Exprivia Threat Intelligence Report

Italia – 2022

future. perfect. simple.

Sommario

Indice delle figure

Indice delle figure - Approfondimenti

Indice delle tabelle

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 31/12/2022. Eventuali dati la cui evidenza è successiva a questa data possono non essere oggetto dell'analisi in questione.

Executive Summary

Nel corso del 2022 abbiamo osservato un progressivo diminuire degli attacchi. Le buone notizie finiscono qui. Infatti, nel corso del 2021 e 2022 in Italia abbiamo osservato una progressiva riduzione della forbice tra attacco e difesa (con qualche piccola eccezione, ad esempio 3Q2022) che culmina nel 4Q2022 con un numero di incidenti superiore al numero di attacchi. Non sorprende pertanto che i malware più utilizzati sono trojan e banking trojan, seguiti da botnet. Insomma, malware che creano dipendenza della vittima dall'attaccante per un periodo lungo. Il fenomeno è ancor più preoccupante se si confronta il numero di incidenti nel 4Q2021 con il numero di incidenti nel 4Q2022. Il dato suggerisce che non solo la forbice si apre, ma anche il numero di incidenti anno su anno aumenta di quasi un terzo. Non va, inoltre, sottovalutato il fatto che il 4Q2021 è stato seguito dal 1Q2022 in cui il numero di incidenti è raddoppiato. Il 2022 passa alla storia come l'anno in cui per la prima volta un conflitto tra stati ha visto le parti combattere anche nell'ecosistema digitale anche se tramite organizzazioni transnazionali. Perlomeno la prima volta che un fenomeno di questo tipo ha avuto una grande attenzione mediatica a seguito di una sempre maggiore dipendenza della società dalla digitalizzazione di processi e servizi. Malgrado la grande attenzione mediatica, il numero di incidenti ed attacchi connessi al conflitto resta statisticamente non fortemente rilevante o perlomeno non rilevante quanto il fattore umano. Per cui se da un lato nel 2020, 2021 e 2022 abbiamo osservato che qualunque evento imprevisto (guerra, pandemia…) ha spesso un impatto nell'ecosistema digitale, dall'altro ad impattare realmente la stabilità dell'ecosistema stesso è la mancanza di consapevolezza della popolazione. La tecnica di attacco più spesso utilizzata resta il phishing talvolta sofisticato ma spesso anche banale e facilmente riconoscibile.
Cresce l'Investment Index su tutto il territorio nazionale e per la prima volta abbiamo un valore quasi comune sia al nord che al centro ed al sud. La messa in sicurezza dei servizi digitali sembra vedere tutto il territorio nazionale muoversi con la stessa velocità.
Diminuiscono anche i dispositivi IoT esposti direttamente su internet e le loro vulnerabilità più comuni sul territorio nazionale con un lieve ritardo per il sud Italia.

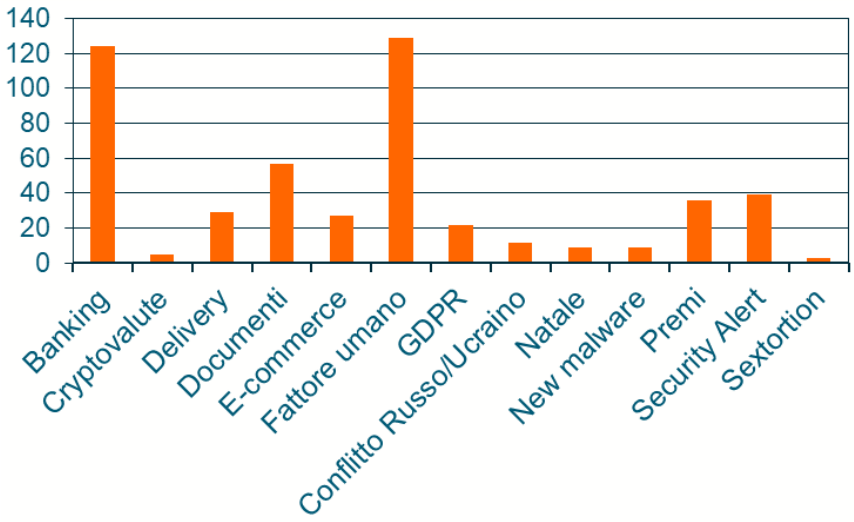

Figura 1 - Tematiche riscontrate di attacchi, incidenti e violazioni privacy nel 2022 in Italia

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 l'andamento del 2022 evidenziando un trend pressoché altalenante degli attacchi, incidenti e 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, incidenti e violazioni privacy, infatti, attraverso l'utilizzo di tecniche sempre più complesse, continua ad essere continuamente più difficile identificare in maniera efficace i cybercriminali.
L'inizio del 4Q2022 parte con un numero nettamente inferiore di casi registrati in tutto il 2022, precisamente 130. Questa evidenza faceva ben sperare, ma dopo un aumento del 23% nel mese di novembre (160), si registra un ulteriore incremento del 98% nel mese di dicembre (257), rispetto al mese di ottobre, rendendolo il mese con il più alto numero di casi registrati, dopo marzo e maggio.
Il 2022 è indubbiamente l'anno più complesso in termini di sicurezza, le aziende continuano a adeguare la propria modalità di lavoro a quella agile. In virtù di ciò i dispositivi utilizzati per il lavoro smart e quelli di rete (non sempre sicuri) offrono numerose possibilità agli attaccanti di trovare dei punti deboli per sferrare i propri attacchi.

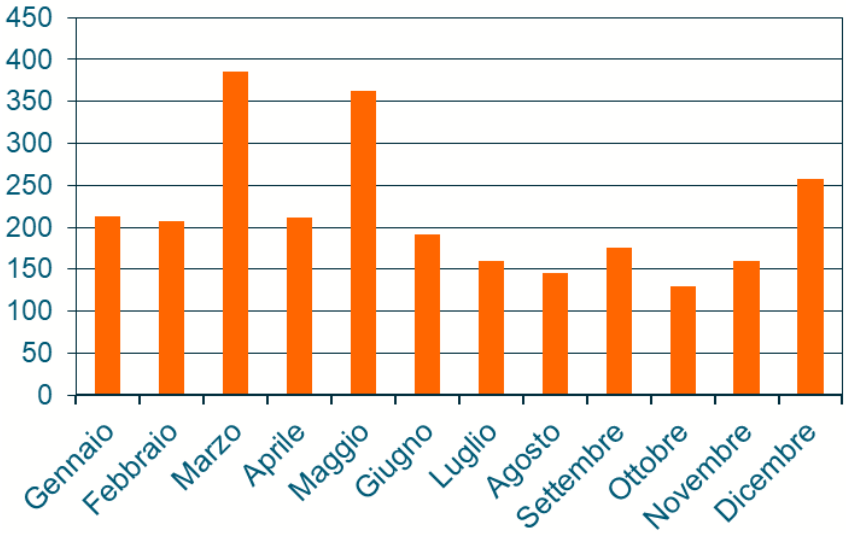

Figura 2 - Numero di attacchi, incidenti e violazioni privacy suddivisi in mesi in Italia nel 2022

Continua il percorso di crescita degli attacchi, incidenti e violazioni privacy. Questo è confermato dalle variazioni annuali, sia cumulate che sullo stesso trimestre, come pure dalle variazioni di momentum. Il dato più eclatante che si può osservare è quello che misura l'incremento annuale dei casi di sicurezza dell'intero 2022, sono ben 2600, che si raffronta con il totale cumulato nell'anno 2021 (1356). Si nota così un trend di crescita del 92%. Questo si manifesta anche sullo stesso periodo oggetto di analisi, il 4Q2022 rispetto al 4Q2021, ed è pari al 21%. Infine, si segnala la crescita del volume dei casi di sicurezza anche rispetto ai dati più recenti: il totale dei casi registrati nel trimestre 4Q2022, son ben 547, mentre quelli raccolti nel Exprivia Threat Intelligence Report 3Q2022, erano 481.

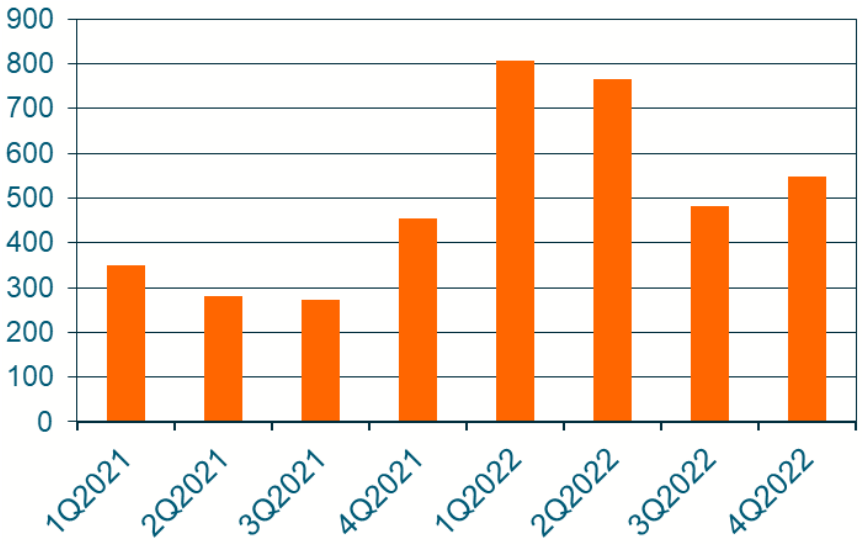

Figura 3 - Numero di attacchi, incidenti e violazioni privacy nel 2021, 2022 in Italia

Nel corso del 2022 sono stati registrati precisamente 1236 attacchi, 1261 incidenti di sicurezza e 103 violazioni privacy.
Rispetto al 2021 per attacchi, incidenti e violazioni privacy si analizza un incremento (+37 % attacchi, +209 % incidenti e +114 % per la violazione della privacy).
Tuttavia, un elemento di particolare rilevanza riguarda l'aumento degli incidenti di sicurezza a discapito degli attacchi informatici: i primi superano per la prima volta i secondi. Questa situazione confrontandola con le analisi effettuate negli anni precedenti evidenzia un drastico peggioramento dello stato della sicurezza informatica nel territorio italiano.
Questi dati fanno riflettere non solo sulle tecniche di attacco, diventate sempre più efficaci, ma anche sulla necessità di investire maggiormente nella cyber security che attua strategie di prevenzione e difesa dagli stessi.

