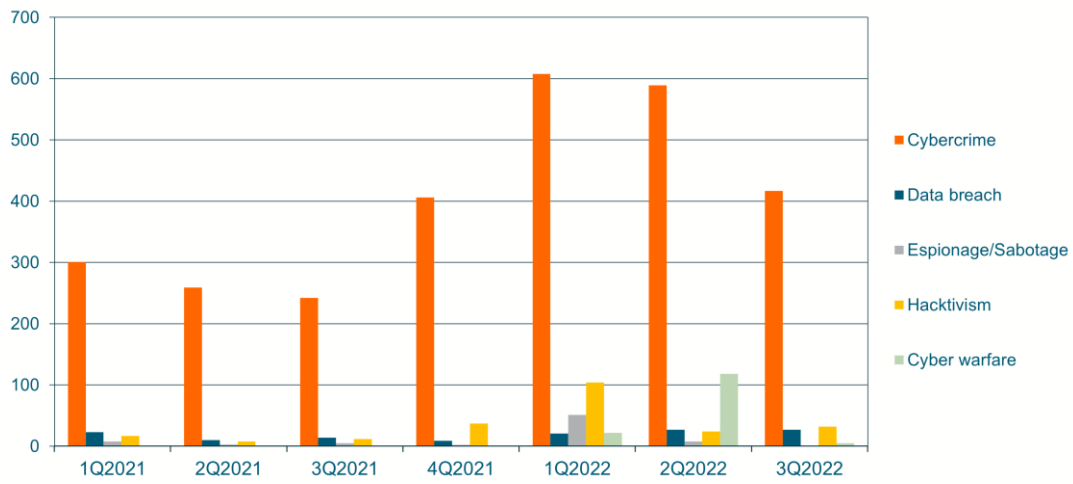

Figura 7 - Conteggio motivazione attacchi, incidenti e violazioni privacy per tipologia nel 1Q2021, 2Q2021, 3Q2021, 4Q2021, 1Q2022, 2Q2022 e 3Q2022 in Italia

Distribuzione geografica

Nel territorio italiano nel 3Q2022, come evidenziato dal grafico, la distribuzione dei fenomeni è piuttosto uniforme. Rispettivamente se ne sono rilevati, dividendo l'Italia in tre macro-aree, 447 nel nord, 448 nel centro ed infine 428 nel sud del paese. La differenza tra la macro-area più colpita e quella meno colpita è solamente del 4% circa.

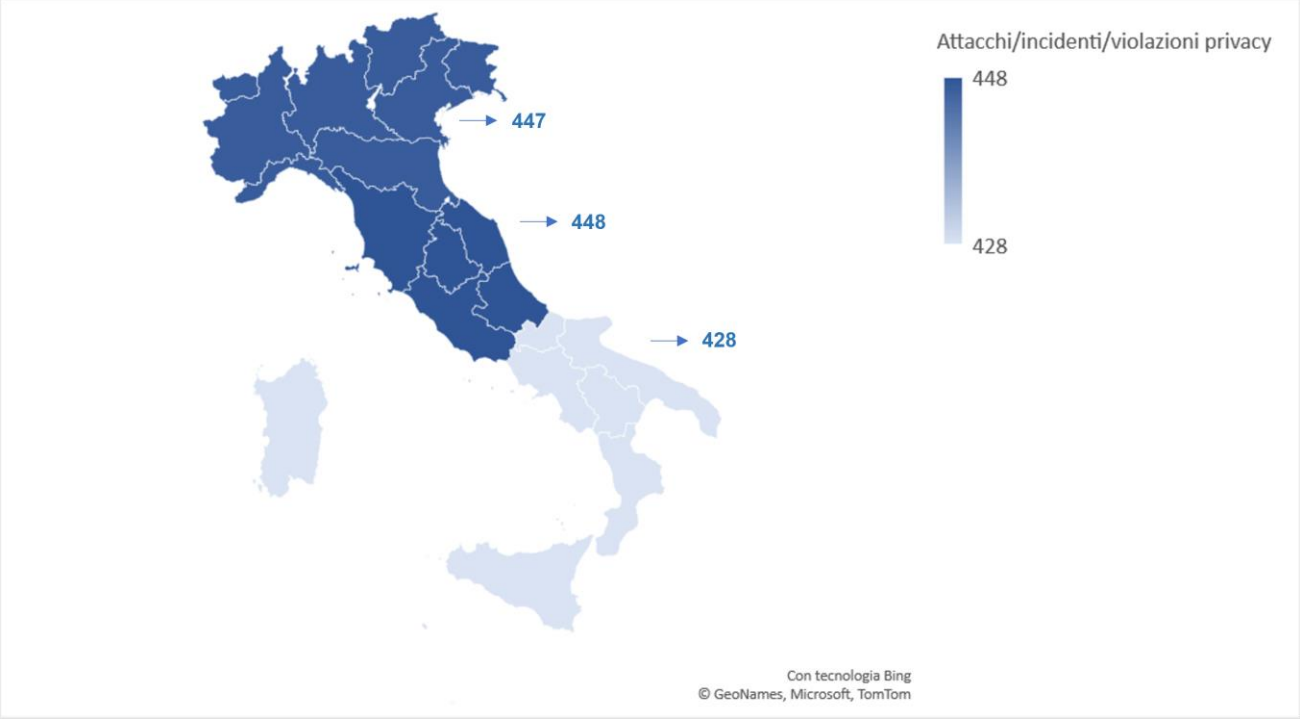

Figura 8 - Distribuzione geografica attacchi, incidenti e violazioni privacy nel 3Q2022 in Italia

Distribuzione vittime per Industria

Appartiene al settore Finance il maggior numero di vittime di attacchi portati a compimento nel 3Q2022. La percentuale sfiora il 37% del totale delle vittime (che sono 481). Continua pertanto il trend rilevato nel 2Q2022 che vede sempre il Finance come settore privilegiato dai cyber-attaccanti, tanto che il numero di attacchi è 2,5 volte superiore al secondo settore più colpito, quello del Software/Hardware (15% degli attacchi sul totale). Anche in questo caso il dato percentuale è speculare a quanto rilevato nel corso del precedente trimestre.
Supera l'11% del totale anche la percentuale degli attacchi al settore industriale, terzo settore di interesse dei cyber criminali.
Gli attacchi alla Pubblica Amministrazione, in percentuale quasi al 10% del totale, restano invece costanti di numero rispetto ai tre mesi precedenti (aprile, maggio e giugno).
In questo trimestre vediamo anche (ri)apparire attacchi, fortunatamente limitati in numero, ai settori Automotive, Cloud, Healthcare e Hospitality.

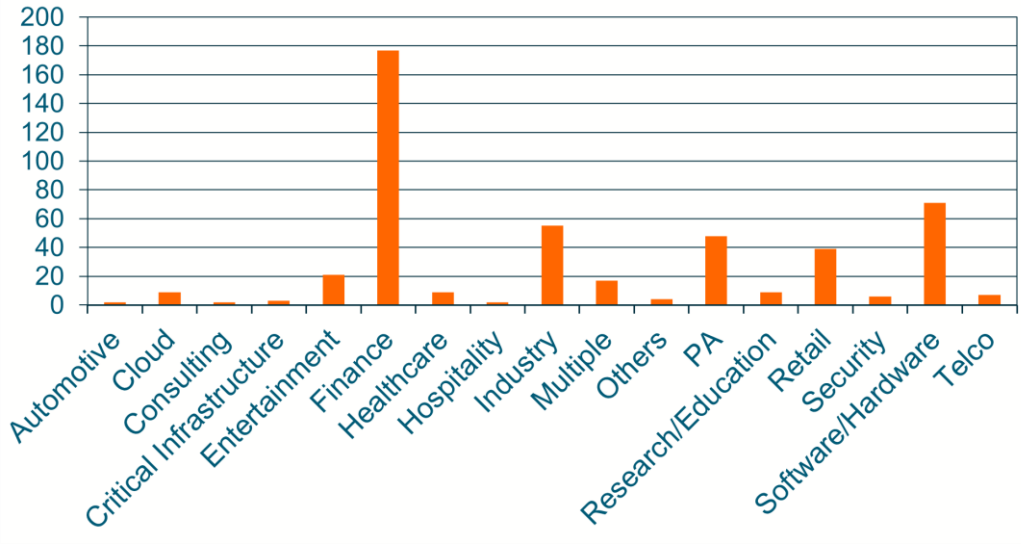

Figura 9 - Tipologia vittime di attacchi, incidenti e violazioni privacy nel 3Q2022 in Italia

Finance

Nel settore Finance, il trend della numerosità di attacchi è in diminuzione rispetto ai quarter immediatamente precedenti, ma comunque in aumento tenendo conto anche dei dati analizzati nel corso del 2021.
Il settore Finance rimane quello maggiormente bersagliato dagli attacchi, con ben 177 casi rilevati dall'Osservatorio nel 3Q2022 e beneficia della diminuzione degli attacchi di Cyber Warfare che erano stati numericamente molto più numerosi nei mesi precedenti.

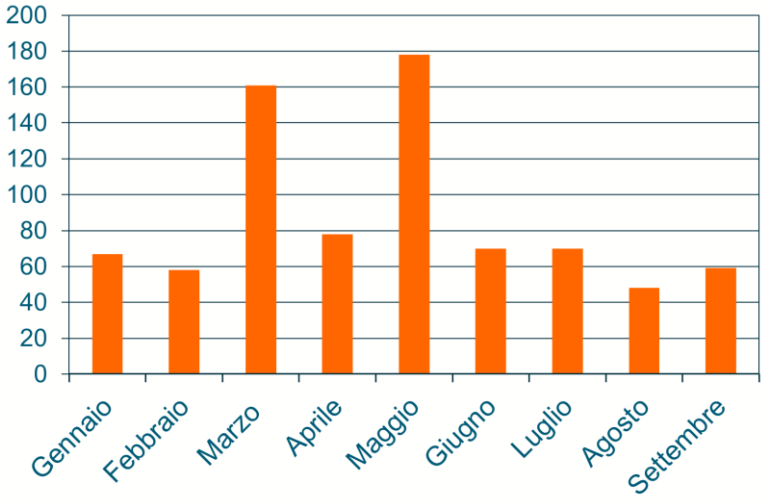

Figura 10 - Attacchi, incidenti e violazione privacy del settore Finance in Italia

Software/Hardware

Nel terzo trimestre del 2022 sono stati registrati 71 casi di sicurezza contro i 130 del trimestre precedente, tutti legati al settore Software/Hardware con un picco di casi a luglio e settembre. Si registra un lieve decremento dei casi, dovuto essenzialmente alle naturali conseguenze dello stop dovuto ai mesi estivi. Tuttavia, già da settembre si registra un re-incremento tipico dell'andamento annuale. Tutto questo con ancora sullo sfondo il conflitto russo-ucraino che foraggia la corsa ai cyber-armamenti, che spinge gruppi cyber criminali ad una massiccia dose di attacchi nei confronti dei Paesi europei.

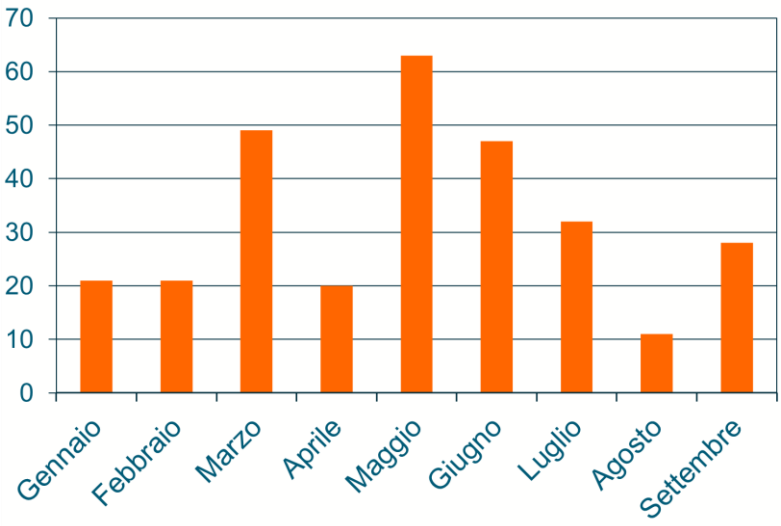

Figura 11 - Attacchi, incidenti e violazioni privacy del settore Software/Hardware in Italia

Industria

Il settore dell'industria, anche nel 3Q2022, rimane al terzo posto nella speciale classifica dei settori maggiormente colpiti con ben 55 casi registrati. A partire da gennaio si può notare un andamento altalenante dei fenomeni di sicurezza informatica; nei primi quattro mesi del 2022 assistiamo ad un trend in aumento del numero di attacchi, incidenti e violazioni privacy, tale trend decresce vistosamente nei mesi di maggio e giugno per poi aumentare nuovamente in maniera costante dal mese di luglio fino a settembre.
Nel 3Q2022 si assiste ad una diminuzione del numero di attacchi, incidenti e violazioni privacy rispetto ai due quarti precedenti, tale diminuzione è pari al 40% rispetto al primo quarto e pari al 37% rispetto al secondo quarto. Nonostante i fenomeni siano diminuiti, nel mese di settembre assistiamo ad un aumento del numero di attacchi, incidenti e violazioni privacy pari a 31, il 21% in più rispetto ai casi verificatosi nel mese precedente di agosto. Inoltre, il mese di settembre risulta essere, insieme al mese di febbraio, il terzo mese peggiore dopo aprile e marzo in termini di casi di sicurezza informatica.
Questa tendenza dovrebbe far riflettere e allarmare chi lavora in questo settore dal momento che gli attacchi rivolti verso il settore industriale possono essere particolarmente rilevanti ed avere impatti devastanti soprattutto se si considerano i settori energetico e manufatturiero.

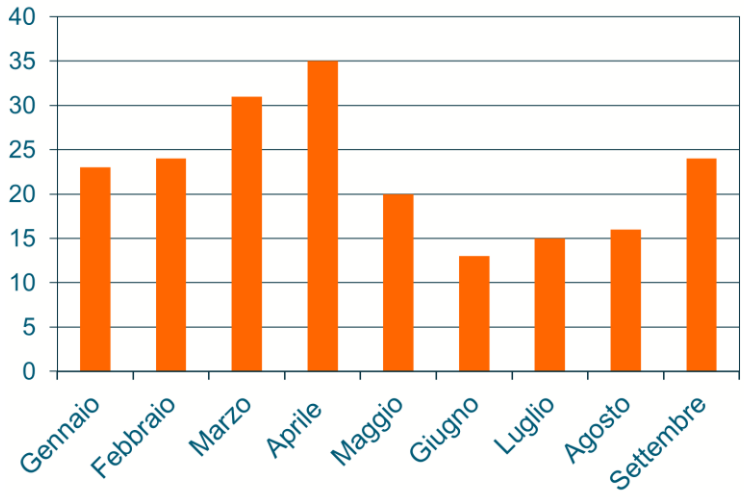

Figura 12 - Attacchi, incidenti e violazioni privacy del settore industria in Italia

Pubblica Amministrazione

Nei primi nove mesi dell'anno in Italia sono stati riscontrati ben 204 fenomeni che hanno interessato il settore della Pubblica Amministrazione. In particolare, nei primi tre mesi se ne sono verificati ben 109, mentre nei successivi quarti rispettivamente 47 nel secondo e 48 nel terzo. Il mese in cui si concentra il maggior numero di eventi è marzo, con ben 53 episodi. Salta subito all'occhio quindi un significativo ribasso dei fenomeni di circa il 57% per entrambi i quarti successivi al 1Q2022 che nell'insieme registrano una totalità di 95 rilevazioni.

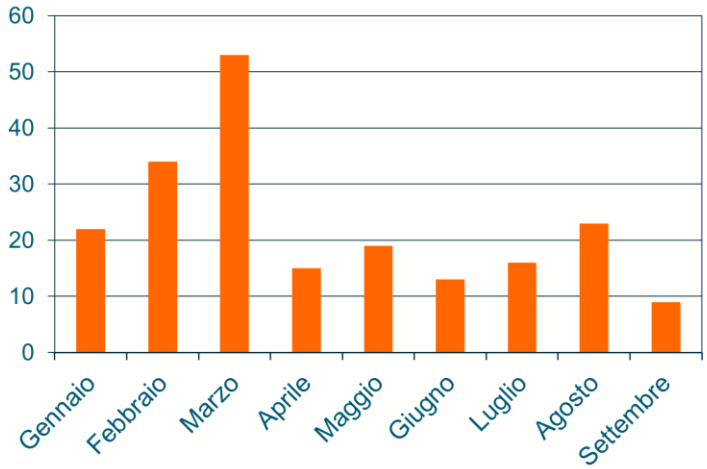

Figura 13 - Attacchi, incidenti e violazioni privacy del settore PA in Italia

Tipo di danno

Le tipologie di attacco perpetrate da criminali informatici nel corso del 3Q2022 proseguono il filone dei mesi precedenti. Si registra infatti nuovamente al primo posto il furto di dati, salito ora ad una preoccupante percentuale del 80% circa sugli attacchi totali. Il furto di dati consiste nell'archiviazione o il trasferimento illegale di informazioni personali, finanziarie o proprietarie. Ciò può includere password, codici software, algoritmi e processi. Il furto di dati può avere gravi conseguenze per le persone coinvolte e le organizzazioni interessate. Ex aequo al secondo posto ove spiccano service interruption (32) e furto di denaro (32) e al terzo posto privacy (29).