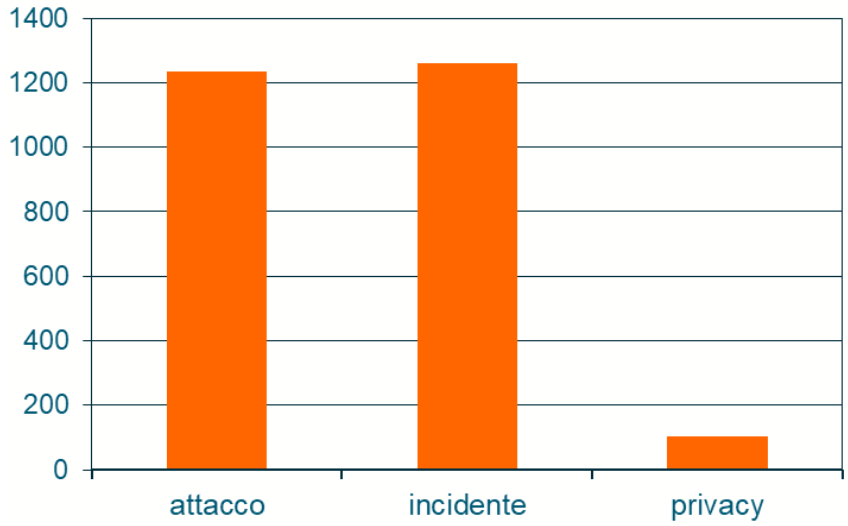

Figura 4 - Numero di attacchi, incidenti e violazioni privacy nel 2022 in Italia

Il grafico sottostante riporta il numero degli attacchi, incidenti e violazioni privacy registrati in Italia nel biennio 2021/2022. Relativamente al primo semestre del 2022, si evidenzia un picco delle attività malevole perpetrate dai Cyber criminali. Analizzando i dati raccolti nell'ultimo trimestre del 2022 e confrontandoli con l'equivalente trimestre dell'anno precedente, si rileva un aumento complessivo del 20% delle attività di Cybercrime.
Analizzando in dettaglio i dati raccolti per gli ultimi due trimestri del 2022, gli attacchi evidenziano un calo del 22%, ed una diminuzione del 20% se si confrontano gli ultimi quarter dei due anni oggetto di analisi. I dati degli incidenti registrano una percentuale del +58,4% rispetto al 4Q2021 e +57,6% rispetto al 3Q2022. Quanto alle violazione privacy si osserva un aumento del 15% rispetto al 3Q2022 ma confrontando lo stesso dato con il 4Q2021 si nota un balzo delle violazioni privacy pari al 343%.

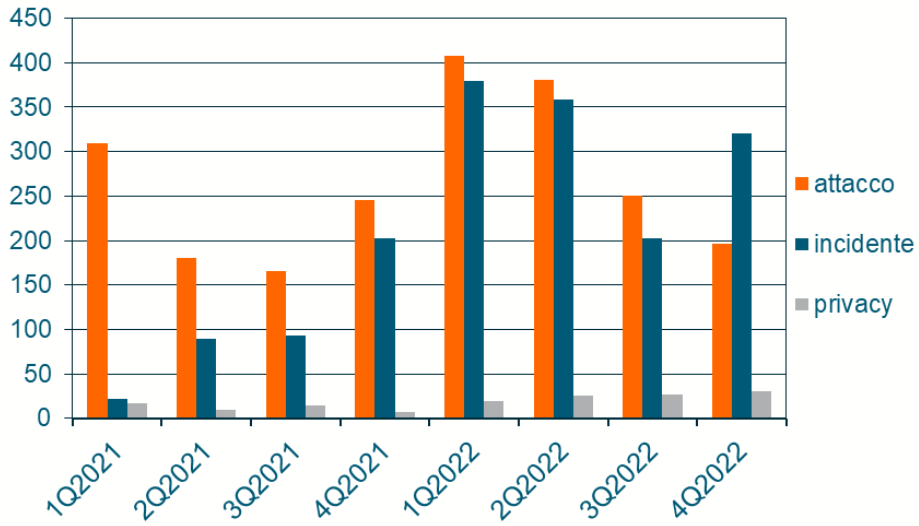

Figura 5 - Numero di attacchi, incidenti e violazioni privacy nel 2021, 2022 in Italia

Motivazione degli attaccanti

Il numero dei fenomeni rilevati per l'anno 2022, ben 2600 sembra confermare la tendenza al raddoppio di anno in anno, difatti per l'anno 2020 l'Osservatorio Cybersecurity di Exprivia rilevava 605 casi, e per il 2021 1356 eventi.
Dall'analisi delle motivazioni emerge che su un totale di 2600 casi, oltre l'80% è riconducibile ad attività criminali, quindi, reati informatici perpetrati attraverso l'ausilio di tecniche e strumenti acquisibili in rete (ad esempio nel Dark Web esiste una vera e propria industria del Malware come le piattaforme di malware-as-a-service), a seguire il 6,8% con 177 casi legati ad hacktivism, a seguire con il 6% casi attribuibili a cyber warfare, il restante 4% legato al data breach ed infine il 2,4% di casi legati a questioni di spionaggio e sabotaggio. Il cybercrime per l'intero 2022 costituisce la motivazione principale che porta gli attaccanti ad agire e a compiere azioni malevole in modo sempre più sofisticato ed efficace.

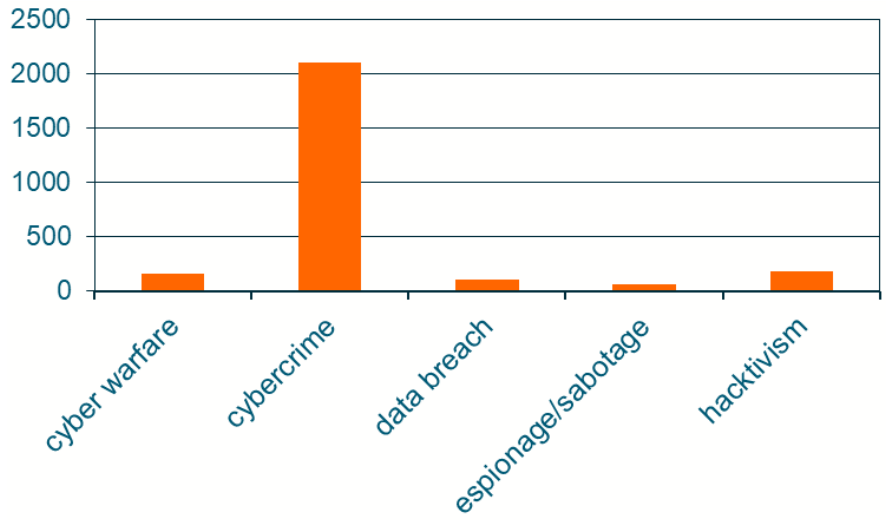

Figura 6 - Conteggio motivazione attacchi, incidenti e violazioni privacy per tipologia nel 2022 in Italia

Come si può notare dal grafico sottostante, negli ultimi sette trimestri è stato il Cybercrime a costituire la maggioranza delle motivazioni dietro gli attacchi, gli incidenti e le violazioni della privacy il cui trend è aumentato significativamente nel 1H2022. Nello specifico, rispetto al 2021 si è registrato un incremento di circa il 73% nel 2022 di attività legate al Cybercrime.
A partire dal 2022, a seguito dei nuovi conflitti bellici dei quali la Russia si è fatta protagonista, si è aggiunto alla lista delle motivazioni il cyber warfare che ha visto un incremento esponenziale con ben 157 fenomeni registrati.
A seguire si registrano fenomeni quali data breach, hacktivism ed espionage/sabotage. Di particolare rilevanza l'incremento delle attività di hacktivism (attività criminali al fine di promuovere una causa politica o sociale) aumentate del 139% rispetto al 2021.

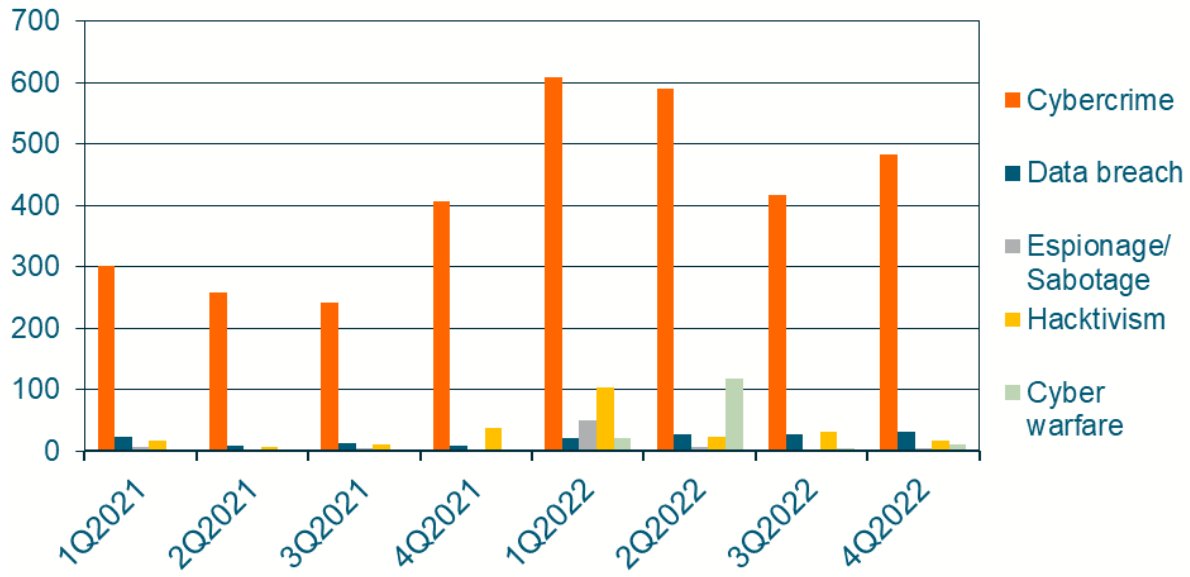

Figura 7 - Conteggio motivazione attacchi, incidenti e violazioni privacy nel 2021, 2022 in Italia

Distribuzione geografica

Al contrario di quanto si possa pensare, i casi di sicurezza avvenuti durante tutto l'arco del 2022 mostrano una certa omogeneità su tutta l'Italia, con una leggera preponderanza nelle regioni del centro-nord. Poco distaccato il sud Italia che registra un numero leggermente inferiore. Nello specifico sono 2323 i fenomeni registrati nel nord Italia, 2311 al centro e 2184 al sud. Un numero complessivo particolarmente elevato, pari ad una media di circa sei attacchi al giorno per regione, a dimostrazione del fatto che il nostro Paese resta uno degli obiettivi sensibili più minacciati da questo tipo di fenomeni.

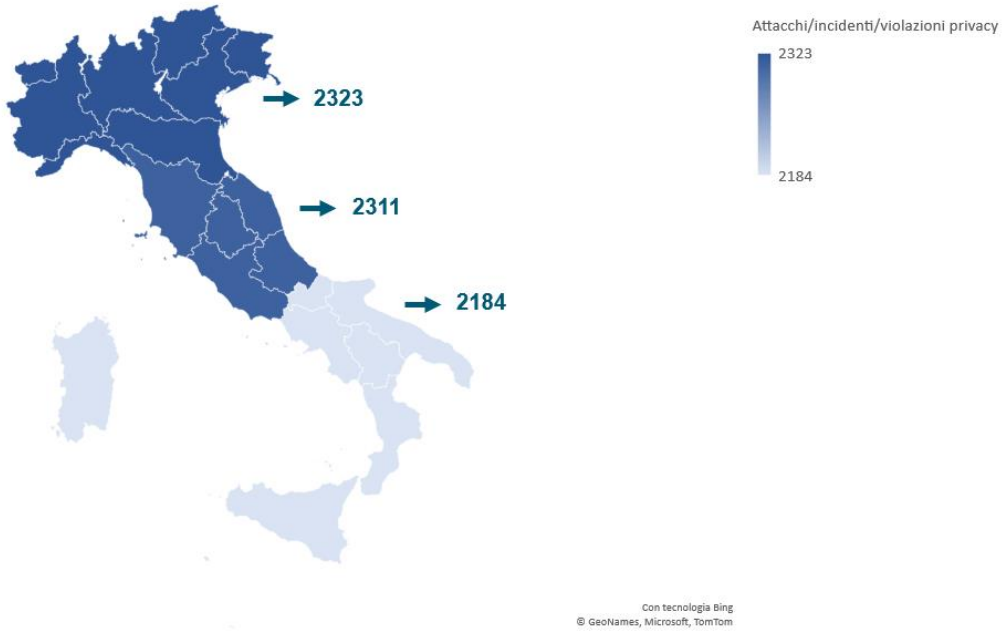

Figura 8 - Distribuzione geografica attacchi, incidenti e violazioni privacy nel 2022 in Italia

Distribuzione vittime per Industria

Appartiene al settore Finance il maggior numero di vittime di attacchi portati a compimento nel corso del 2022, precisamente 939 vittime (36%).
Il numero importante di vittime potrebbe essere dovuto al fatto che le aziende finanziarie gestiscono grandi quantità di dati sensibili e denaro, rendendole un obiettivo attraente per gli attaccanti. Inoltre, il settore finanziario è altamente regolamentato e le conseguenze di una violazione della sicurezza possono essere molto severe, sia in termini di sanzioni che di danni alla reputazione.
Il secondo settore maggiormente colpito è il Software/Hardware con 343 vittime (13%).
Seguono Industria, Pubblica Amministrazione, Retail che si confermano come settori altrettanto vulnerabili con numeri di vittime importanti (circa 300).
Gli altri settori si attestano intorno le 100 vittime.
Colpiscono infine, seppure siano attacchi esigui in numero, le vittime del settore ONG e del settore Religion.
Per quanto riguarda la Pubblica Amministrazione gestisce molti dati sensibili dei cittadini e ha responsabilità importanti nell'amministrazione dello Stato, quindi, può essere un target per i cybercriminali. Spesso le tecnologie utilizzate sono datate e i sistemi obsoleti, dunque, possono essere meno sicuri rispetto alle soluzioni più aggiornate. È importante che le aziende finanziarie e la Pubblica Amministrazione investano in robuste misure di sicurezza per proteggere i propri sistemi informativi nonché i dati dei clienti e quelli dei cittadini.

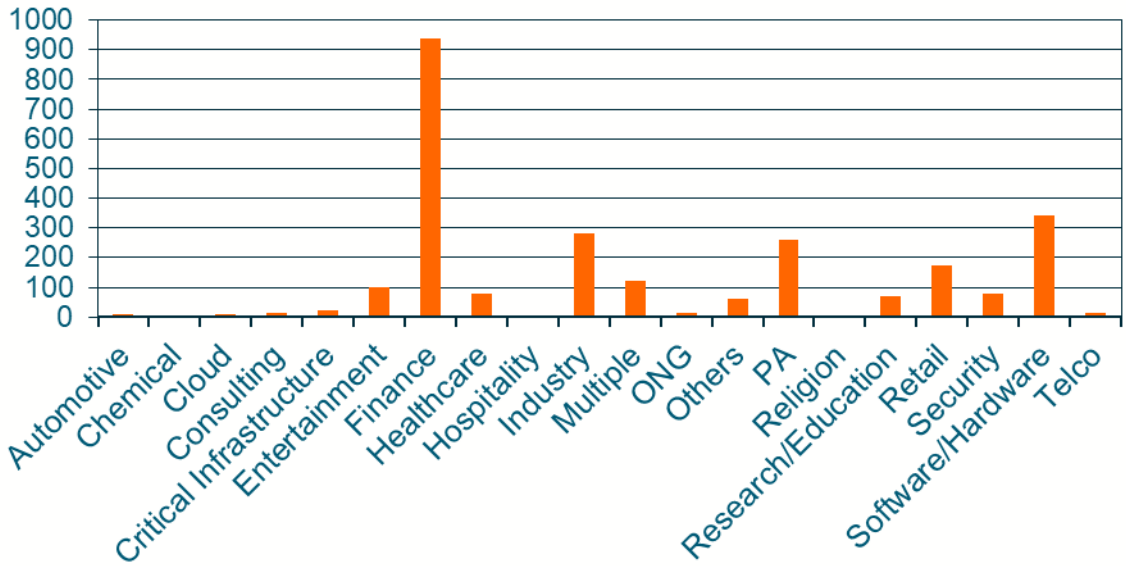

Figura 9 - Tipologia vittime di attacchi, incidenti e violazioni privacy nel 2022 in Italia

Finance

In ambito finanziario, l'andamento degli attacchi registrati durante il corso dell'anno 2022 presenta dei picchi importanti nella prima metà dell'anno, sicuramente alimentati dalle dinamiche geopolitiche internazionali. Il settore in questione è stato messo a dura prova dal conflitto russo-ucraino e ci si aspettava fin da subito un andamento particolarmente ascendente durante tutto il corso dell'anno. Si registra, tuttavia, dopo un netto picco estivo, che il numero totale di attacchi sia leggermente diminuito a partire da agosto fino a stabilizzarsi durante la parte finale dell'anno.
In dettaglio, si registra un calo pari a circa il 46% delle attività malevole tra il 1H2022 e il 2H2022.
Le istituzioni finanziarie tendono ad essere target particolarmente colpiti dal cybercrime. Spesso infatti gli istituti bancari, quelli assicurativi, aziende che forniscono pagamenti digitali e le piattaforme di criptovalute sono al centro degli interessi criminali in quanto possibili fonti di accesso a risorse economiche immediate.

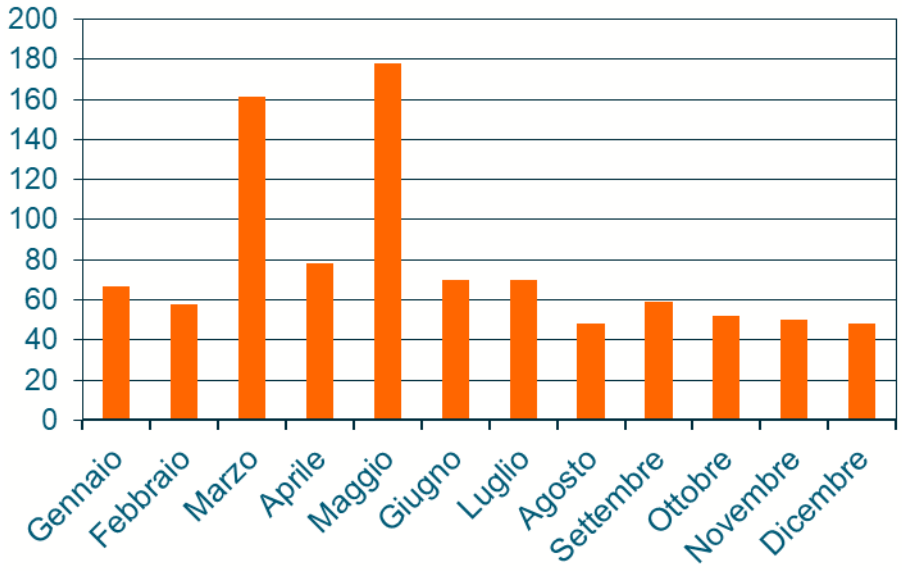

Figura 10 - Attacchi, incidenti e violazione privacy del settore Finance in Italia

Software/Hardware

L'anno 2022 ha visto un marcato aumento degli attacchi informatici alle società di sviluppo software. Questa tendenza è stata particolarmente evidente durante i mesi di gennaio, febbraio, marzo, aprile e maggio. Durante questi mesi ci sono stati numerosi tentativi di violazione dei sistemi di sicurezza rispetto a qualsiasi altro periodo dell'anno.
Nei mesi di gennaio e febbraio si sono osservati 21 tentativi di attacco. A marzo, tuttavia, questo numero è balzato vertiginosamente con 49 casi appartenenti a società di sviluppo software. I numeri di aprile e maggio hanno seguito l'esempio con 20 e 63 casi registrati rispettivamente, indicando una tendenza allarmante verso l'aumento degli attacchi informatici su questo tipo di aziende per tutto il 2022.
Non è chiaro il motivo per cui gli attaccanti abbiano scelto questo particolare momento come loro obiettivo, ma potrebbero aver approfittato di un periodo in cui molte organizzazioni sono concentrate sullo sviluppo di nuovi prodotti o servizi che possono risultare vulnerabili.
Molti software vengono distribuiti su una vasta gamma di dispositivi e sistemi operativi, rendendoli potenzialmente vulnerabili a exploit noti o zero-day.