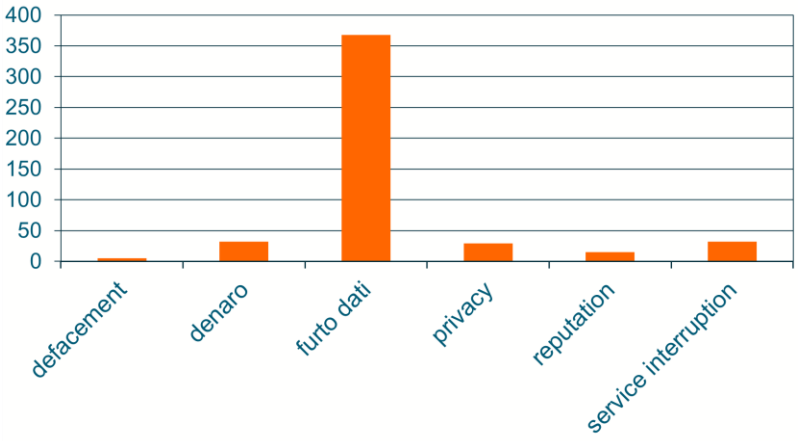

Figura 14 - Tipologia danno di attacchi, incidenti e violazioni privacy nel 3Q2022 in Italia

Come si evince dal grafico nella figura seguente, risulta ben visibile un'imponente crescita relativa al numero dei casi a cavallo tra i due anni (2021 e 2022). Il 2022 prosegue così come si è aperto, ovvero mostrando uno scenario allarmante: il numero dei casi è ampiamente raddoppiato rispetto all'anno precedente a parità di trimestre. La tipologia di attacco si è spostata sempre più verso una combinazione di service interruption e furto di dati, ai quali si aggiunge il furto di denaro, che risulta veicolato attraverso e-mail, solo apparentemente proveniente da istituti finanziari o da siti web che richiedono l'accesso previa registrazione.

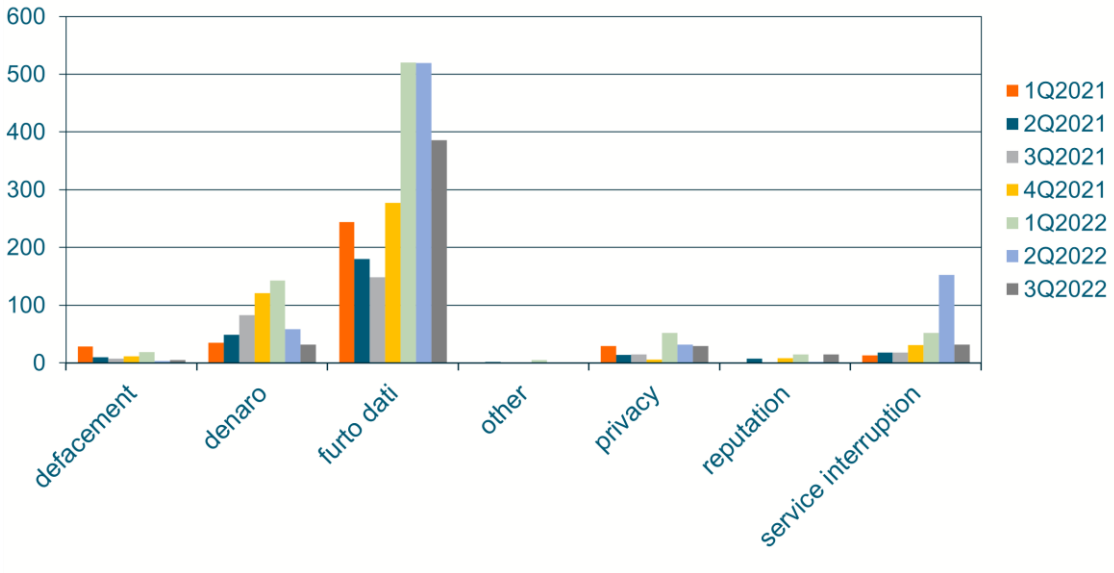

Figura 15 - Tipologia danno di attacchi, incidenti e violazioni privacy nel 1Q2021, 2Q2021, 3Q2021, 4Q2021, 1Q2022, 2Q2022 e 3Q2022 in Italia

Tecniche di attacco

Di seguito è riportato il grafico delle diverse tipologie di attacchi analizzate nel 3Q2022, in riferimento al quarto precedente (2Q2022) è possibile notare un effettivo decremento per quel che riguarda le categorie di attacco DDoS, Malware e Phishing/Social Engineering. Nello specifico sono due le tecniche di attacco maggiormente riscontrate, in ordine: Phishing/Social Engineering (248 casi) e Malware (172 casi), seguiti dagli attacchi Brute Force (25) e Known Vulnerabilities (32) con cui vanno a rappresentare circa il 99% della totalità. Restano invece in numero più contenuto gli attacchi di tipo 0-Day (1), Account Cracking (2) e quelli di DDoS(1). Il primo in classifica, il Phishing/Social Engineering, rappresenta il 59% del numero totale di fenomeni. Questa presenza costante evidenzia che un attacco di phishing può avere sul business delle organizzazioni pubbliche o private molteplici impatti economici.

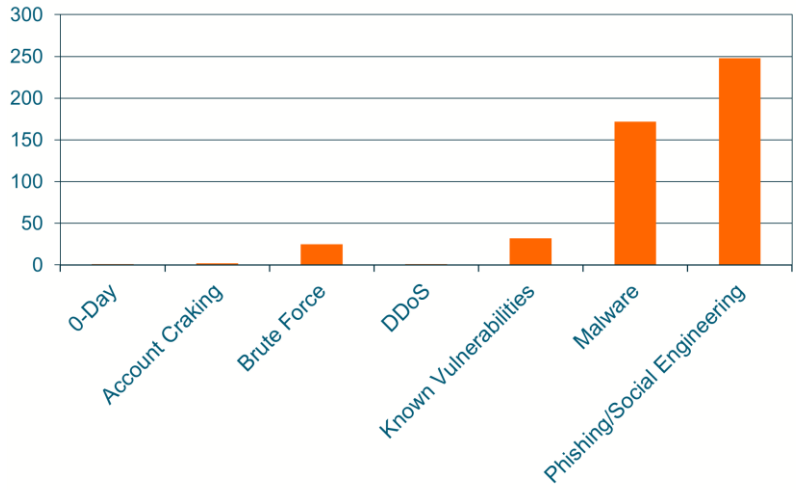

Figura 16 - Tecniche di attacco relative ad attacchi, incidenti e violazioni privacy nel 3Q2022 in Italia

Nel 3Q2022 osserviamo una riduzione generale di numerose tecniche d'attacco.
Colpiscono in particolare i dati relativi agli attacchi DDOS (passati da 112 casi del 2Q2022 ad un solo caso registrato nel 3Q2022) e agli attacchi veicolati tramite Malware, in diminuzione del 45% circa.
Si conferma, inoltre, il trend in discesa degli attacchi commessi tramite Phishing o Social Engineering: dai 389 casi del 1Q2022, passando per i 303 del 2Q2022, si rilevano nel terzo quarto dell'anno 248 casi.
In aumento la tipologia "Brute Force" che, con 25 casi, fa registrare il suo valore più alto dal 2021 ad oggi.
L'utilizzo di vulnerabilità note (32 casi) torna a salire, dopo un calo registrato nel secondo quarto del 2022.
Rimangono pressoché stabili le tecniche "0-Day" e "Account Cracking", che continuano a far registrare casi a singola cifra: un caso relativo a "0-Day" e due relativi al cracking di account.

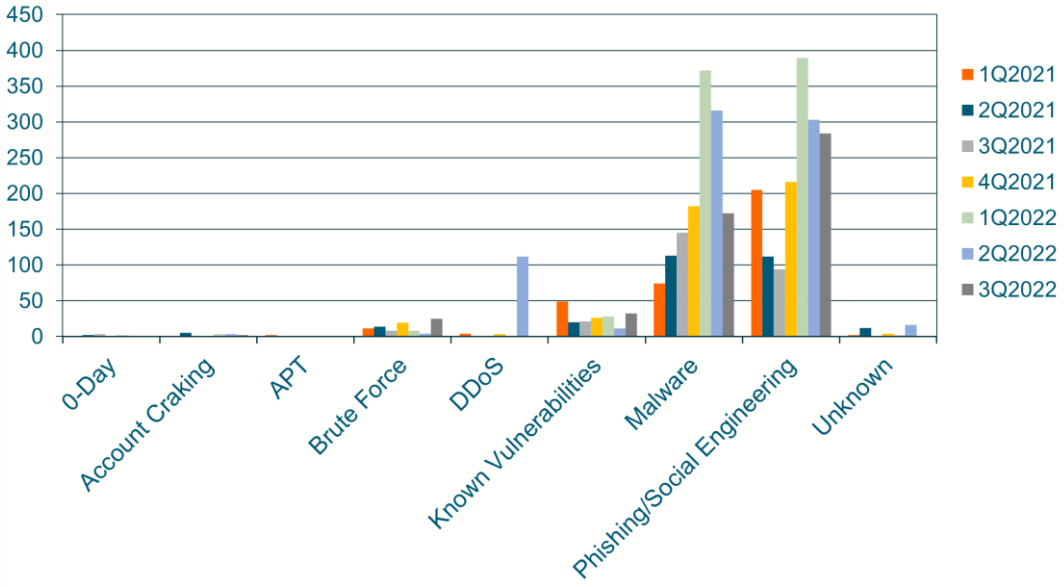

Figura 17 - Tecniche di attacco relative ad attacchi, incidenti e violazioni privacy 1Q2021, 2Q2021, 3Q2021, 4Q2021, 1Q2022 e 2Q2022 in Italia

Nome e tipo di malware

Analizzando il grafico sottostante, si può notare in seguito a una dettagliata analisi eseguita, la presenza di quattro classi di malware ovvero, banking trojan, botnet, ransomware e Trojan. Tuttavia, ciò che desta preoccupazione sono in particolar modo i Trojan, i quali possono trasformare i sistemi informatici in veri e propri zombie con lo scopo di inserire il dispositivo all'interno di una botnet (un sistema utilizzato dai malintenzionati per sferrare attacchi informatici in tutto il mondo). Secondo una classificazione di malware, uno dei Trojan che nell'ultimo periodo ha eseguito attività illecite arrecando danni di reputazione e di compliance è Trickbot, un trojan di livello avanzato che si diffonde principalmente da campagne di spear phishing utilizzando e-mail personalizzate, le quali contengono allegati o collegamenti dannosi, e nel momento in cui sono aperti eseguono codice dannoso. Inoltre, in ambito bancario, notiamo la presenza di un banking trojan chiamato Tinba o TBT che infetta i dispositivi degli utenti finali e tenta di compromettere i loro conti finanziari e di estirpare i fondi presenti. Da non sottovalutare anche i Ransomware che ultimamente stanno provocando gravi danni di reputazione ed economici a livello globale, criptando i dati di varie istituzioni e aziende e successivamente chiedendo un'ingente somma di riscatto che determina una grave disservizio aziendale. Nel 3Q2022 i trojan rappresentano circa il 38% della totalità dei malware, seguiti da banking trojan (16%), botnet (15%) e ransomware (14%).

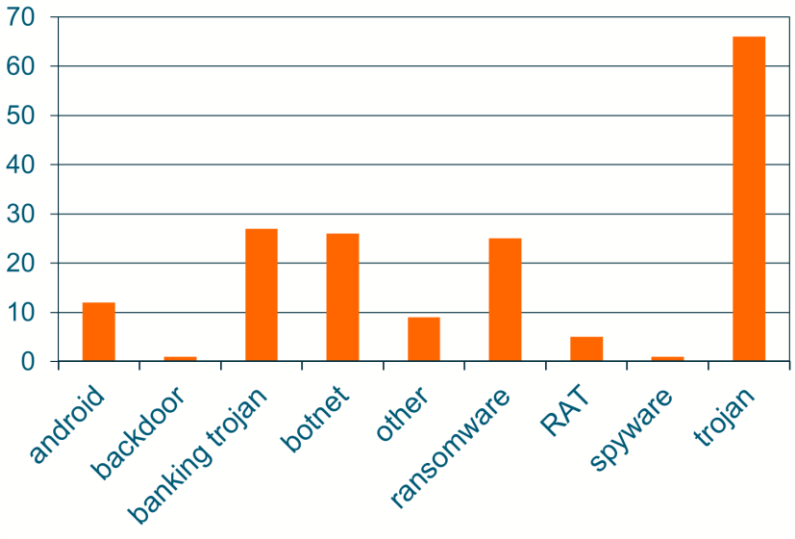

Figura 18 - Tipologie di malware relative ad attacchi e incidenti registrate nel 3Q2022 in Italia

Nel grafico è possibile notare le varie tipologie di malware che hanno causato attacchi ed incidenti nell'intero anno 2021 e nei primi tre quarti del 2022. Nell'intero 2021 sono stati rilevati ben 591 malware responsabili, invece nei soli primi tre quarti del 2022, ovvero i primi nove mesi, se ne sono riscontrati già 861, andando così ad evidenziare un aumento del 46% di attacchi ed incidenti, che si concentrano maggiormente nei primi sei mesi dell'anno. Nello specifico si può notare come i trojan e i banking trojan siano le tipologie di malware più riscontrate in tutti i quarti esaminati, è necessario anche sottolineare come i casi di botnet siano aumentati vertiginosamente nel 2022, specialmente nella prima metà dell'anno, passando da 18 casi in tutto il 2021 ai 197 del 2022.

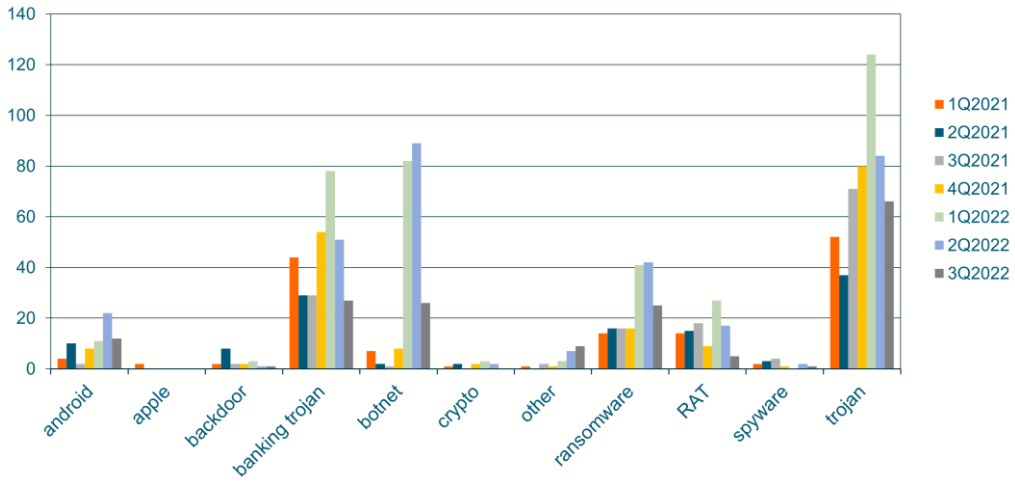

Figura 19 - Tipologie di malware relative attacchi e incidenti registrate 1Q2021, 2Q2021, 3Q2021, 4Q2021, 1Q2022, 2Q2022 e 3Q2022 in Italia

Ransomware

Durante questo penultimo quarto del 2022, è stato identificato un andamento pressoché lineare degli attacchi e incidenti subiti sul territorio italiano. Il mese in cui il numero di casi è stato maggiormente significativo è il mese di marzo in cui sono stati registrati 20 casi. Durante i mesi estivi è ben visibile una lieve decrescita delle segnalazioni di sicurezza in relazione ai periodi in cui la maggior parte delle aziende limitano la propria operatività.

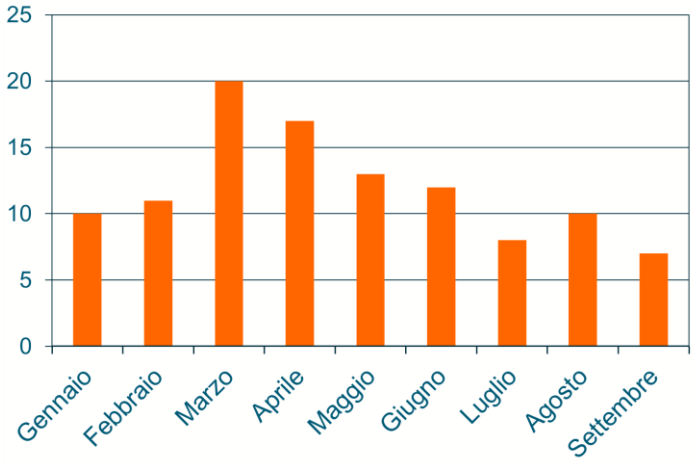

Figura 20 - Ransomware relativi ad attacchi e incidenti registrati in Italia

Trojan

Come precedentemente descritto l'andamento delle minacce ransomware, anche per attacchi di tipo trojan, si è registrato un andamento analogo con una diminuzione dei casi durante i mesi estivi ed un picco segnalato durante il mese di marzo con 65 casi.
Questa minaccia durante gli ultimi mesi è diventata sempre più una certezza per i cyber criminali in quanto permette facilmente di raggiungere un primo contatto con i sistemi da compromettere. Questa tecnica di attacco, in seguito, permette ad un attaccante di impiegare tecniche più invasive sfruttando il trojan installato sui dispositivi compromessi.