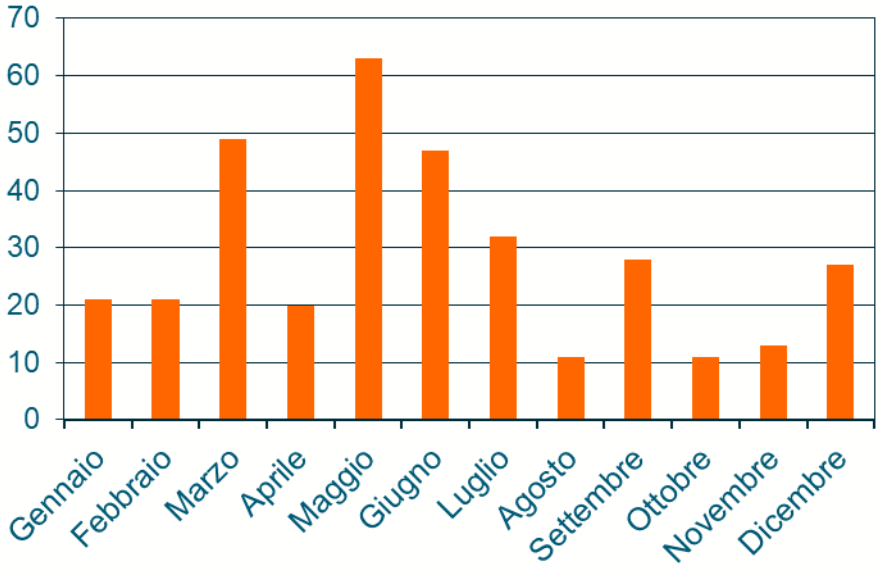

Figura 11 - Attacchi, incidenti e violazioni privacy del settore Software/Hardware in Italia

Industria

Il settore dell'industria, nel 2022, è al terzo posto nella speciale classifica dei settori maggiormente colpiti con ben 280 casi registrati. A partire da gennaio si può notare un andamento altalenante dei casi di sicurezza; nei primi quattro mesi del 2022 assistiamo ad un trend in aumento del numero di attacchi, incidenti e violazioni privacy che tende a decrescere vistosamente nei mesi di maggio e giugno per poi aumentare nuovamente dal mese di luglio fino a novembre. Il 2022 si chiude con lo stesso numero di casi registrati ad inizio anno, infatti, sia nel mese di dicembre che a gennaio sono stati segnalati 23 fenomeni.
Nel 4Q2022 l'incremento registrato è pari al 30% rispetto al quarter precedente, infatti, il mese di novembre risulta essere il secondo mese peggiore dell'intero 2022, dopo aprile, in termini di casi di sicurezza.
Questa tendenza dovrebbe far riflettere gli operatori di questo settore dal momento che gli attacchi rivolti verso l'industria possono essere molto critici ed avere impatti particolarmente rilevanti non solo a livello di perdite finanziarie ma anche a livello reputazionale, di interruzioni di attività e di perdita di informazioni aziendali.

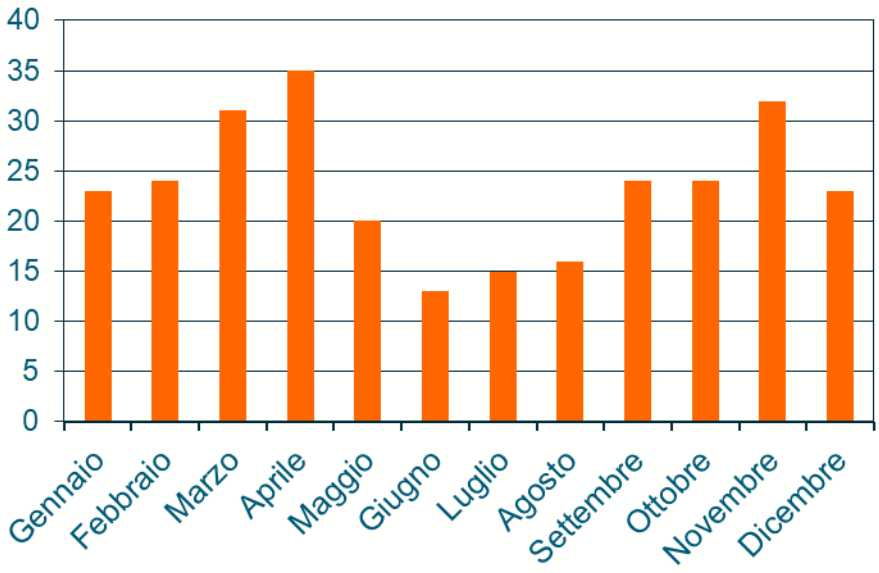

Figura 12 - Attacchi, incidenti e violazioni privacy del settore industria in Italia

Pubblica Amministrazione

Il settore della Pubblica Amministrazione coinvolge infrastrutture ed organizzazioni quali istituzioni educative, aziende ed amministrazioni dello Stato, ma anche camere di commercio, industria, artigianato e tutti gli enti pubblici. Diventa quindi immediato comprendere quali siano le motivazioni che inducono cyber criminali ad attaccare questo settore. I numeri del 2022 parlano chiaro: si sono verificati ben 260 casi di sicurezza che hanno colpito il settore delle PA. Ancor più nel dettaglio sono stati registrati 109 casi nel 1Q2022, 47 nel 2Q2022, 48 nel 3Q2022 ed infine 56 nel 4Q2022. Il mese in cui si concentra il maggior numero di casi è marzo, con ben 53 episodi. Si denotano cali fisiologici in alcuni mesi dell'anno ad intervalli regolari, ma l'andamento complessivo è comunque costante e lineare. Da non sottovalutare comunque un lieve rialzo di circa il 17% negli ultimi tre mesi a dimostrazione di come la recente trasformazione digitale e l'introduzione del lavoro agile abbiano portato ad una notevole esposizione al rischio Cyber tutto il settore delle Pubbliche Amministrazioni.

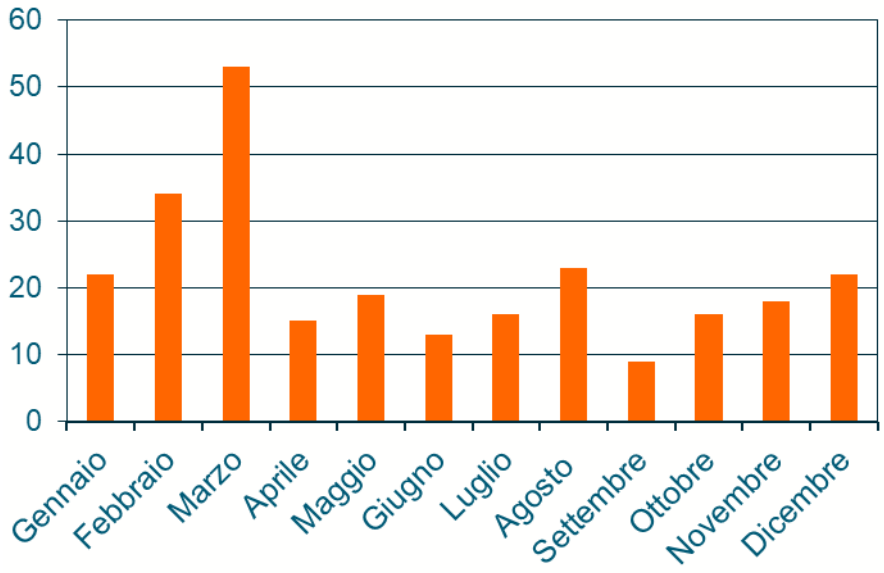

Figura 13 - Attacchi, incidenti e violazioni privacy del settore PA in Italia

Tipo di danno

Categorizzare un incidente informatico in base alla tipologia di danno è estremamente importante, sia per comprendere il contesto dell'attacco, sia per individuarne le tendenze. Come ben sappiamo, perpetrare un attacco informatico non è un banale tentativo di ottenere qualcosa illecitamente, ma spesso cambia motivazioni e target di attacco in base al contesto geopolitico nazionale ed internazionale. Oramai, veri e propri team di attaccanti, sempre più capaci e dotati delle più innovative tecnologie sul mercato non si limitano più a mettere in ginocchio organizzazioni casuali, ma hanno veri e propri pool di target scelti con minuziosa attenzione. Avere a disposizione un conteggio preciso e puntuale di questi attacchi diventa quindi di primaria importanza.
La principale tipologia di danno causato da attacchi informatici, incidenti e violazioni privacy nel corso dell'anno 2022 è senza dubbio il furto dati che caratterizza circa il 70% della totalità delle evidenze acquisite. Non è da sottovalutare il danno economico, il quale risulta associato al 10% degli attacchi informatici individuati e il service interruption (11%).
Di minore rilevanza si osserva privacy (6%).