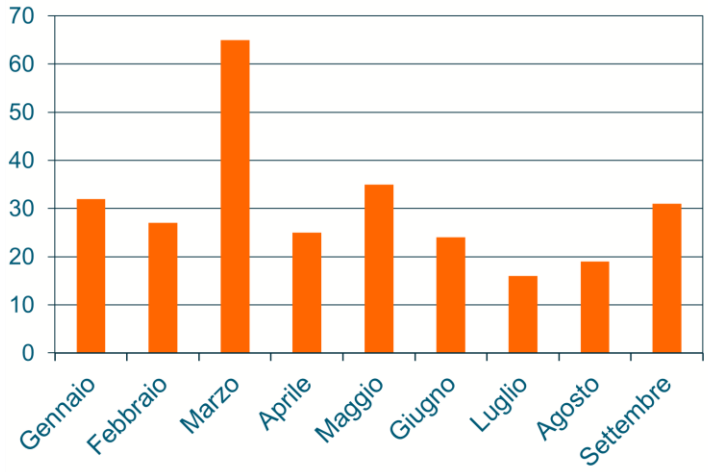

Figura 21 - Trojan relativi ad attacchi e incidenti registrati in Italia

Botnet

In seguito a una dettagliata analisi, possiamo notare un vertiginoso aumento di attacchi relativi a Botnet durante il mese di marzo, maggio e giugno. Per citarne alcune, possiamo fare riferimento alla botnet Mantis, la quale è composta da circa 5.000 bot. Essa si distingue da altre botnet per una serie di motivi fra cui il primo per la sua capacità di eseguire attacchi DDoS HTTPS, che sono di natura costosa a causa delle risorse computazionali necessarie al fine di stabilire una connessione sicura crittografata usando TLS. In secondo luogo, a differenza di altre botnet tradizionali che si basano su dispositivi IoT come DVR e router, Mantis sfrutta macchine virtuali manomesse e potenti server, dotandosi di maggiori risorse. Mantenere sempre aggiornati i software presenti e le patch di sicurezza del sistema operativo proteggerà il sistema dalle infezioni causate da malware e altri attacchi, con lo scopo di eseguire una buona pratica di remediation e adottare politiche di security by detection e security by reaction, al fine di contrastare e mitigare le minacce in maniera celere e proficua.

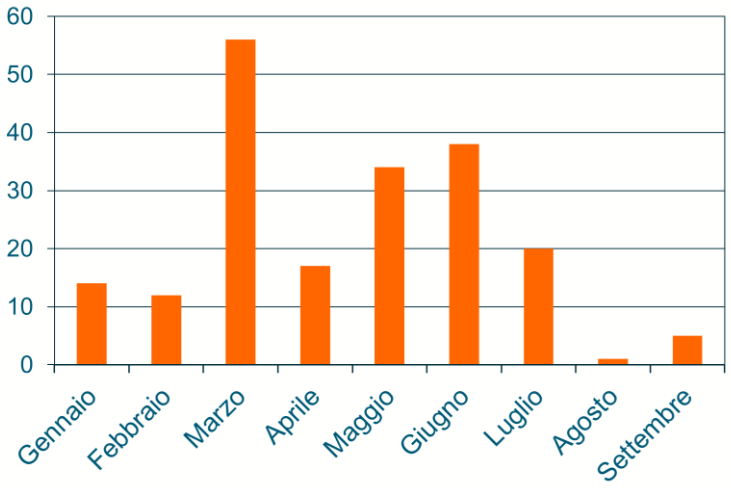

Figura 22 - Botnet relativi ad attacchi registrati in Italia

Sicurezza dei dispositivi IoT 3Q2022

In questa rubrica si discute sull'evoluzione della distribuzione dei dispositivi IoT, con riferimento ai dati del 3Q2022. In prima analisi si può notare come i dispositivi IPv4 connessi in rete siano aumentati di circa il 6%.

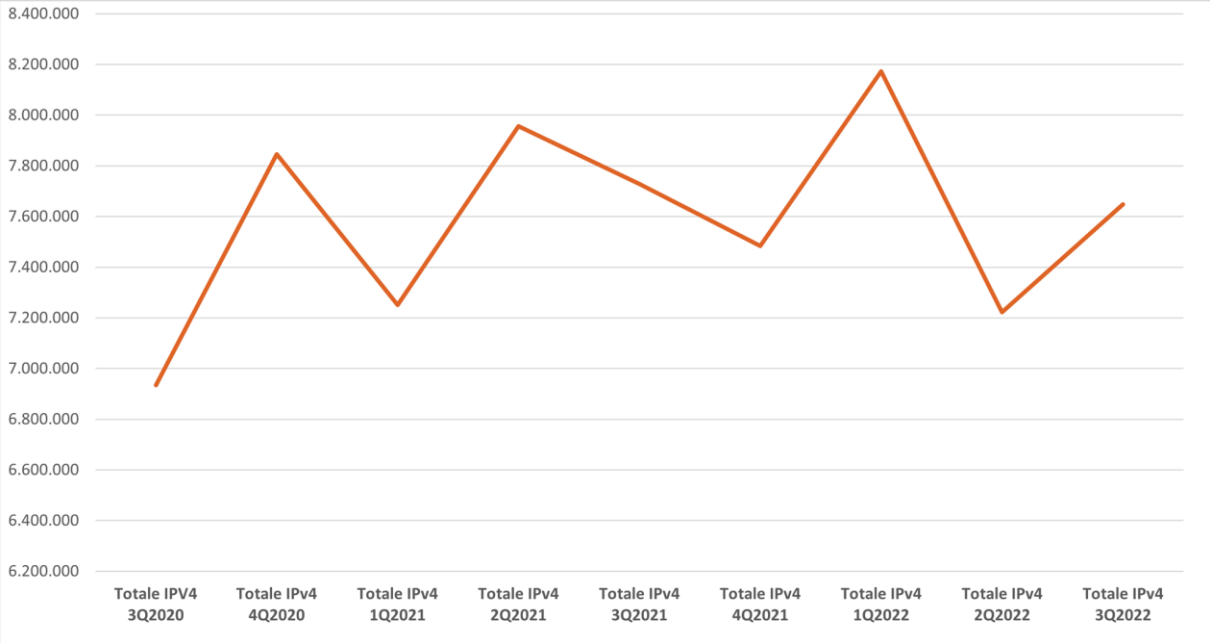

Figura 23 - Situazione italiana dei dispositivi IPv4 3Q2020, IPv4, 4Q2020, IPv4 1Q2021, 2Q2021, 3Q2021,4Q2021 e 1Q2022, 2Q2022 e 3Q2022

In Italia, le industrie con una maggiore presenza di dispositivi IoT sono:

- smart car;
- smart home;
- industrial IoT;
- smart health;
- smart metering;
- smart building.

In questa rubrica è stata mantenuta la distinzione tra dispositivi IT e dispositivi Operational Technology (OT). Nella Figura 24, è mostrato il numero dei dispositivi specifici IoT sottoelencati, rilevati nel 3Q2022. Attualmente sono stati individuati 7.648.395 indirizzi IPv4 di cui 134.083 riferiti a:

- telecamere;
- stampanti;
- firewall;
- router;

- VoIP;
- Dispositivi medicali

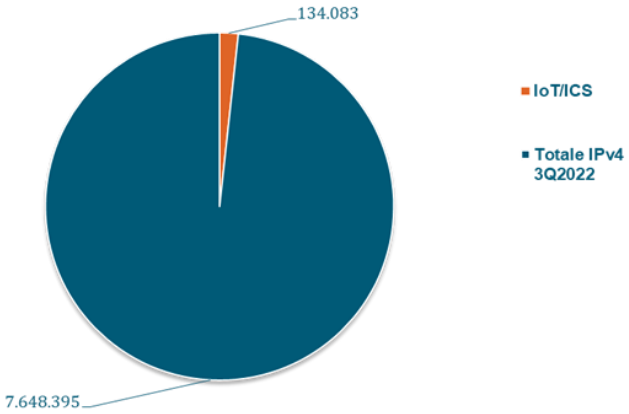

Figura 24 - IoT/ICS vs Others IPv4 3Q2022

Oltre ai dispositivi IoT sono stati individuati 6.388 dispositivi OT. Nel seguente grafico si mostra il numero di dispositivi IT e OT individuati, facenti parte dei 7.648.395.

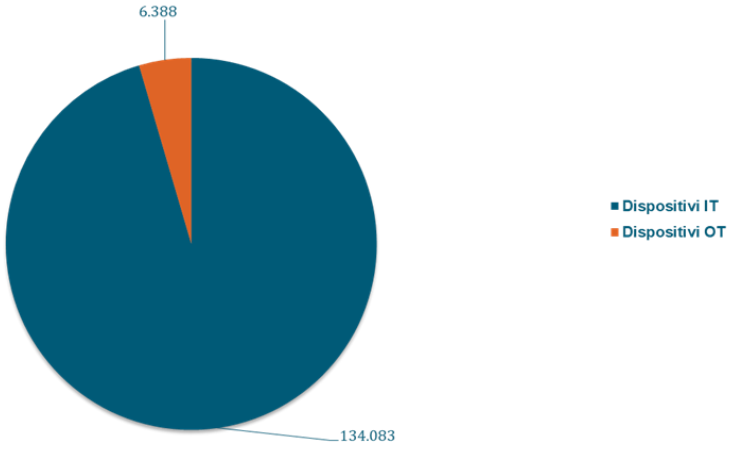

Figura 25 - Dispositivi IoT e OT individuati

Si ricorda che l'esposizione delle informazioni fornite da questi dispositivi potrebbero essere cruciali per la sicurezza del dispositivo stesso e in modo indiretto, per tutta l'infrastruttura IT che li ospita.

L’analisi è focalizzata sulle tecnologie ICS (Industrial Control System) che includono sistema di controllo per la supervisione e acquisizione dati (SCADA), sistemi di controllo distribuiti (DCS), sistemi di automazione industriale e controllo (IACS), controllori logici programmabili (PLC), controllori di automazione programmabili (PAC), unità terminali remote (RTU), server di controllo, dispositivi elettronici intelligenti (IED) e sensori.

Inoltre, l’analisi è stata effettuata anche sui PLC (Programmable Logic Controller), ovvero computer specializzati nella gestione dei processi industriali. Nel 3Q2022 sono stati rilevati 819 dispositivi, in decremento rispetto ai 970 rilevati nel 2Q2022.
Tra i vari PLC analizzati rientrano quei dispositivi riconducibili ai sistemi ICS e che comunicano con protocollo TCP utilizzando la porta 102 (comunicazione con note vulnerabilità).

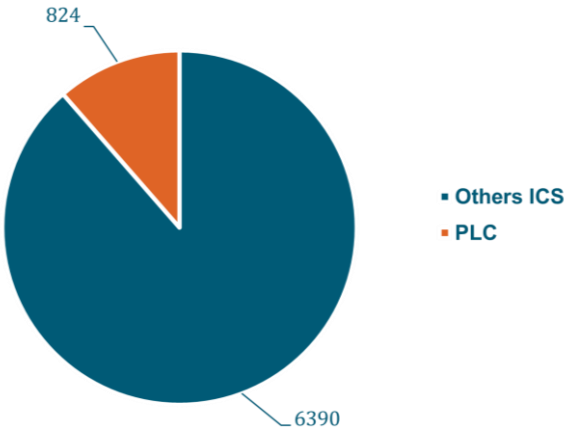

Figura 26 - ICS/PLC individuati 3Q2022

Questo è un dato che continua ad essere allarmante, poiché tali dispositivi risultano essere poco protetti: per molti di essi vengono mostrate informazioni come “riferimenti hardware” e “versione firmware” semplicemente interrogandoli. Esse sono informazioni molto utili nella prima fase di un attacco, ovvero quella della ricognizione, consentendo di ricercare vulnerabilità note o specifici exploit facilmente applicabili.

Con riferimento al grafico sottostante, si nota un incremento dei sistemi industriali rispetto al 2Q2022 di quasi il 13% del numero di dispositivi connessi riconducibili alla categoria OT (insieme dei sistemi utilizzati tipicamente in ambito industriale per il monitoraggio e/o il controllo automatizzato degli impianti).

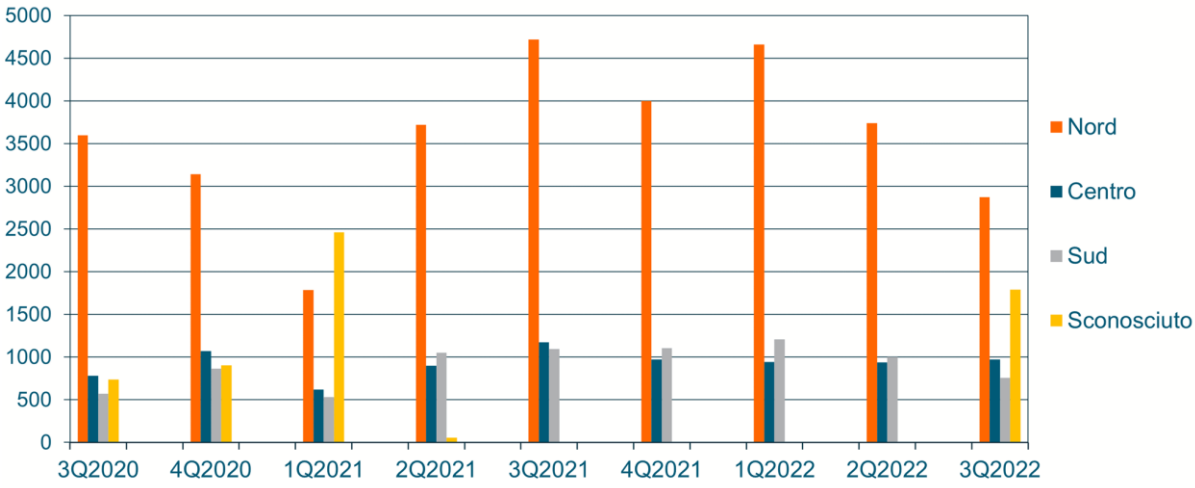

Figura 27 - Sistemi industriali 3Q2020, 4Q2020, 1Q2021, 2Q2021, 3Q2021, 4Q2021, 1Q2022, 2Q2022 e 3Q2022

La distribuzione degli oltre 7 milioni di dispositivi IoT rilevati nel nostro Paese mostra una relazione piuttosto stretta con i livelli di industrializzazione attribuibili alle differenti regioni. La Lombardia si conferma la regione con il più elevato numero di dispositivi IoT connessi, 27.601 i dispositivi individuati, seguita da Lazio (12.992), Campania (8.747) e Veneto (8.372). In fondo a questa particolare classifica la Valle D'Aosta con 70 dispositivi. Sebbene ci sia stato un decremento del numero di dispositivi nelle varie regioni, nel 3Q2022 sono stati rilevati 27.561 dispositivi classificati come sconosciuti. Questo risultato deve essere accolto negativamente poiché si riflette in una diminuzione della difficolta da parte di un attaccante nel riuscire ad accedere ai dispositivi esposti.

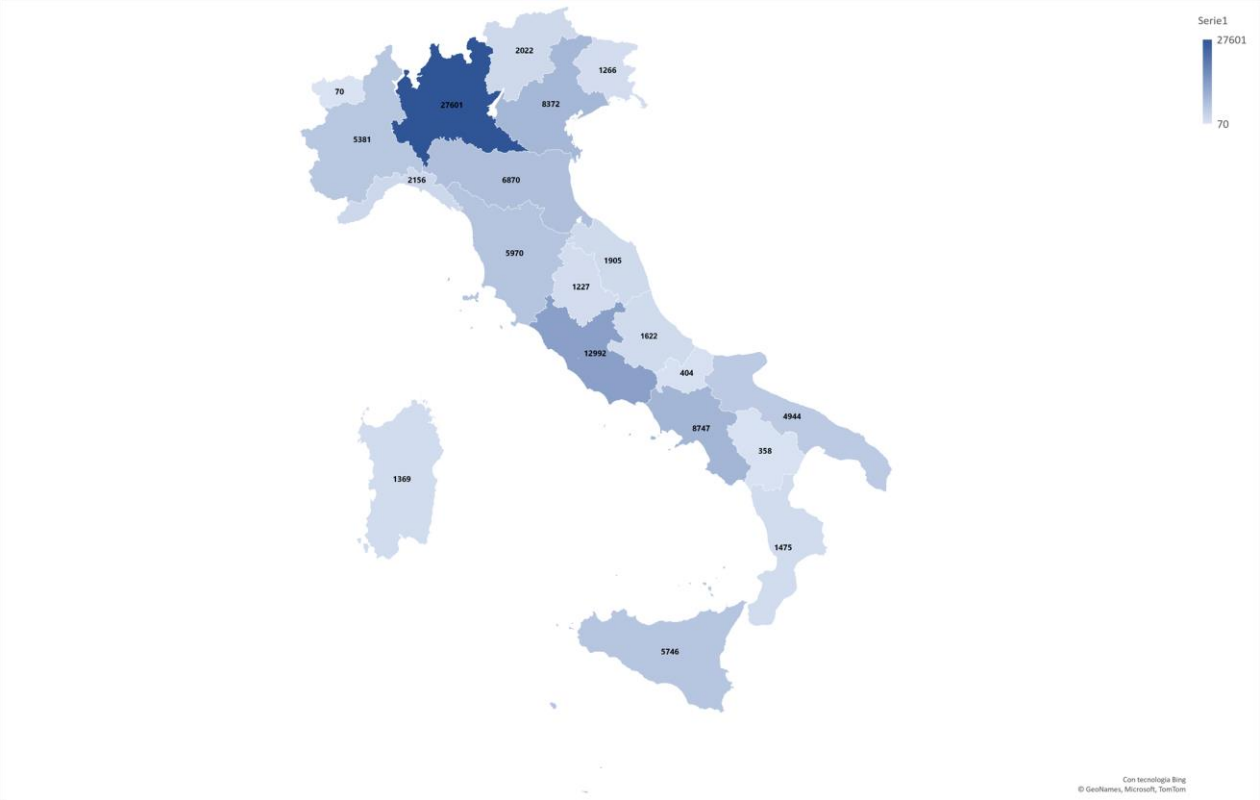

Figura 28 - Distribuzione dei dispositivi IoT nelle regioni italiane 3Q2022

Sono stati analizzati anche i dispositivi che utilizzano protocolli privi di autenticazione. In Italia ne sono stati rilevati 5.828 (un incremento di circa il 4% rispetto ai 5626 rilevati 2Q2022) come si evince in Figura 29.

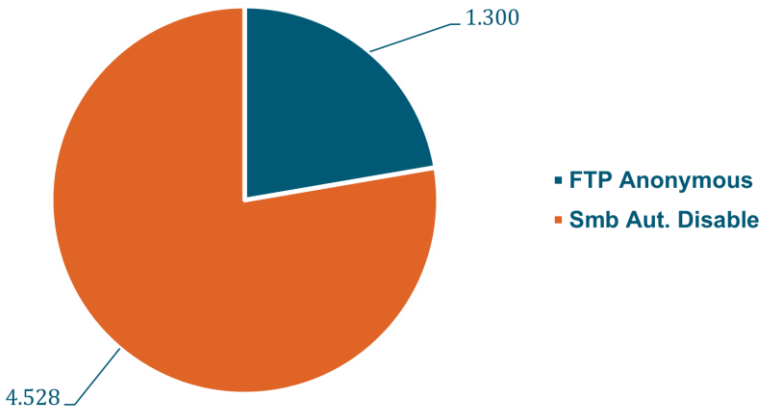

Figura 29 - Protocolli senza autenticazione 3Q2022

È opportuno far osservare che attraverso i dispositivi privi di protocolli di autenticazione è possibile accedere alla rete aziendale e ciò potrebbe essere utilizzata come backdoor indesiderata nella propria rete o comportare una perdita di dati sensibili che esporrebbe l'azienda al pagamento di sanzioni previste dal GDPR, oltre che provocare importanti danni di immagine.

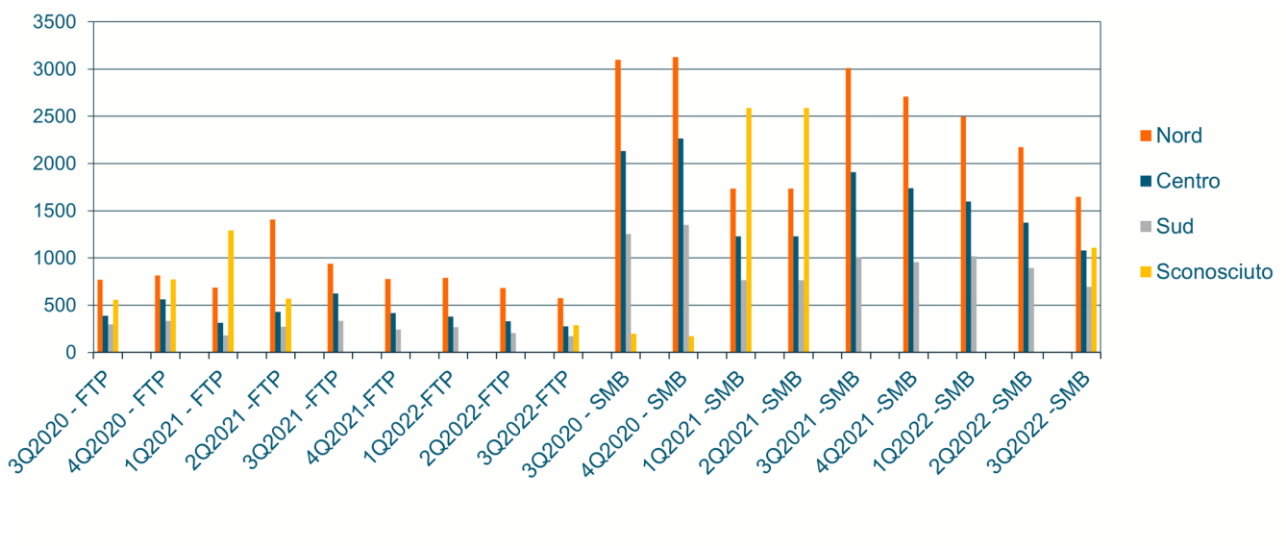

Figura 30 - Distribuzione protocolli senza autenticazione in Italia per area geografica 3Q2020, 4Q2020, 1Q2021, 2Q2021, 3Q2021, 4Q2021, 1Q2022, 2Q2022 e 3Q2022

Quanto ai grafici relativi alla distribuzione dei dispositivi IoT, si nota che tutti i numeri sono in aumento. Dai dati analizzati, infatti, risulta un incremento di 4733 telecamere, 76 stampanti, 3464 router e 26 VoIP ed un decremento di 596 firewall per un totale di 9.809 dispositivi in più. Secondo l'Osservatorio CyberSecurity di Exprivia, questo incremento dei dispositivi esposti rispetto al 2Q2022, è un fatto negativo in quanto aumenta la superfice di attacco. Per quanto riguarda la distribuzione delle telecamere individuate, il primato resta al Nord Italia.
Nel 3Q2022 sono riportate le analisi effettuate sui sistemi VoIP, iniziate nell'ultimo quarter del 2021. È possibile osservare un'inversione di tendenza rispetto al 2Q2022 che aveva registrato un decremento dei sistemi, rilevando attualmente 467 dispositivi rispetto ai precedenti 437. Tale incremento è dovuto principalmente ad un aumento del numero di dispositivi classificati come sconosciuti. Si nota, inoltre, come la presenza di questi dispositivi è particolarmente significativa al centro Italia rispetto al nord e sud Italia nonostante le oscillazioni osservate nei quarter analizzati.

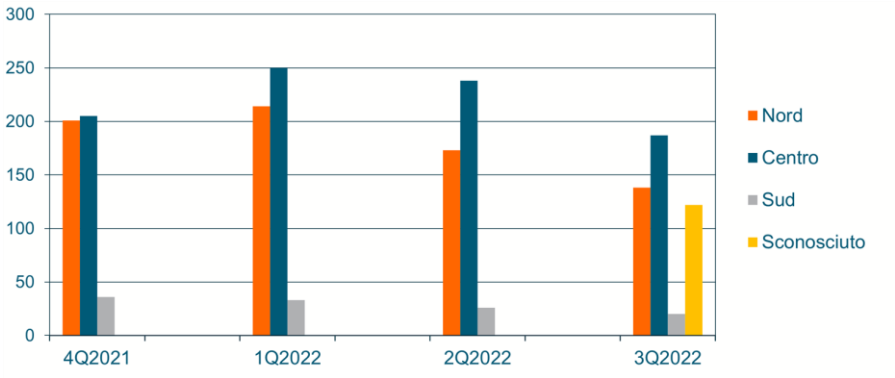

Figura 31 - Distribuzione dispositivi VoIP in Italia per area geografica 4Q2021, 1Q2022, 2Q2022 e 3Q2022

La distribuzione delle telecamere mantiene sempre il primato nel nord Italia con un incremento rispetto al 2Q2022, dovuto alla considerevole presenza di dispositivi classificati come sconosciuti.

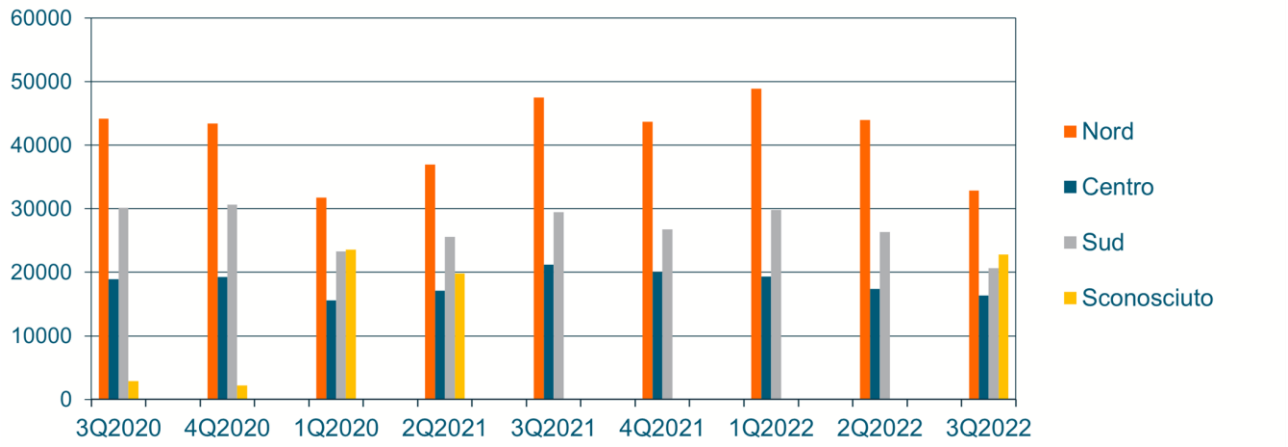

Figura 32 - Distribuzione telecamere in Italia per area geografica 3Q2020, 4Q2020, 1Q2021, 2Q2021, 3Q2021, 4Q2021 e 1Q2022, 2Q2022 e 3Q2022

La distribuzione delle stampanti mantiene sempre il primato nel nord Italia con un decremento da 277 a 218 rispetto al 2Q2022. Anche nelle aeree del centro e sud Italia il numero di stampanti rilevate diminuisce. Tuttavia, nel 3Q2022 sono state rilevate 199 stampanti non classificabili in alcuna area geografica e, che di conseguenza portano ad un aumento del numero totale dei dispositivi.

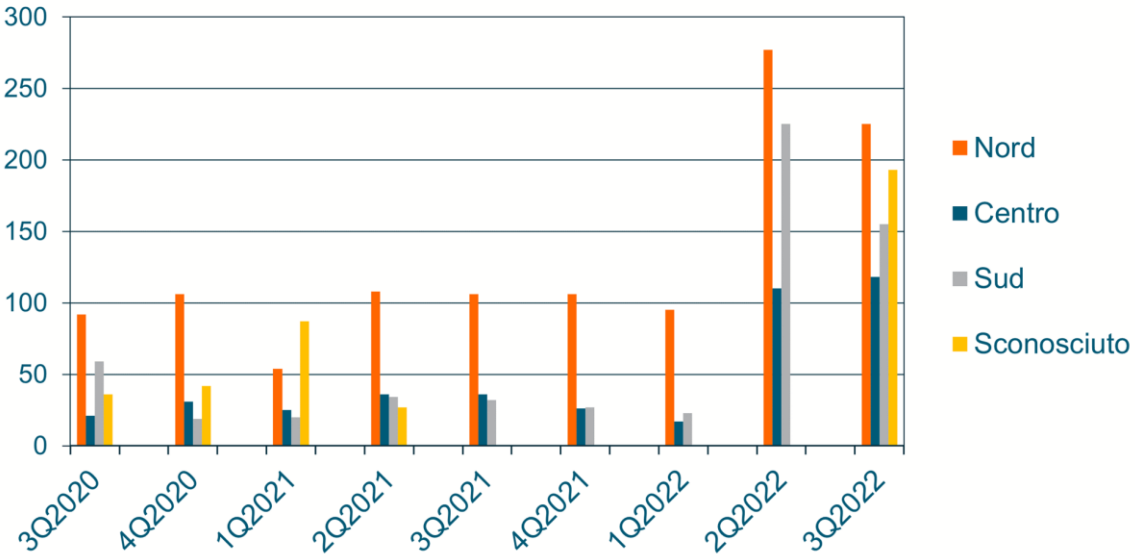

Figura 33 - Distribuzione stampanti in Italia per area geografica 3Q2020, 4Q2020, 1Q2021, 2Q2021, 3Q2021, 4Q2021 e 1Q2022, 2Q2022 e 3Q2022

Per quanto riguarda i firewall si può notare che, nonostante l'incremento del numero di dispositivi sconosciuti, è evidente un decremento dei dispositivi totali, in particolare nel nord Italia.

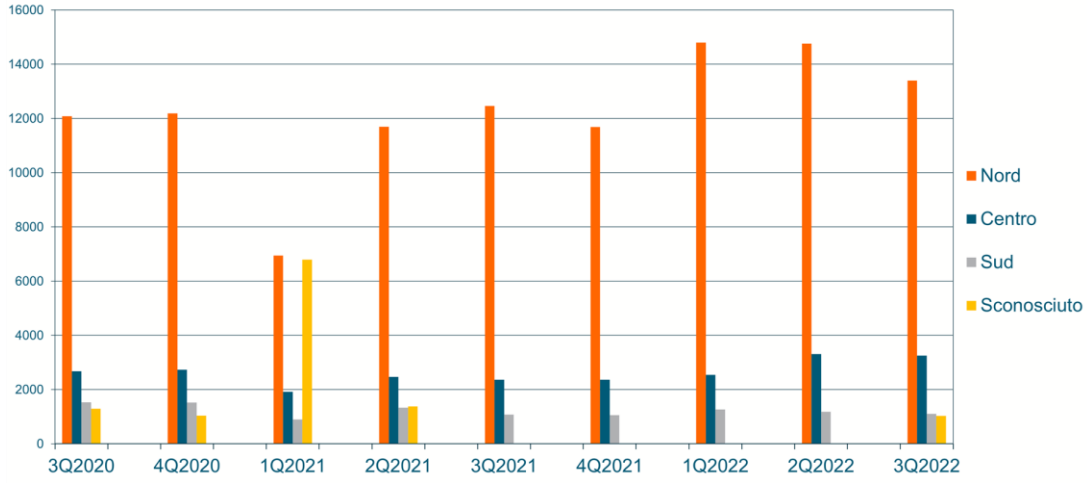

Figura 34 - Distribuzione firewall in Italia per area geografica 3Q2020, 4Q2020, 1Q2021, 2Q2021, 3Q2021, 4Q2021 e 1Q2022, 2Q2022 e 3Q2022

Per i router, si evidenzia un aumento dei dispositivi individuati per quanto riguarda nord (da 5.689 a 6.394) e centro (da 2.028 a 2.076) e un decremento dei dispositivi per quanto riguarda sud (da 2.146 a 1.951) rispetto al 2Q2022. Inoltre, si registrano 2.942 dispositivi non classificabili in alcuna area geografica.

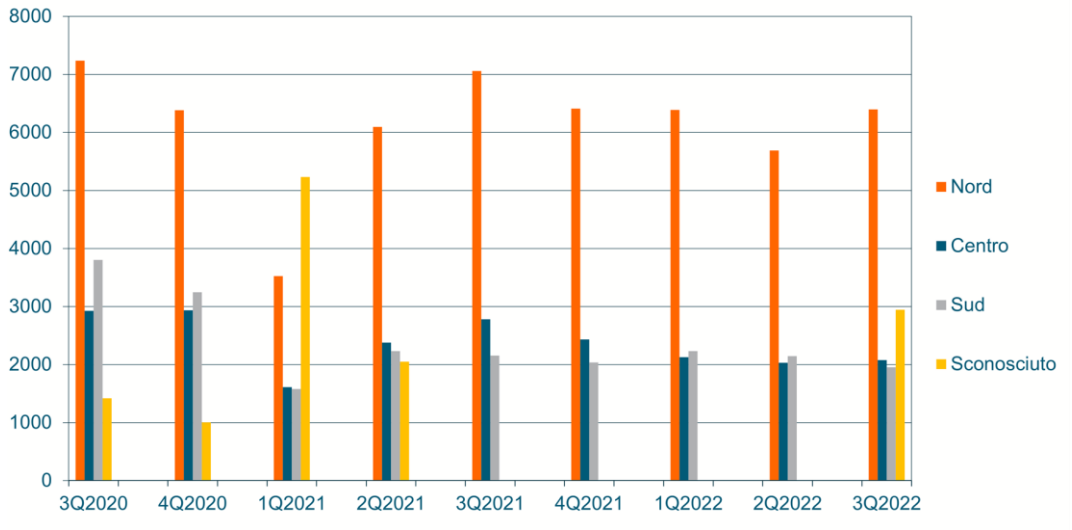

Figura 35 - Distribuzione router in Italia per area geografica 3Q2020, 4Q2020, 1Q2021, 2Q2021, 3Q2021, 4Q2021 e 1Q2022, 2Q2022 e 3Q2022

Nel 3Q2022, vengono aggiunti all'analisi i dispositivi medicali di cui vengono riportati in Figura 36 i risultati ottenuti nel 3Q2022. Come si può notare dal grafico, è stata rilevata una maggior presenza di tali dispositivi a sud, seguita da nord e centro. Inoltre, è presente un numero significativo di dispositivi classificati come sconosciuti (500).