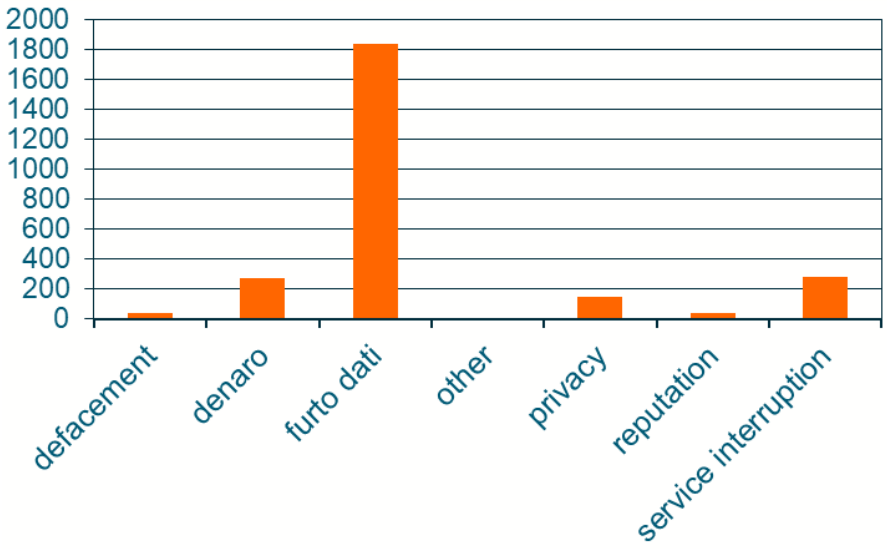

Figura 14 - Tipologia danno di attacchi, incidenti e violazioni privacy nel 2022 in Italia

Il 2022 è stato un anno caratterizzato dal proseguimento lineare e crescente dell'andamento dei 12 mesi precedenti. Continuano ad aumentare i furti di dati, che si portano ora ad una quota di ben 70% sul totale. Di minor entità, ma sempre estremamente rilevanti sono gli attacchi volti ad estorcere denaro o a danneggiare servizi fondamentali per i cittadini e le imprese. A dimostrazione del fatto che se è vero che il denaro resta l'obiettivo primario di questi attaccanti, limitarsi ad esso non è più una prassi.

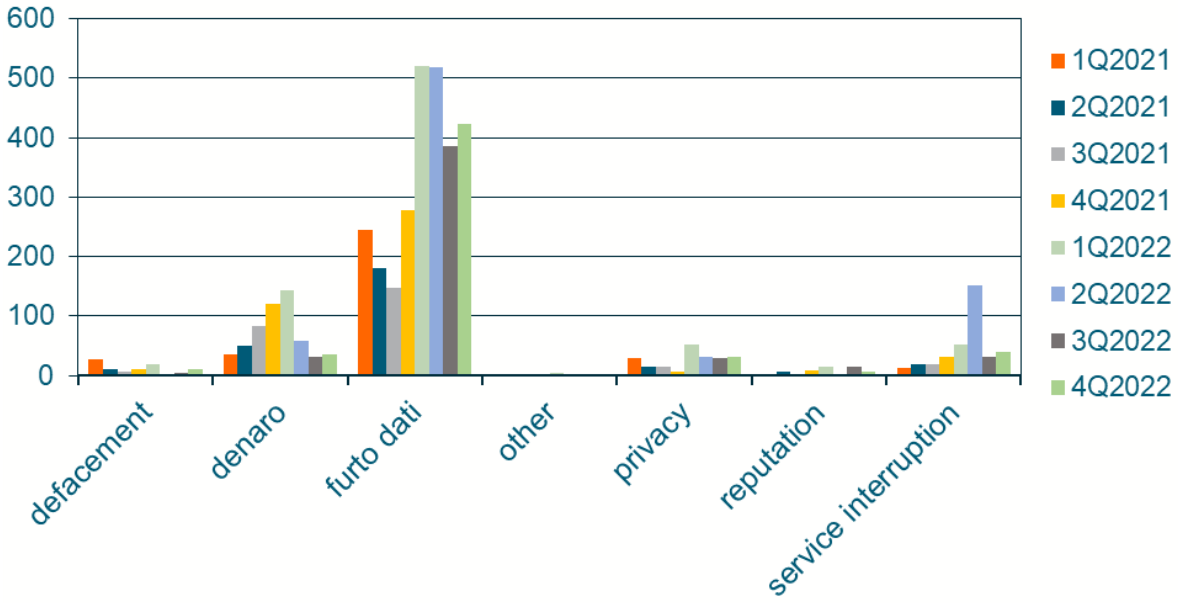

Figura 15 - Tipologia danno di attacchi, incidenti e violazioni privacy nel 2021, 2022 in Italia

Tecniche di attacco

Un attacco informatico è qualsiasi tipo di attacco contro un computer, un sistema informatico, un server o un'infrastruttura di rete, utilizzando una varietà di metodi per rubare, modificare o distruggere dati o un sistema informatico. Può essere perpetrato non solo verso organizzazioni private, ma anche contro un'infrastruttura critica, rischiando così di mettere in ginocchio intere economie di paesi.
Di seguito si riportano valori numerici e relativo grafico delle diverse tipologie di attacchi. Nello specifico tre sono gli attacchi maggiormente riscontrati, nell'ordine: Phishing/Social Engineering con 1133 casi totali (circa il 40%), casi relativi ad installazione ed esecuzione di Malware, ora a quota 1030 casi (poco meno del 40%) e infine Vulnerabilità note sfruttate, a quota 8%. Restano invece in numero più contenuto sia gli attacchi di tipo Brute Force, a sottolineare come ormai stia diventando sempre più una pratica obsoleta, sia gli attacchi DDoS, per cui ormai esistono metodi di protezione/mitigazione altamente efficienti.

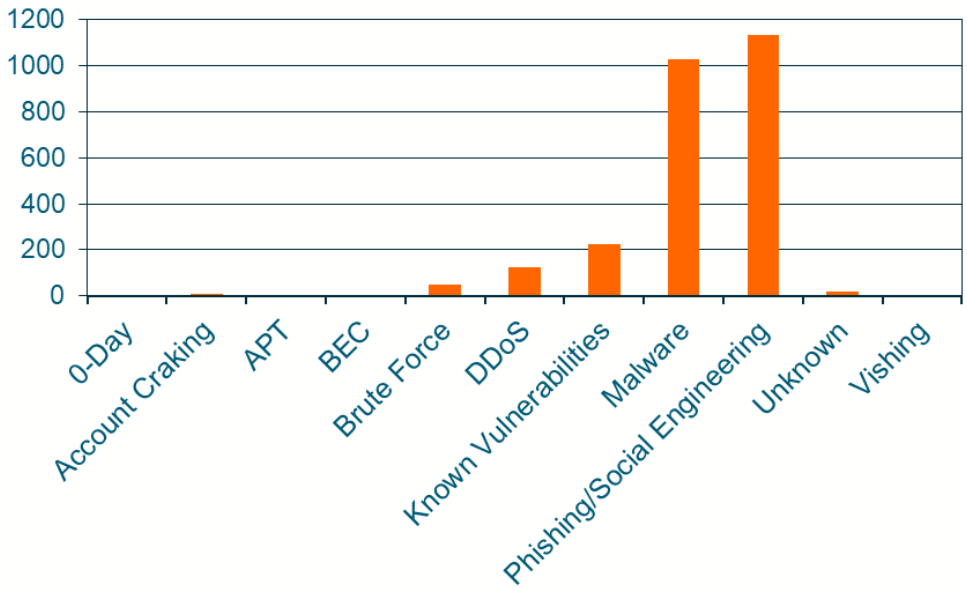

Figura 16 - Tecniche di attacco relative ad attacchi, incidenti e violazioni privacy nel 2022 in Italia

Il 2022 ha visto, rispetto al precedente anno, un aumento generale degli attacchi informatici del 92%.
Durante l'intero 2022 si nota una prevalenza degli attacchi tramite Malware e Phishing/Social Engineering. Entrambe queste tecniche di attacco hanno avuto il loro picco nel 1Q2021, ma negli altri quarti del 2022, gli attacchi registrati tramite queste tecniche sono comunque stati al di sopra della media del 2021.
Rispetto all'anno precedente, gli attacchi messi in atto tramite Malware sono raddoppiati, mentre quelli che coinvolgono campagne di Phishing/Social Engineering sono aumentati dell'86%.
Un importante aumento da segnalare è quello della tecnica DDoS, passata da 7 casi nel 2021 a 126 casi nel 2022, la quasi totalità dei quali è stata rilevata nel 2Q2022.
Anche gli attacchi tramite vulnerabilità note sono aumentati dal 2021. Si registrano infatti 116 casi nel 2021 e 224 casi nel 2022, con un picco nel 4Q2022 (153 casi registrati).