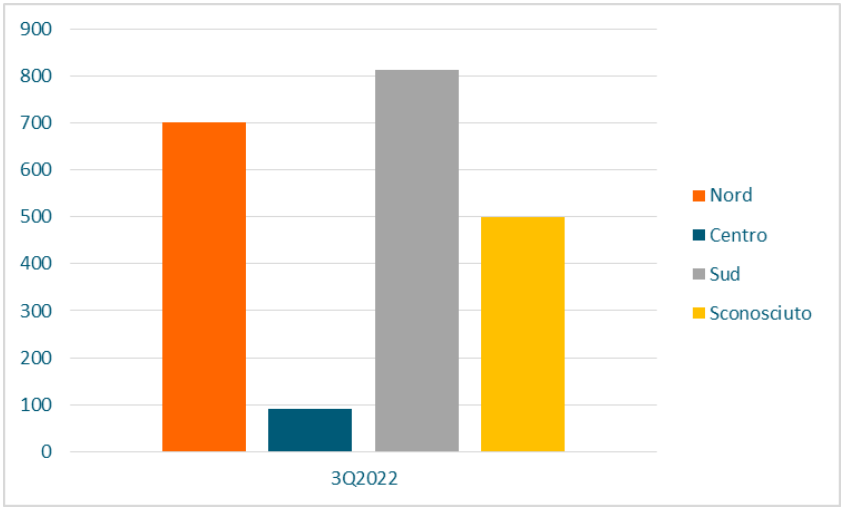

Figura 36 - Distribuzione dispositivi medicali in Italia per area geografica 3Q2022

Stato della sicurezza dei dispositivi IoT 3Q2022

In questa rubrica si illustra l'evoluzione del livello di sicurezza dei dispositivi IoT osservati nel 3Q2022. Per valutare questo livello di sicurezza abbiamo introdotto un nuovo indice di valutazione detto Unsecurity IoT Index (UII). Il valore calcolato mette in relazione il numero di dispositivi IoT vulnerabili con il numero di protocolli privi di autenticazione. In tabella 1 sono riportati i valori di tale indice ottenuti per il 3Q2022:

	3Q2022
N°Protocolli Vulnerabili	5.828
N° Protocolli Totali	148.070
N° dispositivi IoT vulnerabili	28.121
N° dispositivi IoT totali	102.920
Unsecurity_IoT_Index	0,01075

Tabella 1 - Unsecurity IoT Index Totale

Il valore ottenuto è riportato graficamente in Figura 37:

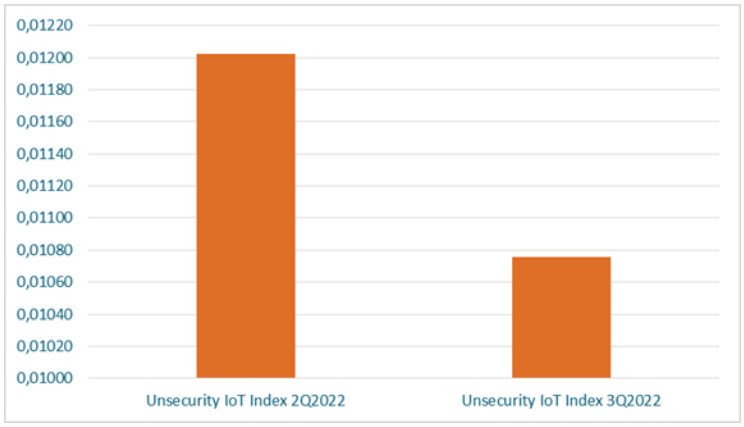

Figura 37 - Unsecurity IoT Index nel 3Q2022

Come si può osservare dalla figura 37 il valore dell'UII nel 3Q2022 è notevolmente inferiore. Ciò è dovuto principalmente ad un abbassamento notevole del tasso di vulnerabilità dei dispositivi IoT che passa dal 31% nel 2Q2022 al 9% nel 3Q2022.

È stato ritenuto opportuno mostrare l'incidenza dell'Unsecurity IoT Index nelle tre aree geografiche del nostro Paese, al fine di evidenziare l'area che presenta il maggiore rischio dovuto alla rilevazione di questi dispositivi.

È stato ritenuto opportuno mostrare l'incidenza dell'Unsecurity IoT Index nelle tre aree geografiche del nostro Paese, al fine di evidenziare l'area che presenta il maggiore rischio dovuto alla rilevazione di questi dispositivi.

I valori di questo indice per il 3Q2022 sono riportati in tabella 2:

	Nord	Centro	Sud	Sconosciuto	Totale
N°Protocolli Senza Autenticazione	2222	1352	869	1397	5.828
N° Protocolli totali	65.462	29.561	19.039	34.008	148.070
N° dispositivi IoT vulnerabili	9.131	4.529	6.726	7.179	28.121
N° dispositivi IoT totali	37192	17.843	22.522	25.568	102.920
Unsecurity_IoT_Index	0,00833	0,01161	0,01363	0,01153	0,01075

Tabella 2 - Unsecurity IoT Index per Area Geografica

I valori riportati in tabella 2 sono mostrati graficamente in Figura 38:

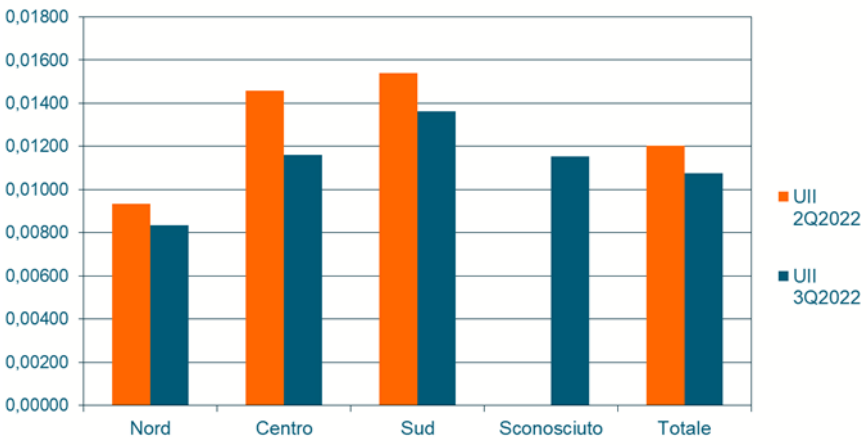

Figura 38 - Unsecurity IoT Index per Area Geografica

L'indice calcolato ci consente di stabilire il livello di rischio cyber per area geografica. Il valore calcolato per l'Unsecurity IoT Index delle varie aree geografiche, rapportato a quello totale, deve essere considerato come valore pesato in base sia al numero dei dispositivi osservati e protocolli totali utilizzati, sia all'insieme dei sistemi che presentano vulnerabilità di protocollo e di autenticazione.

Se il valore dell'indice per area geografica è inferiore al valore dell'indice totale italiano il rischio è minimo, come accade per il valore ottenuto per il Nord Italia. Al contrario, se tale valore supera l'indice totale, il rischio di esposizione ad attacchi cyber per i dispositivi IoT in questa area geografica è alto.
Questo si può osservare per le altre due aree dove si è registrato un aumento di circa l'8% per il Centro e di oltre il 26% per il Sud, rispetto al totale.
È evidente come il decremento del valore dell'UII nazionale si riflette anche sulle varie aree geografiche italiane.
A questo punto dello studio sono stati valutati quali dispositivi analizzati presentavano il maggior rischio procedendo con il calcolo dell'UII per ogni dispositivo IoT considerato. Rispetto al 2Q2022 sono stati aggiunti all'analisi anche i dispositivi medicali. I risultati ottenuti sono di seguito riportati in tabella:

	Stampanti	Telecamere	VoIP	ICS	PLC	Dispositivi medicali	Totale
3Q2022	0,01882	0,01159	0,00077	0,00076	0,01201	0,00340	0,01075

Tabella 3 - Unsecurity IoT Index per Dispositivo

I valori riportati in tabella sono mostrati graficamente in Figura 39:

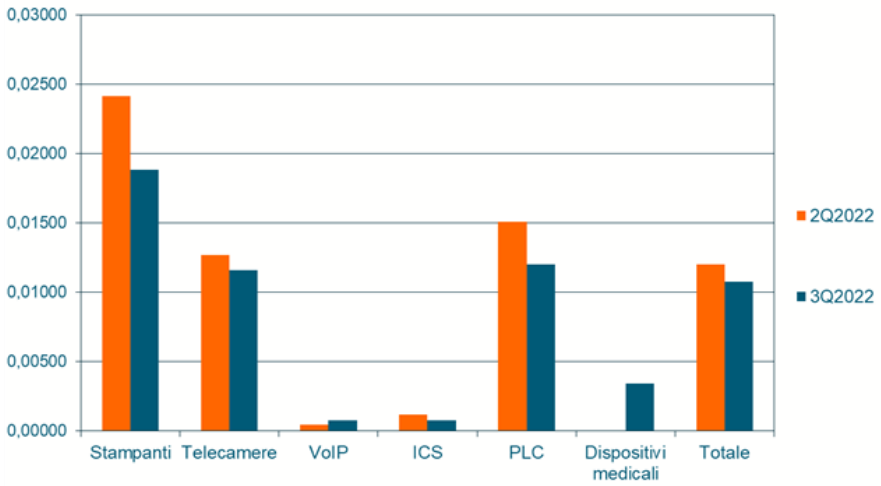

Figura 39 - Unsecurity IoT Index per Dispositivo

Dall'analisi si evince che i dispositivi a maggior rischio sono le stampanti. Questo è evidente se si considera che 329 stampanti su un totale di 688 sono vulnerabili (circa il 48%). Inoltre, come si può vedere, il valore dell'indice delle stampanti è superiore di circa il 75% rispetto al totale.
Anche i PLC hanno un alto livello di rischio in quanto superano di circa il 12% il valore totale. Infatti, sul totale dei dispositivi PLC circa il 30% è vulnerabile.
Per quanto riguarda i dispositivi medicali, si ha che solo l'8,6% dei dispositivi è vulnerabile, pertanto questi presentano un basso rischio.
Una considerazione analoga può essere fatta per i dispositivi ICS e per i VoIP System che presentano il minor rischio possibile poiché solo il 2% dei dispositivi risulta essere vulnerabile.

Le telecamere, infine, hanno un indice di insicurezza quasi pari al valore totale calcolato ed i due grafici sono quasi coincidenti; è possibile, quindi, asserire che tali dispositivi hanno un rischio medio. Infatti, su 92.456 telecamere totali, 27.227 sono risultate vulnerabili pari ad una percentuale di vulnerabilità di circa il 29%.

Oltre all'analisi dei grafici ricavati dal calcolo dell'indice UII, viene introdotto un nuovo valore adimensionale detto IoT Vulnerability Entropy Index (IVEI), dato dal rapporto tra il numero di vulnerabilità dei dispositivi IoT ed il numero totale delle vulnerabilità. I risultati ottenuti sono riportati in tabella 4:

Data	IoT_Vulnerability_Entropy_Index (IVEI)
01/09/2020	0,00096
01/12/2020	0,02032
01/03/2021	0,00045
01/06/2021	0,01898
01/09/2021	0,00108
01/12/2021	0,00173
01/03/2022	0,00050
01/06/2022	0,00042
01/09/2022	0,00084

Tabella 4 - IoT Vulnerability Entropy Index

I risultati ottenuti vengono mostrati graficamente in Figura 40:

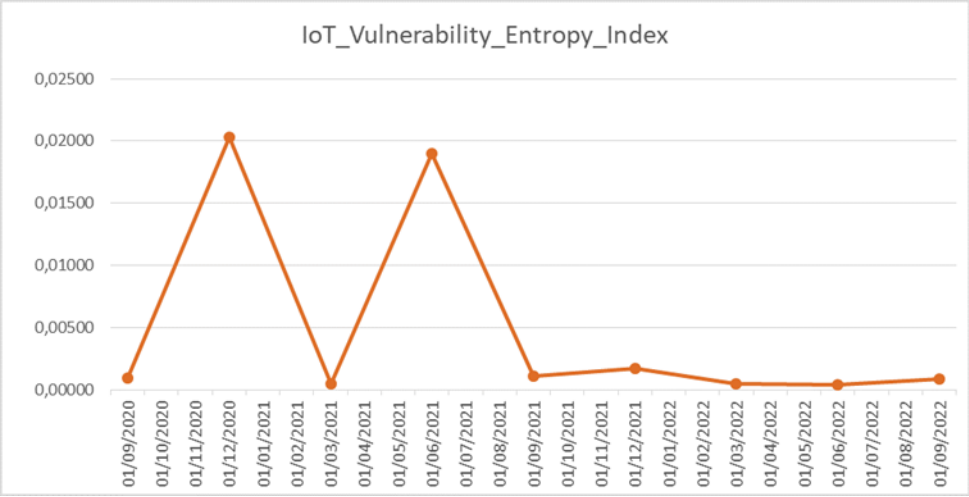

Figura 40 - IoT Vulnerability Entropy Index

Dall'analisi delle vulnerabilità correlate a tali dispositivi sono emerse delle criticità che hanno fatto registrare un picco dell'indice nei periodi compresi tra settembre e dicembre 2020 e tra marzo e giugno 2021, dovuti principalmente alla scoperta di vulnerabilità di uno specifico componente hardware utilizzato su numerosi dispositivi IoT.
Si è potuto osservare che delle 1064 vulnerabilità IoT rilevate nel periodo preso in esame, 901 erano dovute a potenziali rischi nell'utilizzo di tali componenti in ambito mobile su dispositivi quali smartphone, tablet e smartbook, con un'incidenza di circa l'85%. A partire da giugno 2021 il numero di vulnerabilità correlate a tali componenti è tendenzialmente diminuito, pertanto, da questa data in poi, è stato possibile notare come l'IVEI tenda a diminuire fino a raggiungere un andamento quasi costante a partire da settembre 2021.

Nel settore IoT resta comunque costante la minaccia di nuove vulnerabilità rilevate, così come è stato osservato nel 2Q2022 e nel 3Q2022. Di seguito sono riportate le CVE che hanno presentato la maggiore criticità o causato un significativo impatto sulla sicurezza:

- CVE-2022-33005: Una vulnerabilità cross-site scripting (XSS) che consente agli attaccanti di eseguire script web arbitrari tramite un payload predisposto inserito nel campo di testo "Nome";
- CVE-2022-29556: Il microservice iot-manager consente SSRF perché l'integrazione dell'IoT Hub fornisce diverse primitive SSRF che possono eseguire azioni cross-tenant tramite endpoint API interni;
- CVE-2022-24796: Esiste una vulnerabilità RCE (Remote Code Execution) nella funzione di caricamento dei file dell'interfaccia WebUI di RaspberryMatic. La mancata convalida/sanificazione dell'input nel meccanismo di caricamento dei file consente agli attaccanti remoti non autenticati con accesso di rete all'interfaccia WebUI di ottenere l'esecuzione arbitraria dei comandi del sistema operativo tramite metacaratteri shell nella stringa di query HTTP;
- CVE-2022-23266: Una falla di sicurezza in software antivirus per i dispositivi IoT potrebbe comportare vulnerabilità quali Remote Code Execution, Elevazione dei Privilegi o Information Disclosure;
- CVE-2022-25651: Corruzione della memoria nell'host bluetooth a causa di un overflow di numeri interi durante l'elaborazione del profilo BT HFP-UNIT;
- CVE-2022-22083: Denial of Service (DoS) a causa del danneggiamento della memoria in sistemi utilizzabili per realizzare ambienti mobili su dispositivi quali smartphone, tablet e smartbook;
- CVE-2022-22072: L'overflow del buffer può verificarsi a causa della non corretta convalida della lunghezza delle informazioni dell'applicazione NDP.

Stato della sicurezza dei settori economici italiani 3Q2022

In questo approfondimento si osserva l''evoluzione del livello di sicurezza dei settori economici italiani in riferimento al 3Q2022.
Per valutare tale livello di sicurezza Exprivia ha introdotto un nuovo indice di valutazione detto "Investment Index (II)" che mette in correlazione l'impatto di ogni vulnerabilità rilevata da Exprivia e il numero di occorrenze di queste ultime, per ognuna delle aziende monitorate.
Il valore ottenuto viene poi normalizzato in un intervallo tra 1 e 10.
Il valore 1 rappresenta un livello di sicurezza molto basso, indicando che l'azienda analizzata ha una forte esposizione al rischio cyber mentre il valore 10 rappresenta un livello di sicurezza elevato con conseguente minore esposizione al rischio di subire attacchi informatici.
Nell'analisi sono state prese in considerazione le cinque aziende leader dei seguenti settori economici:

- Automotive
- Consulting
- Critical Infrastructure
- Educational
- Entertainment
- Finance
- Healthcare
- Hospitality
- Industrial
- ONG
- Public Administration
- Religion
- Retail
- Security
- Software
- Telco

Per ognuna delle cinque aziende di ogni settore economico sono state valutate tutte le vulnerabilità, è stata applicata la formula vista precedentemente e successivamente è stata fatta una media per calcolare l'II del settore economico analizzato.