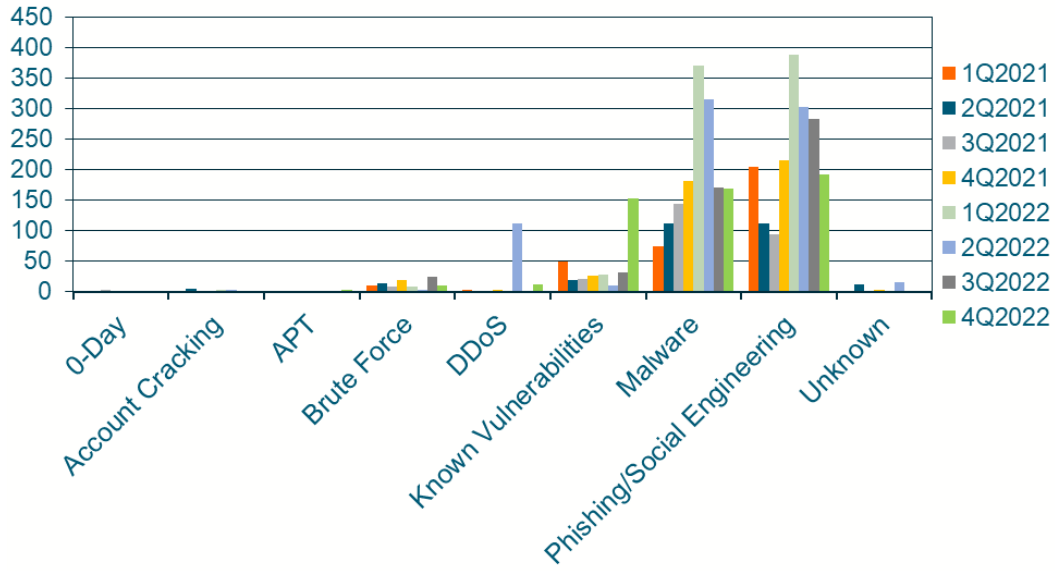

Figura 17 - Tecniche di attacco relative ad attacchi, incidenti e violazioni privacy nel 2021, 2022 in Italia

Nome e tipo di malware

Analizzando il grafico sottostante, si può notare in seguito a una dettagliata analisi, la presenza di quattro classi di malware ovvero, Trojan (346), botnet (213), banking Trojan (190) e Ransomware (130). Tuttavia, ciò che desta preoccupazione sono in particolar modo i Trojan, i quali possono trasformare i sistemi informatici in uno zombie al fine di inserire il dispositivo all'interno di una botnet, ossia una rete di computer infettati da Software dannoso in modo da essere controllato in remoto mediante un server C&C. Secondo una classificazione di malware, uno dei Trojan che nell'ultimo periodo ha eseguito attività malevole arrecando danni di reputazione e di compliance è IceID anche conosciuto con il nome di Bokbot, un malware che sfrutta come modello di Business, Malware-as-a-Service (MaaS), un framework in grado di distribuire malware il quale facilita l'attaccante nel condurre attacchi complessi senza la necessità di conoscere tecniche avanzate. Tra le peculiarità di questo malware vi sono la possibilità di propagarsi sulla rete, monitorare le attività del sistema infetto e trafugare informazioni sensibili. Inoltre, presenta un'architettura modulare che è simile a quella adottata dai RAT o dei malware loader, che consente all'attaccante di ottenere il controllo del sistema infetto o di eseguire file binari da remoto. IceID è una delle famiglie malware maggiormente diffuse sul territorio italiano e si candida a prendere il posto del famigerato Emotet, il malware più diffuso al mondo. In ambito mobile, ci sono Anubis (banking trojan per Android), Hydra (banking trojan per sottrarre credenziali finanziarie) e il Malware-as-a-Service (MaaS) AlienBot. Tuttavia, da non sottovalutare, troviamo anche i Ransomware. Essi arrecano 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 un grave disservizio aziendale.

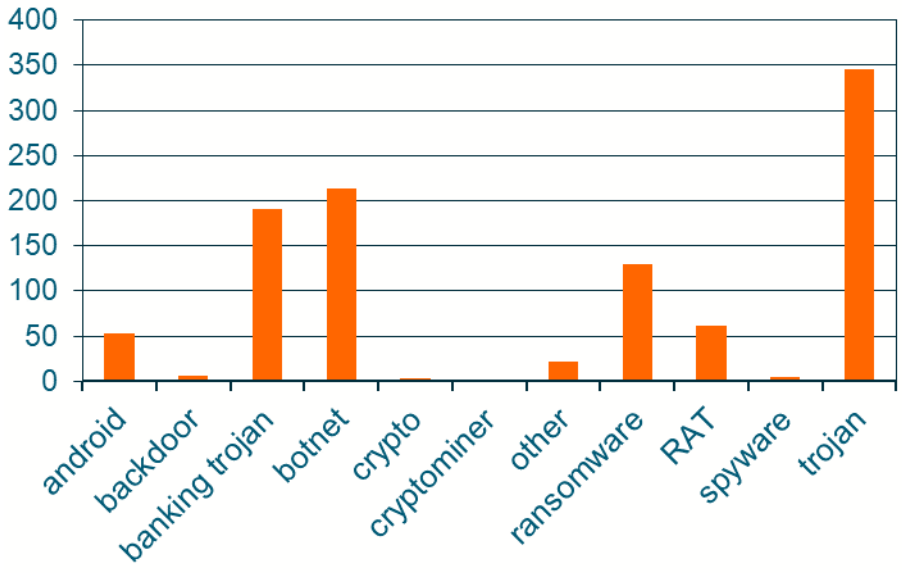

Figura 18 - Tipologie di malware relative ad attacchi e incidenti registrate nel 2022 in Italia

Dal grafico sottostante è possibile riscontrare quali siano le tipologie di malware che hanno causato attacchi nell'intero arco del 2021 e del 2022. In tutto il 2021 ne sono stati conteggiati 591, mentre nel 2022 ne sono stati rilevati 1031 rappresentando un significativo aumento del 43%. I Trojan e i Banking Trojan restano le

due categorie di malware più rilevate nel corso dei due anni con rispettivamente 346 e 190 rilevazioni. Preoccupante come il numero di botnet e ransomware sia cresciuto vertiginosamente, si è passati dai 18 casi di botnet nel 2021 ai 213 nel 2022, mentre per quanto riguarda i ransomware si è osservata una crescita dai 62 casi del 2021 ai 130 del 2022, rappresentando un incremento di circa il 110%.

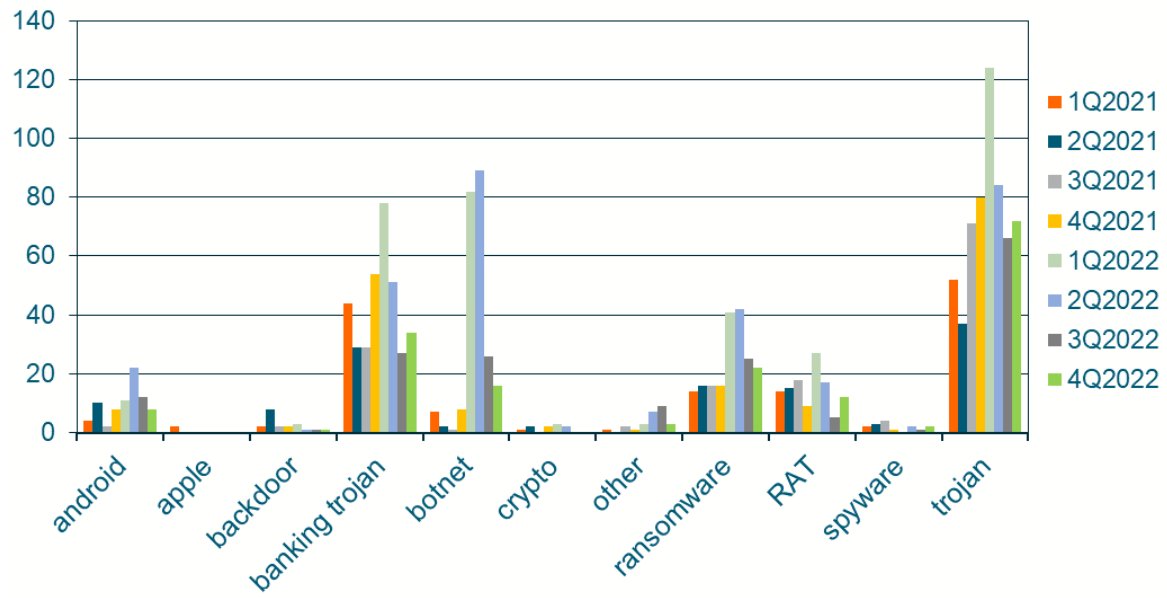

Figura 19 - Tipologie di malware relative attacchi e incidenti registrate nel 2021, 2022 in Italia

Ransomware

I ransomware rientrano tra le categorie più frequenti di virus utilizzati per perpetrare cyber attacchi. Questa tipologia di vettore malevolo è particolarmente nociva in quanto realizzata per impossessarsi del computer di un utente, crittografarne i dati e quindi richiedere un riscatto per ripristinarne il funzionamento.
I dati raccolti durante l'arco dell'anno 2022 mostrano l'andamento degli attacchi di tipo Ransomware che sono avvenuti sul territorio italiano durante gli ultimi 12 mesi.
Dal grafico seguente emerge un andamento lineare e costante di attacchi, con punte di attività in picchi concentrati nel periodo primaverile. Diversa la curva nei periodi estivi, durante i quali le attività malevole sono particolarmente ridotte. Questo modello è dovuto al fatto che gli aggressori traggono vantaggio dalle tendenze stagionali e dalle festività, poiché le organizzazioni e personale coinvolto tendono ad essere meno vigili durante determinati periodi. Inoltre, le aziende mostrano di essere più vulnerabili durante alcuni mesi dell'anno particolarmente delicati come agosto, durante il quale molte risorse sono assenti per ferie e le infrastrutture di rete non efficientemente monitorate.

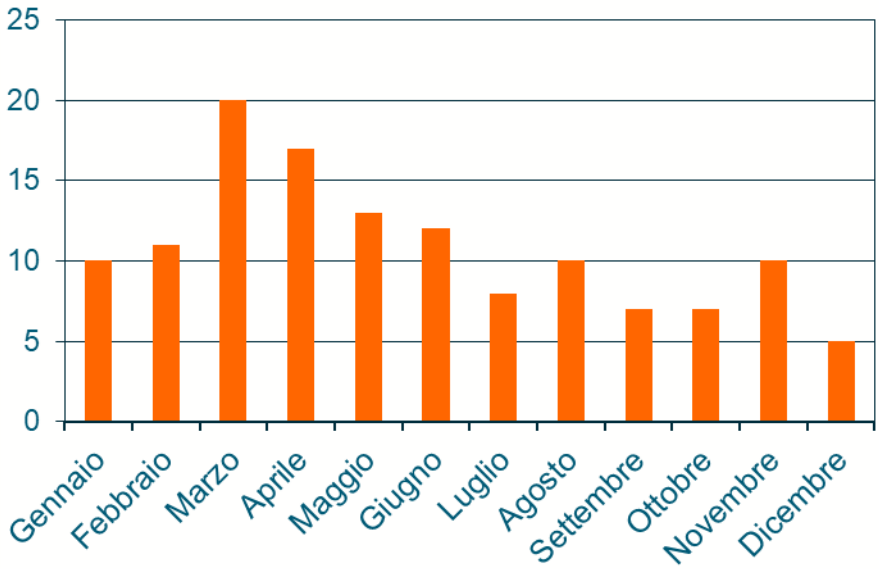

Figura 20 - Ransomware relativi ad attacchi e incidenti registrati in Italia

Trojan

Un virus è un vettore d'attacco che comunemente si moltiplica cercando di infettare file o altri computer diffondendosi nella rete. I trojan, invece, fungono da vera e propria esca con l'obiettivo di nascondersi all'interno dei computer al fine di permettere il trasferimento di malware pericolosi. Per questo motivo, i trojan, possono essere particolarmente pericolosi in quanto attori silenziosi alla ricerca di informazioni sensibili o breach di sicurezza. I dati raccolti descrivono l'andamento dei casi di sicurezza in cui sono stati utilizzati mezzi di attacco che includono un Trojan.
La tendenza dell'anno 2022 mostra come i cybercriminali si siano adattati alle nuove tecnologie e abbiano cercato di sfruttarne le vulnerabilità per ottenere l'accesso a informazioni confidenziali. Si tratta anche della dimostrazione che la consapevolezza degli utenti è sempre più importante quando si parla di proteggere i propri dati da eventualità come attacchi informatici.
Inoltre, è importante notare che mentre il numero totale degli attacchi fosse in diminuzione verso la fine dell'anno rispetto ai primi mesi (da 65 a 17). Questa situazione indicherebbe che i cybercriminali siano diventati più aggressivi nell'utilizzare tecniche avanzate per violare le reti informatiche con lo scopo di rubare dati personali ed economicamente di valore, affidandosi a tecniche più sofisticate rispetto al mero utilizzo di un trojan.

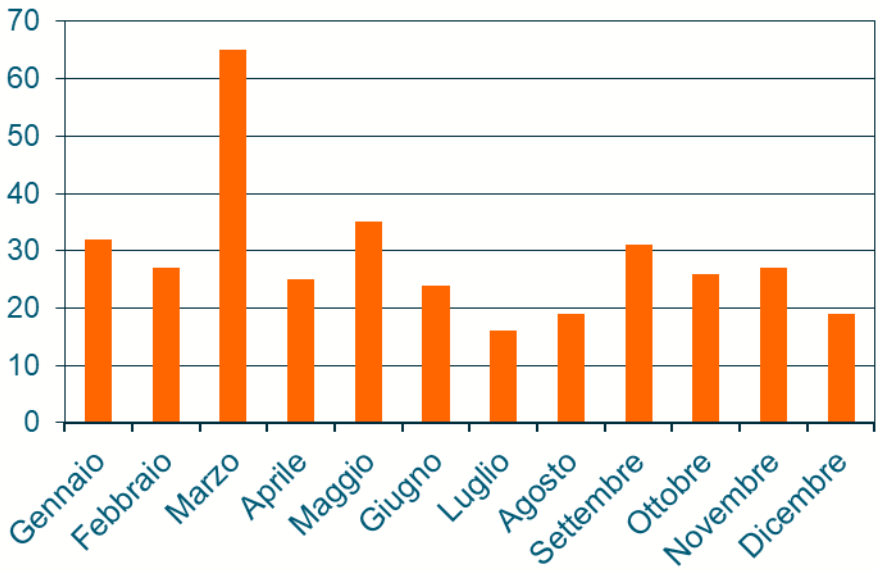

Figura 21 - Trojan relativi ad attacchi e incidenti registrati in Italia

RAT

Un malware che permette l'accesso ad un computer e a tutti i dispositivi ad esso collegati, in via remota, è detto Remote Access Trojan (RAT). Nel corso del 2022 si può notare un vertiginoso aumento di attacchi di questo tipo. Evidenti sono i picchi dei mesi di marzo (13) e aprile (10). Il RAT si serve di una backdoor costituita da tre parti: il server, che in questo caso è installato sulla macchina target, il client che è il device dell'attaccante, lo scanner, inoculato anch'esso sulla macchina target con lo scopo di individuare eventuali servizi sensibili nascosti dietro porte aperte, ossia quegli applicativi che permettono a un device di attivare più connessioni contemporaneamente utilizzate come utili canali di comunicazione. Nel momento in cui lo scanner trova una porta aperta, il client e il server entrano in comunicazione e l'attaccante ha il pieno controllo della macchina target. Attacchi di questo tipo sono particolarmente complessi da portare a termine e spesso vengono individuati da sistemi di difesa come Antivirus. Il numero di questi attacchi, infatti, è ancora relativamente ridotto, ma assolutamente da non sottovalutare data la pericolosità della violazione in caso di successo.

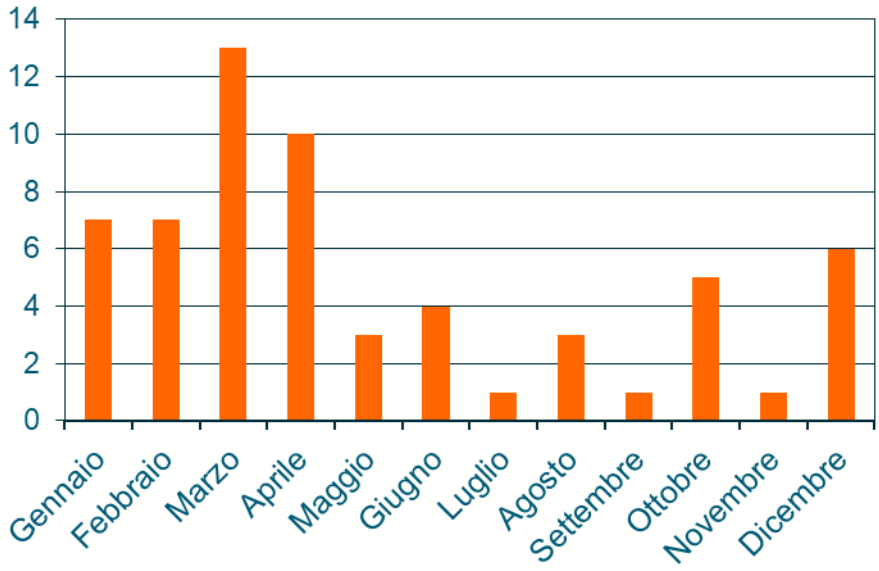

Figura 22 - RAT relativi ad attacchi ed incidenti registrati in Italia

Stato della sicurezza dei dispositivi IoT 4Q2022

In questa rubrica si discute sull'evoluzione della distribuzione dei dispositivi IoT, con riferimento ai dati del 4Q2022. In prima analisi si può notare come i dispositivi IPv4 connessi in rete siano diminuiti di circa l'8%.

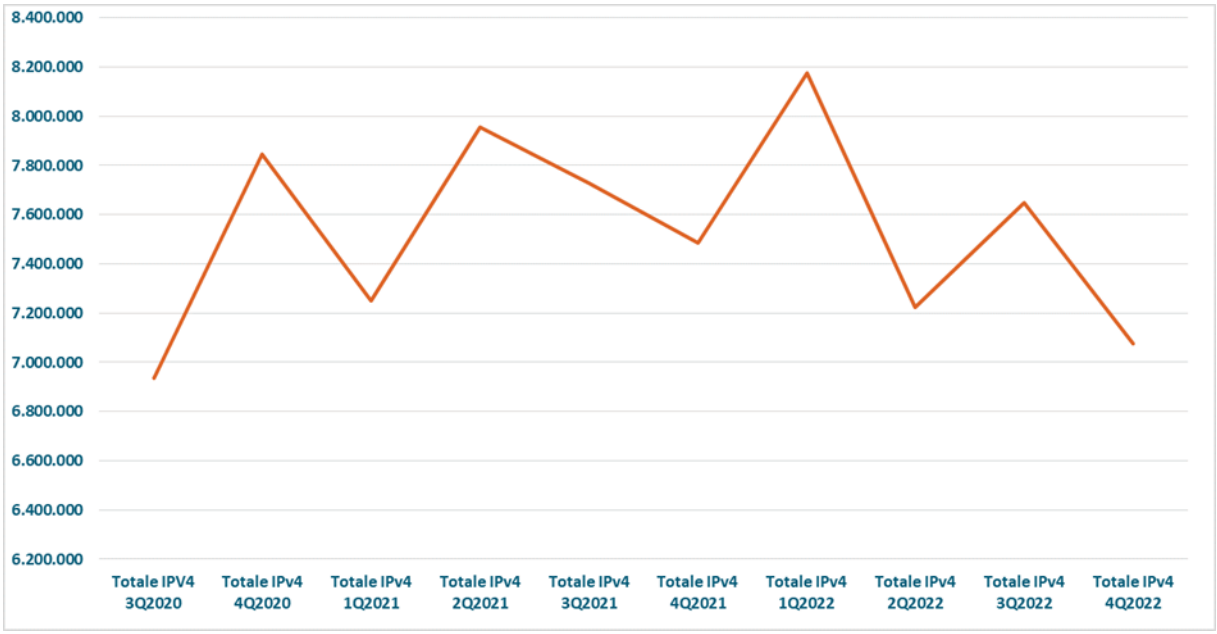

Figura 23 - Situazione italiana dei dispositivi IPv4 3Q2020, 4Q2020, 1Q2021, 2Q2021, 3Q2021, 4Q2021, 1Q2022, 2Q2022, 3Q2022 e 4Q2022