In tabella 5 vengono riportati i risultati ottenuti comparati con quelli del 2Q2022:

	Investment Index 2Q2022	Investment Index 3Q2022
Automotive	9,8973	9,9349
Consulting	9,4898	9,5440
Critical Infrastructure	9,5781	9,5427
Education	9,8347	9,8346
Entertainment	7,2762	7,7040

Finance	9,9526	9,9692
Healthcare	9,9895	9,9925
Hospitality	9,9881	9,9863
Industrial	9,9986	9,9989
ONG	9,9862	9,9844
PA	9,9876	9,9896
Religion	9,9994	9,9991
Retail	9,2437	9,8880
Security	9,9977	9,9984
Software	9,9982	9,9984
Telco	9,8224	9,9005

Tabella 5 - Investment Index media di ogni settore economico analizzato nel 3Q2022

I risultati ottenuti vengono mostrati graficamente in Figura 41:

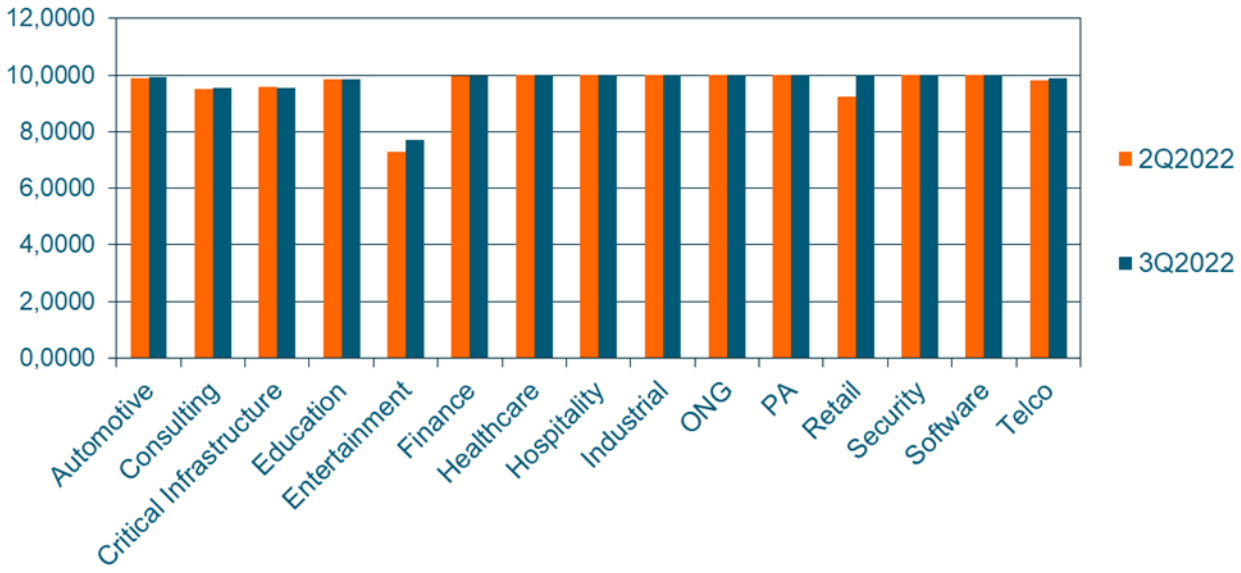

Figura 41 - Rappresentazione grafica dell'Investment Index media per ogni settore economico analizzato

Dalla figura precedente risulta che il settore avente il minor numero di vulnerabilità, ovvero la minor esposizione al rischio, è il settore Religion con il valore di II più alto (pari a 9,9991), in decremento rispetto a quello del 2Q2022.

Il settore con il più alto numero di vulnerabilità, ovvero la più alta esposizione al rischio, è il settore dell'Entertainment presentando un II pari a 7,7040 (in aumento rispetto a quello del 2Q20022 in cui era stato rilevato un II pari a 7,2762).
Rispetto al quarter precedente è evidenziabile una impercettibile miglioramento nell'efficienza degli investimenti in tutti i settori economici analizzati.
A questo punto dell'analisi si vuole valutare in quale area geografica si abbia il miglior livello di sicurezza possibile. I valori per Nord, Centro e Sud sono riportati in tabella 6 comparati con quelli del 2Q2022:

	Investment Index 2Q2022	Investment Index 3Q2022
Nord	9,6108	9,7051
Centro	9,7891	9,8492
Sud	9,9897	9,9921

Tabella 6 - Investment Index per Area Geografica

I risultati mostrati in tabella vengono mostrati graficamente in figura 42:

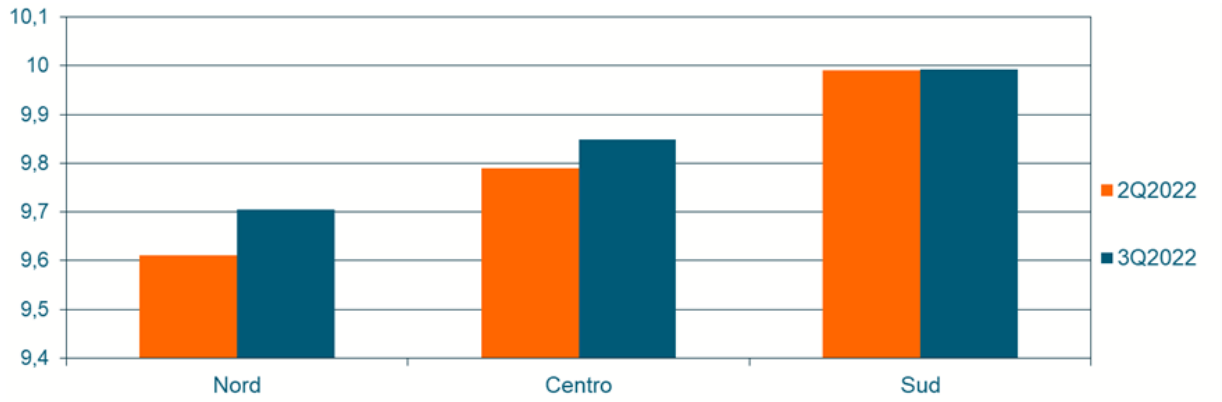

Figura 42 - Investment Index per Area Geografica

Dalla figura si evince come, rispetto al quarter precedente, ci sia stato un notevole miglioramento dell'efficienza degli investimenti a Nord, un miglioramento moderato al centro ed un miglioramento lieve a sud.

Il nuovo indice (Investment Index) appena introdotto, mostra quanto siano efficaci gli investimenti aziendali in ambito cyber security, fortemente influenzato dalla velocità con cui le aziende affrontano il progresso tecnologico senza un adeguato supporto alla protezione delle nuove soluzioni introdotte.

Stato delle vulnerabilità sul territorio nazionale 3Q2022

Exprivia crede nel valore della condivisione e mette a disposizione i dati rilevati sulle vulnerabilità dei prodotti maggiormente utilizzati in Italia dal suo Osservatorio a beneficio di chi lavora nel mondo della CyberSecurity. In questo articolo verranno evidenziate alcune vulnerabilità, individuate dal nostro Osservatorio, che riguardano prodotti utilizzati sul territorio italiano.
Per ciascuna vulnerabilità è stata individuata la relativa CVE (ove è stato possibile), il danno che ha provocato, la tipologia della vittima, la sua gravità e la diffusione della tecnologia vulnerabile sul territorio italiano.
La maggior parte delle vulnerabilità individuate sono state pubblicate dal CSIRT (Computer Security Incident Response Team) nazionale e sono state rilasciate delle patch per eliminarle.

Le vulnerabilità individuate nei mesi di luglio, agosto e settembre hanno toccato differenti aeree del territorio italiano creando non poche problematiche. In questo terzo quarto del 2022 è stato registrato un andamento constante rispetto ai tre mesi precedenti. Il numero vulnerabilità riscontrate è molto alto, un prodotto vulnerabile può mettere in serio pericolo tutti coloro che utilizzano quotidianamente qualsiasi tipo di tecnologia, soprattutto in questo periodo storico dove gran parte della popolazione italiana utilizza vari strumenti tecnologici sia per lavorare che per studiare da remoto.

Le vulnerabilità individuate negli ultimi tre mesi del 2022 hanno interessato differenti aeree del territorio italiano creando non poche difficoltà.
Nel grafico possiamo vedere come il settore dove le vulnerabilità sono state maggiormente individuate sono in ambito "*Industria*", 20%. Le vulnerabilità che hanno come vittima le industrie possono creare danni economici nel momento in cui viene individuata una falla bloccante per l'intera produzione.
Nel 3Q2022 sono state un gran numero di vulnerabilità in ambito "*Security*", il 18%. Questo dato è molto importante inquanto vulnerabilità di questo tipo sono molto pericolose perché interessano strumenti che hanno come intento la protezione delle infrastrutture e degli utenti stessi. Riguardano tecnologia come antivirus, firewall e VPN.
In questo ultimo quarto si è riscontrato un netto decremento delle vulnerabilità relative alle *telecomunicazioni* rispetto al quarto precedente, il cinquanta percento. Evitare queste vulnerabilità è di vitale importanza perché una falla in questi sistemi può provocare danni consistenti anche dal punto di vista della privacy dell'utente.
Anche in questo quarto sono presenti vulnerabilità di tipo "*Software/Hardware*". Una falla in un software o hardware può creare danni ingenti sia dal punto di vista della privacy che dal punto di vista economico.
Nel terzo quarto del 2022 rispetto al secondo non sono state registrate vulnerabilità legate alle *infrastrutture critiche*. Un aspetto da non sottovalutare perché una vulnerabilità ad un sistema di utilizzato in una infrastruttura critica potrebbe causare danni sia all'ente stesso ma anche alla collettività, in quanto questi enti erogano servizi di prima necessità.
In questo quarto è stato riscontrato un netto incremento delle vulnerabilità in ambito "*Browser",* più del doppio. Una vulnerabilità di questo tipo può provocare perdite di dati e privacy da parte dell'utente. Un cybercriminale, sfruttando questa vulnerabilità, è in grado di appropriarsi di tutti i dati di navigazione e soprattutto delle password salvate dal Browser.
Come nei tre mesi precedenti, anche in questo secondo quarto sono state riscontrate vulnerabilità relative ai *sistemi operativi*. Un sistema vulnerabile può causare qualsiasi genere di disservizio e danno.
Nel 3Q2022 sono state riscontrate anche vulnerabilità che riguardano i sistemi e-commerce. Una vulnerabilità di questo tipo può causare un mal contento su una grande fascia di utenti che utilizzano questi siti per effettuare acquisti online.
Da evidenziare il dato relativo alle vulnerabilità legate ai software che permettono la *conservazione di documenti,* quasi 8 volte superiore al quarto precedente. Questo tipo di vulnerabilità mette a rischio la privacy e l'integrità del contenuto di questi documenti creando danni sia economici che d'immagine alle vittime.

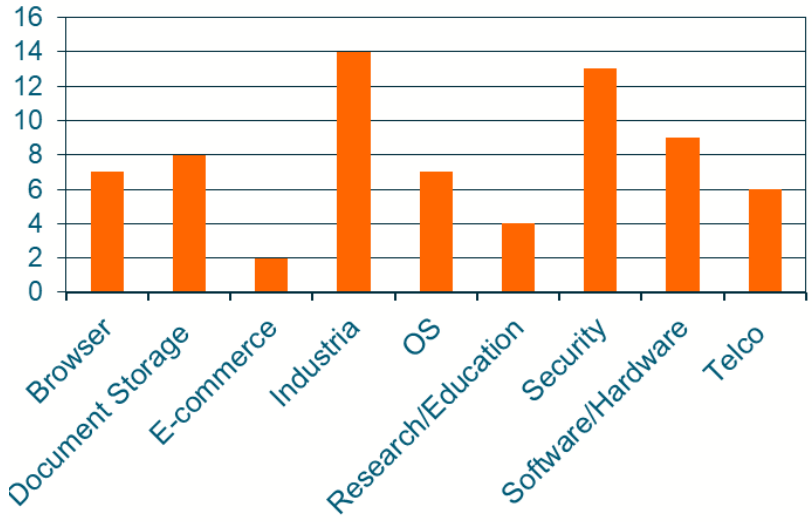

Figura 43 - Tipologia vittima 3Q2022

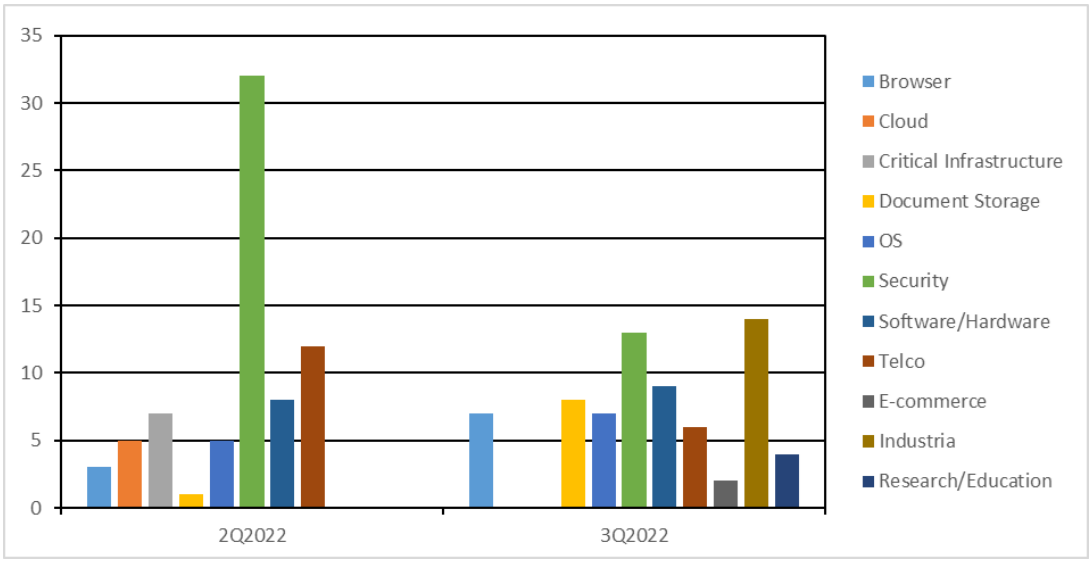

Figura 44 - Tipologia vittima 2Q2022 e 3Q2022

Analizzando invece la tipologia dei danni generati a seguito delle vulnerabilità individuate emergono alcuni aspetti interessanti.

In questo secondo quarto del 2022 la tipologia di danno più riscontrata è "*Denial of Service*", 20%. Questa vulnerabilità crea importanti disservizi all'intero sistema rendendolo inutilizzabile.

Nel 3Q2022 è stato registrato un decremento delle vulnerabilità che causano danni di tipo di "*Privilege escalation*", del 37% rispetto il quarto precedente. Una falla di questo tipo permette di acquisire il controllo di risorse di macchina normalmente oscurate ad un utente. Un user con maggiori autorizzazioni di quelle previste dallo sviluppo originale o fissate dall'amministratore di sistema può, ovviamente, operare azioni inattese e perciò non autorizzate.

Come nel secondo quarto anche nel secondo sono state riscontrate un gran numero di vulnerabilità che causano danni di tipo "*Remote code execution*". Questo tipo di danno è molto rischioso in quanto rende possibile, ad un malintenzionato, di eseguire codice malevolo da remoto senza che la vittima sia a conoscenza. Tra gli obiettivi principali di un attacco RCE si annovera il furto di credenziali privilegiate il cui utilizzo amplia il perimetro di accesso verso altre tipologie di dati e altri sistemi raggiungibili dal sistema compromesso.

Nel 3Q2022 è stato registrato un lieve decremento per quanto riguarda le vulnerabilità che causano la *perdita di dati*. Questa tipologia di vulnerabilità è sfruttata dai cybercriminali per recuperare dati sensibili e utilizzarli per i propri scopi. Questo perché i dati sono sempre più importanti per i cyber criminali.

Le vulnerabilità che provocano "*Service interrupt* hanno registrato un netto aumento, quasi dieci volte in più rispetto i mesi precedenti. Esse provocano non pochi problemi sia per coloro che stanno lavorando in smart working, i quali si sono visti il proprio dispositivo non funzionare, e sia per alcuni studenti che hanno la necessità di seguire le lezioni da remoto.

Rispetto il secondo quarto del 2022, in quest'ultimo quarto è stato registrato un lieve incremento delle vulnerabilità che causano danno di tipo "*C&C*". Falle che provocano danni di tipo Command and control sono molto pericolose in quanto un cybercriminale potrebbe prendere il controllo del proprio dispositivo creando non pochi problemi.

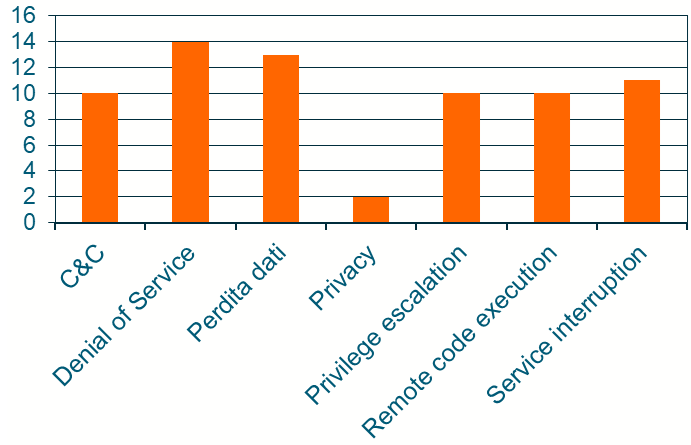

Figura 45 - Tipologia danno 3Q2022

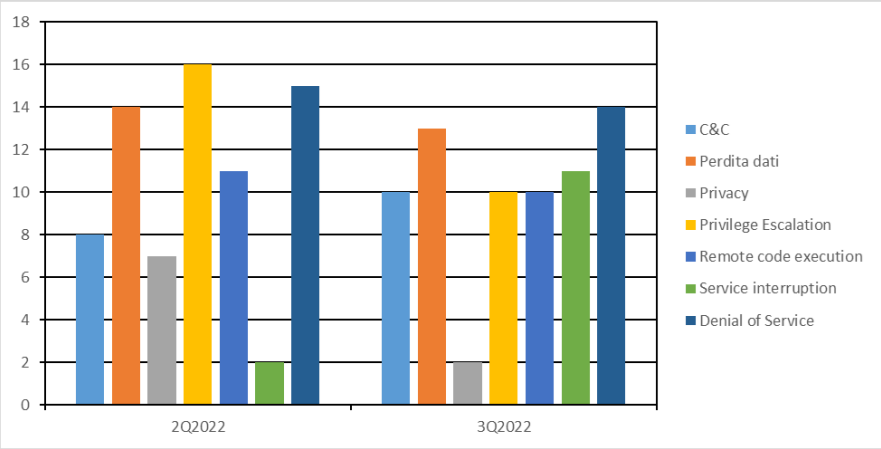

Figura 46 - Tipologia danno 2Q2022 e 3Q2022

Tutte le vulnerabilità individuate dal nostro Osservatorio nel 3Q2022 hanno criticità abbastanza elevata. Sono state riscontrate esattamente 21 critiche, 40 alte e 9 risultano medie. Questo sta a significare che la maggior parte delle vulnerabilità possono creare problemi su qualsiasi fronte, dalla perdita di dati personali o di denaro, a problemi sulla comunicazione. Per evitare qualsiasi problematica e limitare i danni sarebbe necessario rendere pubblica la vulnerabilità individuata affinché non venga sfruttata dai cybercriminali per i propri scopi. Perciò è di fondamentale importanza rimanere aggiornati sulle nuove vulnerabilità, questo è possibile grazie al CSIRT nazionale o sui rispettivi siti delle case produttrici delle tecnologie utilizzate.

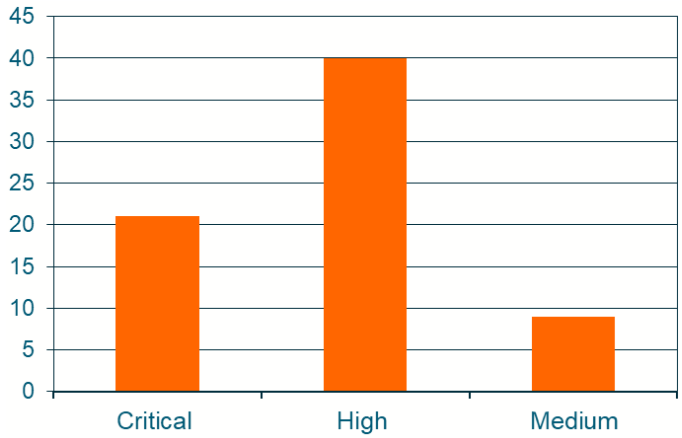

Figura 47 - Severity vulnerabilità 3Q2022

Malware 3Q2022

Alina

Alina, già noto dal 2012, è conosciuto meglio come Alina POS in quanto specializzato nell'attaccare sia dispositivi POS terminali che computer con software POS dedicato.
In questi anni il malware ha subito vari sviluppi e aggiornamenti. Ad oggi utilizza e sfrutta nuove tecniche e procedure di attacco al fine di evitare di essere rilevato e sfuggire ai controlli.
L'obiettivo di Alina è stato da sempre quello di esfiltrare e rubare i dati delle carte di credito per poterli rivendere e generare così un processo di contrabbando. Inizialmente sfruttava il protocollo https, oggi invece l'unico canale di comunicazione utilizzato dal malware è il servizio DNS.
Durante le transazioni con carta di credito, i dati vengono solitamente decrittografati e tenuti temporaneamente in memoria dal software POS in forma non crittografata. È proprio questo il momento in cui Alina preleva dalla RAM del terminale o PC infetto le informazioni non crittografate presenti sulla carta di credito, le analizza verificandone la correttezza e le trasmette al server C2 attraverso un tunneling DNS che permette di evadere i controlli di sicurezza.
Cercare di evitare questi malware ad oggi è molto difficile. Sicuramente tutte le aziende fornitrici di sistemi POS devono prevedere adeguate misure di protezione prevedendo non solo il monitoraggio del traffico http/https ma anche e soprattutto quello DNS. In questo modo è possibile individuare e bloccare le eventuali richieste sospette consentendo agli esercenti e alla propria clientela di operare in sicurezza.

BianLian

BrianLian è un ransomware in grado di adeguare le sue operazioni alle capacità dei sistemi di protezione che ha causato diverse vittime BrianLian è scritto nel linguaggio di programmazione opensource GoLang che può essere implementato, vanificando il reverse engineering e compromettendo contemporaneamente più piattaforme.

Utilizza una backdoor speciale per mantenere un accesso costante alla rete e recuperare in ogni istante payload arbitrari dai server remoti. Rimane all'interno del sistema per circa sei settimane dal momento in cui l'attore malevolo ottiene l'accesso iniziale e l'evento di crittografia effettivo.

Il ransomware esegue tre attività:

- Una volta inserito nel dispositivo, inizia a scansionare e a criptare i file presenti nel dispositivo;
- Dopo aver completato il processo di crittografia, richiede un riscatto attraverso una nota dove fornisce le istruzioni per ripristinare i propri file crittografati minacciando che i dati prelevati e bloccati verranno pubblicati se il pagamento non avviene entro 10 giorni.
- Ultimate le precedenti, si autoelimina

Come per tutte le tipologie di malware e ransomware, per difendersi dagli attacchi, gli utenti possono attivare e aggiornare i programmi su computer e ogni dispositivo connesso. Inoltre, si consiglia sempre di utilizzare esclusivamente strumenti legittimi, prestare attenzione ad allegati e collegamenti presenti in e-mail e messaggi sospetti. Indispensabile è dotarsi di un antivirus affidabile installato e mantenuto aggiornato, eseguendo scansioni regolari del sistema.

ChromeLoader

Il malware ChromeLoader è un tipo di virus già noto in passato che ha recentemente registrato un picco improvviso e inaspettato. Si tratta di un browser hijacker e browser infection threat, pervasivo e persistente, che può modificare le impostazioni di Chrome e reindirizzare le vittime verso siti pubblicitari, andando a monetizzare i clic sui siti di advertising e distribuendo ransomware.
Le estensioni del browser permettono di aggiungere funzionalità per gestire al meglio la navigazione dell'utente, influendo sull'esperienza di navigazione dell'utente finale.
Per insidiarsi nel sistema, gli autori utilizzano un file di archivio ISO. Nel momento in cui viene installata l'estensione malevola, attraverso l'uso di PowerShell, le problematiche di sicurezza per gli utenti diventano importanti soprattutto se ChromeLoader è impiegato come infostealer o spyware per esfiltrare dati dalle sessioni del browser di un utente.
La nuova variante di ChromeLoader risulta anche più aggressiva della precedente.
L'installazione del malware sul PC avviene nel momento in cui l'utente fa clic sul link Install che esegue un file batch. È anche previsto l'avvio automatico mediante l'aggiunta di una chiave al registro di sistema di Windows.
Per evitare di incappare in questa e in altre minacce informatiche è essenziale proteggere il proprio computer con un buon software antivirus.

CloudMensis

Il malware CloudMensis, così denominato perché usa i nomi dei mesi per classificare le directory, spia gli utenti di Mac compromessi e utilizza servizi di archiviazione cloud pubblici per comunicare con i suoi operatori. Al momento CloudMensis è una minaccia per i soli utenti Mac. Una volta ottenuta l'esecuzione del codice e i privilegi amministrativi, CloudMensis esegue un primo stadio del malware che apre le porte a un secondo livello più ricco di funzionalità tramite un servizio di cloud storage, in grado di raccogliere informazioni. L'intento degli aggressori è quello di esfiltrare documenti, screenshot, allegati e-mail e altri dati sensibili.
Apple ha recentemente riconosciuto la presenza di spyware che prendono di mira gli utenti dei suoi prodotti e sta presentando in anteprima la modalità Lockdown su iOS, iPadOS e macOS, che disabilita le funzioni spesso sfruttate per ottenere l'esecuzione del codice.
Come sempre, è consigliabile l'utilizzo di Mac aggiornati per evitare eventuali elusioni della protezione.

CobaltStrike

Colbalt Strike è uno dei tool di Adversary Simulation in ambito di cybersicurezza e dai cybercriminali più noti e apprezzati per le attività di Red Teaming. Infatti, se da un lato riesce a riparare eventi malevoli, allo stesso tempo può essere integrato ad altri strumenti e potenziare l'efficacia dell'attacco.
Colbalt Strike è stato sviluppato dal famoso sviluppatore e ricercatore in ambito di sicurezza informatica, Raphael Mudge. Viene utilizzato per effettuare attività di penetration test ed emulare potenziali attacchi esterni.
Il tool è in grado di selezionare e replicare, senza sconti, tecniche e tattiche di attacco nei confronti di reti e sistemi informatici. Offre un agent post-sfruttamento e canali segreti per simulare un silenzioso attore incorporato a lungo termine nella rete.
I moduli di Cobalt Strike sono personalizzati e richiedono firme uniche e risulta estremamente semplice il suo utilizzo.

È stato sviluppato nel 2012 e rilasciato come piattaforma autonoma di emulazione delle minacce, ma viene utilizzato anche da criminali informatici e APT nelle loro campagne in quanto le sue caratteristiche integrate consentono di distribuirlo e attivarlo rapidamente indipendentemente dal livello di complessità del responsabile o dalla disponibilità di risorse umane o finanziarie.
Le sue caratteristiche consentono di distribuirlo e renderlo operativo in modo rapido e può essere acquistato direttamente dal sito web del vendor oppure all'interno del dark web all'interno di numerosi forum di hacking, in versioni craccate.

DawDropper

DawDropper è un malware per Android, in grado di causare numerosi danni al dispositivo che ne viene. Il suo scopo è manipolare il sistema Android, sfruttando le vulnerabilità di Android e manipolarlo. Grazie alla sua caratteristica, può effettuare un contagio a catena ed è offerto dai suoi progettisti come servizio Malware-as-a-Service (MaaS). I criminali possono usarlo per difendere il software dannoso a pagamento.
Può infettare attraverso:
• Il download di un qualsiasi tipo di applicazione di terze parti al di fuori di Google Play Store.
• L'iniezione di uno script dannoso a causa del tocco di un collegamento dannoso o di un reindirizzamento del browser.
• Pubblicità pericolosa di un'App legittima che reindirizza ad una pagina di script di virus.
• Allegato in e-mail infette.
• Ingegneria sociale.
Una volta che si inserisce nel dispositivo, ottiene i permessi per controllare le attività dell'utente ed esegue azioni in background, in modo indisturbato e scarica/installa malware aggiuntivo, soprattutto trojan bancari, che hanno la capacità di forzare l'apertura di pagine Web di phishing camuffate da siti di banche online o di sovrapporre app bancarie con finestre che registrano le credenziali di accesso immesse al loro interno.
DawDropper può causare più infezioni del sistema che possono portare a gravi problemi di privacy, perdite finanziarie significative e furto di identità.
Oltre al furto delle Informazioni personali e finanziarie rubate all'utente, quali messaggi privati, accessi/password, il malware riduce le prestazioni del dispositivo, scarica rapidamente la batteria, diminuisce la velocità di Internet. Fortunatamente un software anti-malware legittimo è in grado di rilevare la sua presenza e di eliminarlo.

DcRat

DCRat è un trojan commerciale che ha come obiettivo principale quello di effettuare esfiltrazione dei dati in quanto supporta il keylogging e il furto di informazioni riservate come le credenziali dai browser Web installati e dai client FTP. È stato sviluppato da un singolo operatore, noto come "boldenis44", "crystalcoder" o "Coder" (in caratteri cirillici), che sottopone il malware a un costante aggiornamento per svolgere al meglio la sua funzione principale: rubare dati. Viene venduto su AppStore come un qualsiasi programma legittimo.
Si basa su un modello SaaS e include tre componenti:

- un file eseguibile che agisce da client,
- una pagina PHP per l'endpoint C2 (command-and-control)
- uno strumento di amministrazione.

Le funzioni DCRat includono:

- Registrazione chiavi
- Fare screenshot
- Prelevare cookie, password e contenuti dei moduli dai browser Web installati
- Rubare le credenziali dai client FTP installati come FileZilla
- Rubare il contenuto degli appunti
- Raccoglie le informazioni sulla macchina (nome computer host, nome utente host, posizione del paese, prodotti di sicurezza installati, ecc.)
- Invia le informazioni raccolte a un server C2.

Gli operatori hanno la possibilità di espandere e personalizzare le funzionalità del trojan per vari scopi ed esecuzione di codice arbitrario.
All'interno del canale telegram, sono disponibili informazioni circa gli aggiornamenti che i criminali effettuano costantemente. All'interno della chat è stato annunciato che ci sarà un rinnovamento di un plug-in per il furto di criptovalute. Di conseguenza, oltre allo scopo principale per il quale è stato creato, ovvero rubare dati, può causare ulteriori danni. Il criminale può mantiene la persistenza a lungo termine e rubare informazioni di identificazione personale (PII) e dati riservati.

EnvyScout

EnvyScout è un nuovo ceppo di malware utilizzato in un attacco di phishing in Italia da parte di un indirizzo falso denominato "cancelliere governo.it". I responsabili dell'operazione provengono da APT29, un gruppo di hacker ben conosciuto che probabilmente ha anche legami con la Russia. Altri nomi usati per designare lo stesso attore della minaccia sono Nobelium, SolarStorm, DarkHalo, NC2452 e StellarPartile.
EnvyScout è un dropper dannoso in grado di offuscare e scrivere su disco un file ISO dannoso tramite un allegato alle e-mail di spear-phishing.
EnvyScout è progettato per rilasciare il payload della fase successiva sul sistema infetto, acquisendo ed esfiltrando determinati dati, come le credenziali NTLM degli account Windows.
L'utente riceve file allegato HTML / JS, malevolo, distribuito con il nome "NV.html". Quando viene eseguito, il file NV tenterà di scaricare un'immagine sul sistema locale.
Se il file immagine viene avviato dall'utente, verrà visualizzato un collegamento denominato NV che eseguirà un file nascosto denominato "BOOM.exe". Il file nascosto fa parte del payload della fase successiva per il malware BoomBox.
Allo stesso tempo, le credenziali di Windows NTLM dell'utente connesso possono essere inviate a un server remoto sotto il controllo degli hacker. I criminali informatici possono quindi tentare di raggiungere la password in testo normale contenuta nei dati tramite metodi di forza bruta.

Graphite

Si tratta di un malware che si diffonde attraverso un documento PowerPoint. Peculiarità di graphite è che non contiene nessuna macro, ma sfrutta una tecnica di esecuzione del codice che si attiva passando semplicemente il mouse, senza nessun clic.
Una volta aperta la presentazione ppt, passando il mouse su un collegamento ipertestuale in essa contenuta, che funge da trigger per la distribuzione di uno script PowerShell dannoso, viene scaricata una versione del malware Graphite. Una volta installato, il malware comunica con un server di comando e controllo attraverso il dominio "graph[.]Microsoft[.]com" abusando del servizio che fornisce l'accesso alle

risorse Microsoft Cloud. I probabili obiettivi dell'operazione includono probabilmente entità e individui che operano nei settori della difesa e del governo dell'Europa e dell'Europa orientale.

Hydra

Hydra è un trojan bancario presente su Android che riesce ad aggirare le barriere protettive del Play Protect del Play Store e ad infettare il dispositivo del malcapitato una volta che questo ha proceduto con il download e l'installazione di alcune app che sono portatrici del virus.
In particolare, le applicazioni prese di mira sono quelle bancarie e questo trojan presenta determinate funzionalità che gli consentono di prendere il controllo del dispositivo: dalla gestione completa degli SMS alla possibilità di accedere al device compromesso tramite TeamViewer, al furto del PIN ed all'interazione del bot con il C2 per ricevere comandi ed eseguire nuove istruzioni.
L'obiettivo, quindi, è quello di rubare dati personali degli utenti, nello specifico: carte di credito, account bancari, numeri di telefono, indirizzi mail, oltre che ovviamente credenziali personali, da sfruttare per campagne phishing successive o per attivare silenziosamente servizi in abbonamento sulla scheda SIM dell'utente.
Il malware è veicolato attraverso un link presente all'interno di un SMS e la pagina di download è visibile solo se visitata da un browser che si presenti con User-Agent Android. Il file malevolo in questione è un APK che viene scaricato dai server Discord.
Un modo per difendersi da questo trojan è quello di verificare i file che si stanno andando ad eseguire assicurandosi di non aprire mai un allegato, un link o un programma fino a quando non si è sicuri che questi provengano da una fonte sicura. Una volta eseguito il download in locale, bisogna controllare il file scaricato con l'esecuzione di un software antivirus per verificare l'eventuale presenza di virus o trojan
Questo malware è rivolto principalmente ad utenti Italiani, anche se si è scoperto che, essendo in grado di effettuare un controllo sull'IP con cui il dispositivo è connesso alla rete Internet, riesce ad analizzare anche il country code. Al momento risulta che gli unici paesi esclusi dalla compromissione siano Russia e Ucraina.

Lunar

Lunar è un malware che sta spopolando tra gli adolescenti. È stato rilevato un malware di tipo as-a-service con un prezzo estremamente contenuto: dai 5 ai 25 dollari, venduto all'interno del server Discord. Le indagini condotte hanno evidenziato che il costo così basso è dovuto al target di utenti/clienti e ideatori per lo più teenager.
Si tratta di un malware builer generato con lo scopo di provocare fastidi e noie alle vittime, più che un reale danno, dato che tra le sue principali funzioni presenti vi sono plugin inviati dai membri della community.
Lo scopo di Lunar è di attirare l'attenzione all'acquisto delle funzionalità che permettono di colpire account gaming, per eliminare le cartelle relative a vari videogame (Fortnite, Minecraft) o di aprire ripetutamente finestre del browser con le pagine indesiderate. Si nasconde come gioco craccato o hack di gioco o renderli poco appariscenti utilizzando icone e nomi di file di eseguibili di giochi legittimi.
È un malware creato "su misura" con le componenti desiderate e può includere l'opzione di furto di dati come le password dell'utente, ma non solo perché Lunar potenzialmente espone le vittime al furto dei dati anche sensibili.
Gli sviluppatori del malware sono un gruppo di criminali non professionisti e poco attenti, infatti hanno condiviso informazioni varie dai sui loro account social.

NullMixer

NullMixer è un dropper, scoperto dagli esperti di Kaspersky, capace di installare sul computer oltre 20 malware differenti come spyware, trojan, backdoor, stealer, miner ecc..
La strategia utilizzata dai criminali è far apparire i siti nelle prime posizioni di Google. In questo modo, l'utente in cerca di un software, visita il sito e clicca sul link. Viene immediatamente scaricato un file ZIP protetto da password, il dropper viene eseguito e Microsoft Defender viene disattivato.
Attraverso NullMixer si può rubare qualsiasi dato dal computer, di ogni tipo. L'utente si accorgerà dell'esecuzione di molteplici malware in quanto il PC diventerà inutilizzabile; a questo punto, l'unica soluzione sarebbe la reinstallazione del sistema operativo.

PureMiner

PureMiner è un malware che viene distribuito dal loader iniziale Pure Crypter ed è veicolato tramite mail con allegati Zip da cui viene estratto un SCR. Ha l'obiettivo di rubare informazioni e dati sensibili delle vittime
PureCrypter è una botnet di tipo Malware as a Service (MaaS) scritto in C#, che esiste dal 2021, in grado di generare una lunga catena di propagazione di una qualsiasi altra famiglia di malware ad esso vincolante iniettandoli nei processi vitali del sistema operativo colpito. È un eseguibile .NET che gira su ambiente Windows.
Questo loader utilizza i suffissi dei nomi delle immagini combinandoli con inversione, compressione e crittografia al fine di evitare il rilevamento.
PureCrypter è solito utilizzare il meccanismo del pacchetto che consiste in due eseguibili: downloader e injector. Il downloader è il responsabile della propagazione dell'iniettore e rilascia ed esegue il payload finale injector sulla macchina di destinazione. L'injector utilizza trucchi e tecniche come l'offuscamento binario, il rilevamento dell'ambiente di runtime, l'avvio di processi puppet, ecc per aggirare gli antivirus.
È un malware che si intercetta potenzialmente tramite internet, quindi, per evitare di essere infettati occorre non solo prestare elevata attenzione a ciò che si scarica analizzando attentamente la fonte di provenienza, ma occorre installare sul proprio computer una soluzione antivirus altamente efficiente e mantenere aggiornato il sistema operativo

WinGo

Il Trojan WinGo è un malware che infetta i computer e che agisce come spyware, downloader e backdoor. Il suo scopo è quello di indebolire il sistema per iniettare altri virus alterando gli elementi vitali necessari per il corretto funzionamento del sistema ovvero le impostazioni del sistema, modificando i criteri di gruppo e il registro.
Il virus contenuto in questo malware, consente ai criminali informatici di rubare dati personali, da rivendere su Darknet, attraverso l'utilizzo di funzioni adware e browser hijacker. Funzioni che consentono di fare soldi grazie alla visualizzazione di banner che vengono creati. Ogni visualizzazione incrementerà il "bottino".
Essere infettati da questo trojan è molto semplice se non si è attenti durante la navigazione su internet. Basta cliccare su annunci pubblicitari di strani siti Web o aprire popup presenti nel browser per avviare il processo di infezione. È importante, quindi, sapere cosa è legittimo e cosa no, e soprattutto prestare attenzione prima di effettuare un semplice "click".

YTStealer

Come suggerisce il nome, il nuovo virus YTStealer è stato progettato per attaccare un bersaglio specifico: gli YouTubers. Il virus fa parte della famiglia degli infostealer e prende di mira YouTube per rubare i cookie di autenticazione dei canali e prenderne possesso.
Il virus cerca di insediarsi sui computer inviando email o messaggi che invitano a scaricare software di editing video, trucchi per videogiochi o crack per Spotify Premium o Discord Nitro infettati da malware.
Una volta insediato nel sistema, il malware ispeziona i file di database del browser per individuare i token di autenticazione dei canali YouTube, raccolgliendo molti più dati, inclusi il nome del canale, la data di creazione, il numero di iscritti, lo stato ufficiale e i dettagli sulla monetizzazione.
Gli account YouTube rubati vengono venduti sul dark web e i prezzi variano in base alle dimensioni del canale. Inoltre, gli hacker tendono a chiedere un riscatto ai proprietari originali con la promessa di restituire i loro spazi (cosa che quasi mai avviene), continuando poi a contattare i follower lanciando truffe che si basano su improbabili investimenti in criptovalute.
Un buon modo per difendersi potrebbe essere sloggarsi dal proprio account YouTube e riaccedere dopo qualche minuto, affinché i token di autenticazione vengano aggiornati, invalidando i precedenti.

Autori

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

Antonio Pontrelli, ha conseguito la laurea Magistrale in Sicurezza Informatica presso l'università di Bari, attualmente svolge l'attività penetration testing, vulnerability assessment e ricopre il ruolo di SOC Analyst e CyberSecurity Specialist presso Exprivia.
Infine, è speaker di eventi nazionali come ITASEC e Clusit.

Carlo Falciola: ha conseguito la laurea in scienze della Informazione presso l'Università degli Studi di Milano. Attualmente è responsabile della prevendita e dello sviluppo commerciale dell'offerta CyberSecurity per tecnologie, progetti e servizi, con particolare attenzione ai mercati finanziari e assicurativi, all'industria e alla pubblica amministrazione in Exprivia. Le sue attività spaziano dallo scouting tecnologico, alla progettazione della offerta, alla costruzione di proposte per i mercati target e alla gestione di progetti di delivery delle soluzioni.

Rosita Galiandro ha conseguito la laurea Magistrale in Sicurezza Informatica presso l'Università di Bari.
Attualmente ricopre il ruolo di Responsabile Osservatorio CyberSecurity presso Exprivia.
Contribuisce alle attività di prevendita e collabora in piani di insegnamento sul progetto *CyberChallenge* con diverse università nell'ambito CyberSecurity.

Fabiano Vincenzo Malerba ha conseguito la laurea magistrale in International Relations presso la Luiss Guido Carli (Roma)**.** In Exprivia ricopre il ruolo di Security Analyst e event collector all'interno della DFCY-CY Digital Factory cybersecurity, sezione offering service.

Ernesto Vignes dal 1998 collabora con diverse realtà del settore IT come sistemista dal 2015 presso Exprivia partecipa a diversi progetti in ambito Telco & Media ricoprendo il ruolo di system engineer.
Attualmente collabora con la DFCY-CY Digital Factory CyberSecurity di Exprivia, ove si occupa delle soluzioni di IdAM.

Gaetano Scavo, ha conseguito la laurea Magistrale in Sicurezza Informatica presso l'università di Bari, attualmente svolge l'attività penetration testing, vulnerability assessment e ricopre il ruolo di SOC Analyst presso Exprivia**.**

Gianluca Porcelli, ha conseguito la laurea Magistrale in Ingegneria Informatica presso il Politecnico di Bari.
In Exprivia ricopre il ruolo di SOC Analyst contribuendo ad attività di risk assessment, penetration testing e vulnerability assessment.

Michele Cortese, ha conseguito la laurea Magistrale in Ingegneria Informatica presso il Politecnico di Bari.
Attualmente ricopre il ruolo di Security Analyst presso Exprivia.
Svolge attività di delivery e si occupa della formalizzazione dei processi aziendali critici. Inoltre, è impegnato nella progettazione di un framework innovativo per la simulazione di un cyber range.

Antonio De Chirico, ha conseguito la laurea Magistrale in Sicurezza Informatica presso l'università di Bari, attualmente svolge l'attività di SOC Manager, Responsabile del Global Response Team e Digital Forenser in Exprivia. La sua esperienza nell'ambito della sicurezza è maturata nella Polizia Postale e delle Comunicazioni, dove per 15 anni ha svolto il ruolo di investigatore informatico e CTU per diverse Procure. Negli ultimi 5 anni ha svolto il ruolo di coordinatore della U.O. ICT presso il Centro Unico di Back Up della Polizia di Stato.

Carmelo Amoroso, da sempre appassionato di Telematica ed Informatica, inizia la propria carriera come tecnico sistemista presso vari clienti in Sicilia. Dopo un periodo di Formazione su SAP nella sede tedesca di Walldorf e di consulenza su vari clienti in ambito Telefonico e Assicurativo, si è spostato nel ramo dei Trasferimenti Telematici occupandosi della sicurezza, continuità operativa e Disaster & Recovery della piattaforma di Data Transfer per una azienda italiana operante nella logistica e nel settore bancario e assicurativo.
Attualmente come membro della DFCY-CY Digital Factory CyberSecurity di Exprivia ricopre il ruolo di CyberSecurity Analyst.

Luisa Colucci, ha conseguito la laurea in Informatica presso l'Università degli Studi di Pisa. Attualmente ricopre il ruolo di Solution Design Manager nella unit di CyberSecurity di Exprivia. Precedentemente ha ricoperto il ruolo di Security Architect nella divisione Security di IBM. Ha lavorato negli ultimi 10 anni nel campo della CyberSecurity acquisendo un'ampia conoscenza dei processi, delle tecnologie e del mercato. Nel suo passato ha ricoperto ruoli di leadership in un contesto lavorativo europeo ed è stata speaker in eventi nazionali e internazionali sulla CyberSecurity come ITASEC e Cybertech Tel Aviv.

Giuseppe Troianiello, CyberSecurity Analyst con particolare esperienza nel mercato finance, in Exprivia è responsabile di progetti in ambito IAM, PAM e Data Protection. Si occupa di A&D per lo sviluppo e il delivery di nuovi software, di installazione configurazione ed integrazione di prodotti di mercato, di customizzazione di applicativi esistenti.
Tra le sue attività inoltre vi è la fornitura di soluzioni applicative per l'adeguamento delle aziende alla normativa GDPR.

Giacomo Gorrieri, ricopre il ruolo di Operation Manager della Unit di CyberSecurity di Exprivia.
È laureato in Informatica ed Odontoiatria ed ha conseguito il Master di II Livello in "Governance e Audit dei Sistemi Informativi" presso il Dipartimento di Informatica dell'Università di Roma "La Sapienza". I suoi principali settori di competenza sono: il Project Management, IT Governance e Gestione di Processi aziendali.

Luigi Florio, ha conseguito la laurea in Scienze dell'Informazione presso l'Università degli Studi di Pisa.
Project Manager certificato PMP® si occupa principalmente di Privileged Access Management per l'unità cybersecurity di Exprivia. Più recentemente ha seguito progetti in ambito SAP per l'area sistemistica/infrastrutturale e di integrazione svolgendo anche attività di presales.

Ilaria Bruno, ha conseguito la laurea magistrale in Ingegneria Gestionale in Operation Management presso il Politecnico di Bari.
In Exprivia ricopre il ruolo di Customer Success all'interno della DFCY-CY, Digital Factory cybersecurity, sezione Offering.

Mariavittoria Ugirashebuja, ha conseguito la laurea magistrale in Ingegneria Gestionale in Operation Management presso il Politecnico di Bari.
Attualmente in Exprivia ricopre il ruolo di Solution Designer all'interno del SOC della DFCY, Digital Factory cybersecurity.

Mauro Gadaleta, ha conseguito la laurea magistrale in ingegneria delle telecomunicazioni con specializzazione in cybersecurity presso il Politecnico di Bari.
Attualmente svolge attività di gestione del portale CSIRT e ricopre il ruolo di SOC Analyst.

Gianmarco Cosoli, Dopo aver conseguito la laurea triennale in Informatica e Tecnologie per la Produzione del Software presso l'Università degli Studi di Bari, ha trascorso un periodo come sviluppatore backend di soluzioni Enterprise .NET (C#).
Ha un Master in Cyber Security: reti, sistemi e cloud e all'interno della Digital Factory di sicurezza si occupa di attività di security analysis.

Graziano Specchierla, ICT Security Consultant nella CyberSecurity Digital Factory di Exprivia, precedentemente Security Architect in IBM Security.
È coinvolto nel disegno di soluzioni, sviluppo del business e delivery sulle tematiche di sicurezza orientate principalmente al digital trust, alla gestione degli endpoint, alle implementazioni di soluzioni innovative.
Ha al suo attivo molti progetti, in varie aree dell'Information Technology, nelle discipline del system & network management, mobile management e del monitoraggio, in vari settori d'industria.

Micaela Petruzzelli, ha conseguito la laurea magistrale in Economia e Management presso l'Università di Bari.
Ha esperienza come analista funzionale e PMO nel settore gare e nell'ambito della Pubblica Amministrazione. In Exprivia si occupa di Offering Development all'interno della DFCY, Digital Factory Cybersecurity.

Marialuisa Gallo, ha conseguito la laurea triennale in Economia e Commercio presso l'Università Politecnica delle Marche.
In Exprivia ricopre il ruolo di business analyst all'interno della unit cybersecurity, svolgendo attività di sviluppo di nuovi servizi.

Gianmarco Troia, ha conseguito la laurea triennale in Informatica e Tecnologie per la Produzione del Software presso l'Università di Bari. Attualmente in Exprivia ricopre il ruolo di SOC Analyst nella Digital Factory Cybersecurity.

Sorgenti di Informazioni

1. https://securityaffairs.co/wordpress/
2. https://www.enforcementtracker.com/
3. https://thehackernews.com/
4. https://sicurezza.net/
5. https://www.cybertrends.it/
6. https://www.bleepingcomputer.com/
7. https://www.CyberSecurity360.it/
8. https://www.poliziadistato.it/
9. https://www.hackread.com/
10. https://www.forbes.com/
11. https://www.garanteprivacy.it/
12. https://www.cert-pa.it/
13. https://success.trendmicro.com/
14. https://www.commisariatodips.it/
15. https://www.securityinfo.it/
16. https://www.repubblica.it/
17. https://www.twitter.com/
18. https://threatpost.com/
19. https://wired.it/
20. https://zerobin.net/
21. https://d3lab.net/
22. https://teconologia.libero.it/
23. https://chietitoday.it/
24. https://cybersecnatlab.it/
25. https://cyware.com/
26. https://medium.com/
27. https://reporterpress.it/
28. https://agi.it/
29. https://csoonline.com/
30. https://cert-agid.it/
31. https://csirt.gov/
32. https://www.difesaesicurezza.com/
33. https://www.ilsole24ore.it/
34. https://www.linkedin.com/
35. https://www.hdmotori.it/
36. https://www.key4biz.it/
37. https://www.cert-agid.gov.it/
38. https://www.ivg.it/
39. https://www.leggo.it/
40. https://yoroi.company/
41. https://www.corriere.it
42. https://www.ferrovie.info
43. https://www.spcnet.eu
44. https://www.trend-online.com
45. https://www.insicurezzadigitale.com

46. https://www.tecnoandroid.it
47. https://www.zeusnews.it
48. https://www.ilsussidiario.net
49. https://smarthome.hwupgrade.it
50. https://www.aboutpharma.com
51. https://www.swascan.com
52. https://www.hdblog.it
53. https://www.lagazzettadelmezzogiorno.it
54. https://leganerd.com
55. https://www.inforisktoday.com
56. https://www.msn.com
57. https://it.sputniknews.com
58. https://tecnologia.libero.it
59. https://techcrunch.com
60. https://hackerjournal.it
61. https://www.money.it
62. https://infopcfacile.it
63. https://it.cointelegraph.com/
64. https://www.ilcrivello.it
65. https://www.smartworld.it
66. https://www.rainews.it
67. https://www.ilrestodelcarlino.it
68. https://www.china-files.com
69. https://corrierealpi.gelocal.it
70. https://www.zoom24.it
71. https://www.nordmilano24.it
72. https://www.lanazione.it/
73. https://www.ilmessaggero.it
74. https://www.mediasetplay.mediaset.it
75. https://www.ictbusiness.it
76. https://www.upguard.com/
77. https://www.techradar.com
78. https://tech.fanpage.it
79. https://www-swascan-com.
80. https://computerweekly.it
81. https://www.helpmetech.it
82. https://www.adnkronos.com
83. https://www.hwupgrade.it
84. https://www.improntaunika.it
85. https://www.laleggepertutti.it
86. https://cyware.com
87. https://twitter.com/securityaffairs
88. https://twitter.com/Slvlombardo
89. https://twitter.com/faffa42
90. https://twitter.com/zlab_team
91. https://twitter.com/_odisseus
92. https://twitter.com/SofiaSZM
93. https://twitter.com/CSDistrict
94. https://www.securityinfo.it

95. https://www.redhotcyber.com
96. https://tech.everyeye.it
97. https://www.corrierecomunicazioni.it
98. https://quifinanza.it
99. https://www.formulapassion.it
100. https://www.corriereromagna.it
101. https://www.tomshw.it
102. https://www.veneziatoday.it
103. https://gamerant.com
104. https://leganerd.com
105. https://dday.it
106. https://english.kyodonews.net
107. https://www.laprovinciacr.it
108. https://www.securityopenlab.it
109. https://www.361magazine.com
110. https://content.upguard.com
111. https://www.itnews.com.au
112. https://twitter.com/ErmesCyberSec
113. https://www.matricedigitale.it