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 4Q2022. Attualmente sono stati individuati 7.075.538 indirizzi IPv4 di cui 112.938 riferiti a:

- telecamere;
- stampanti;
- firewall;
- router;
- VoIP;
- Dispositivi medicali;

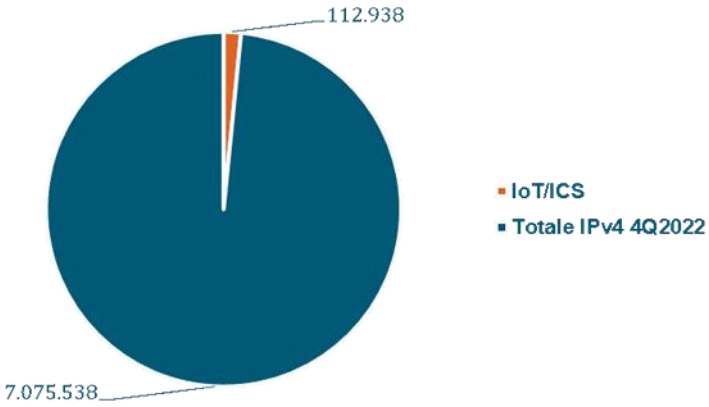

Figura 24 - IoT/ICS vs Others IPv4 4Q2022

Oltre ai dispositivi IoT sono stati individuati 5.583 dispositivi OT. Nel seguente grafico si mostra il numero di dispositivi IT e OT individuati, facenti parte dei 7.075.538.

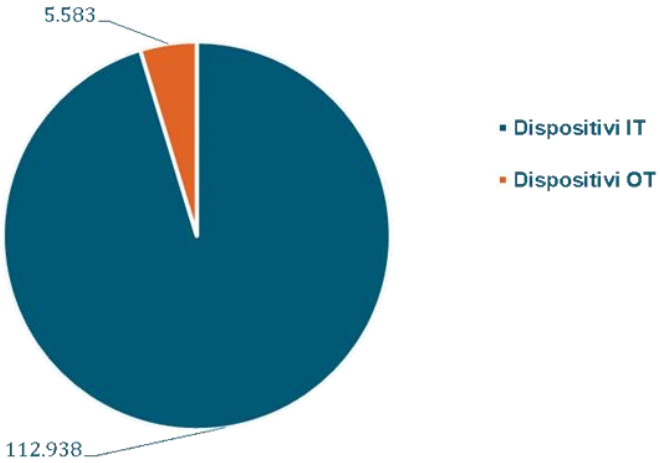

Figura 25 - Dispositivi IT e OT individuati

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.

L’analisi è focalizzata anche sui PLC (Programmable Logic Controller), ovvero computer specializzati nella gestione dei processi industriali. Nel 4Q2022 sono stati rilevati 821 dispositivi, in lieve aumento rispetto agli 819 rilevati nel 3Q2022.
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).

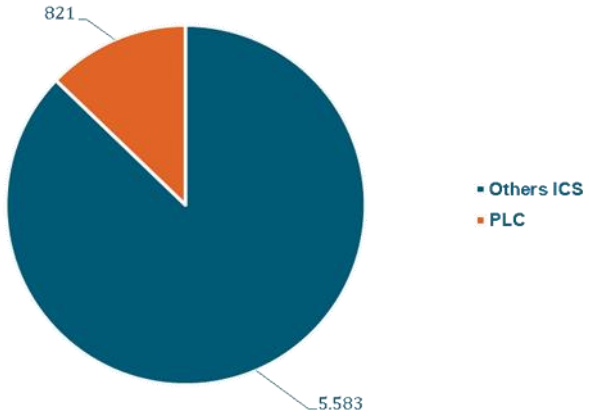

Figura 26 - ICS/PLC individuati 4Q2022

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 decremento dei sistemi industriali rispetto al 3Q2022 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).

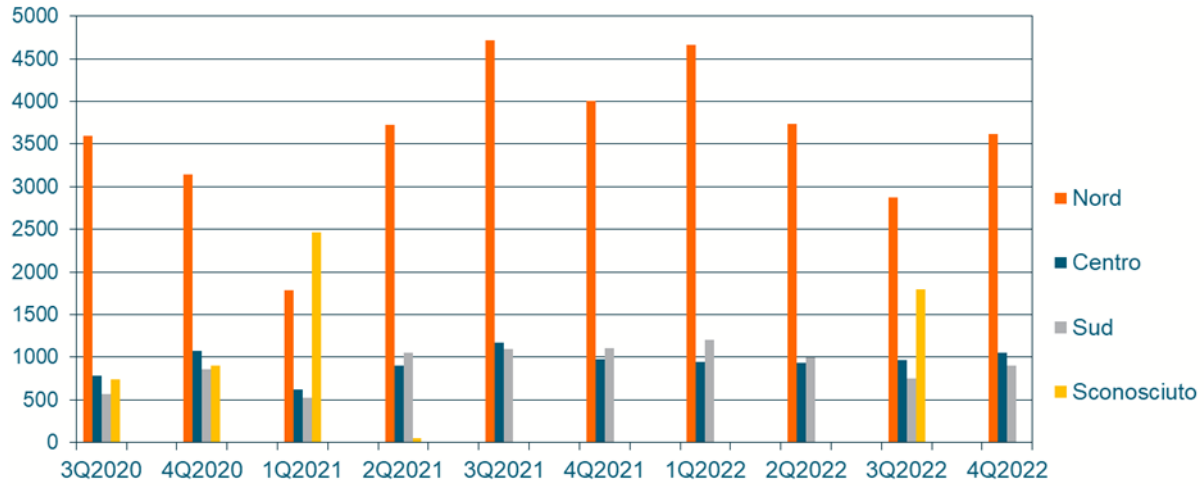

Figura 27 - Sistemi industriali 3Q2020, 4Q2020, 1Q2021, 2Q2021, 3Q2021, 4Q2021, 1Q2022, 2Q2022, 3Q2022 e 4Q2022

La distribuzione degli oltre sette 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, 24.873 i dispositivi individuati, seguita da Lazio (14.380), Campania (11.431) e Veneto (9.528). In fondo a questa particolare classifica la Valle D'Aosta con 114 dispositivi. Sebbene ci sia stato un lieve incremento del numero di dispositivi nelle varie regioni, nel 3Q2022 erano stati rilevati 27.561 dispositivi classificati come sconosciuti non presenti in questo Quarter. Di conseguenza il numero totale di dispositivi esposti è notevolmente diminuito. Questo risultato deve essere accolto positivamente poiché si riflette in un aumento della difficolta da parte di un attaccante nel riuscire ad accedere ai dispositivi esposti.

Figura 28 - - Distribuzione dei dispositivi IoT nelle regioni italiane 4Q2022

Sono stati analizzati anche i dispositivi che utilizzano protocolli privi di autenticazione. In Italia ne sono stati rilevati 4.656 (un decremento di circa il 20% rispetto ai 5.828 rilevati nel 3Q2022) come si evince in Figura 29:

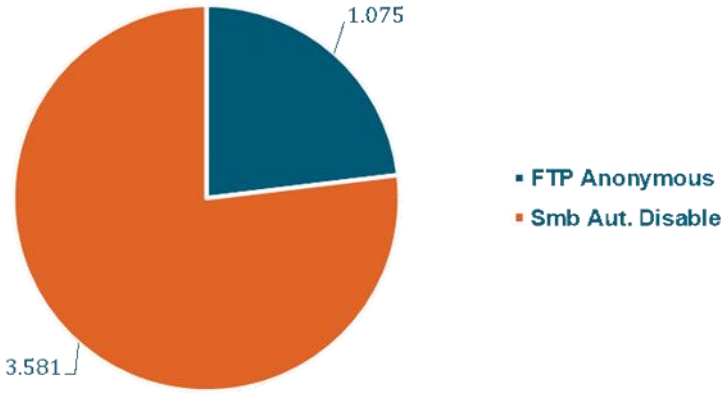

Figura 29 - Protocolli senza autenticazione 4Q2022

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.

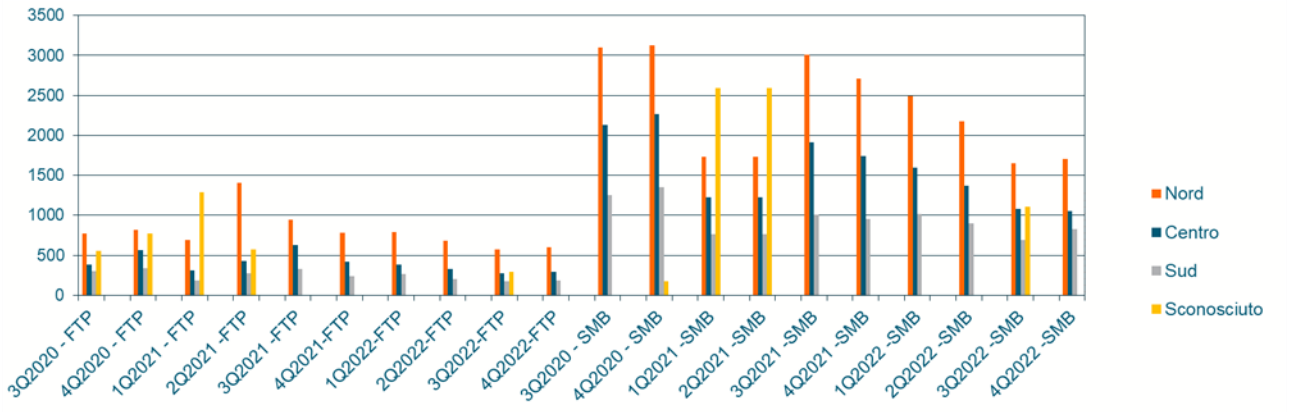

Figura 30 - Distribuzione protocolli senza autenticazione in Italia per area geografica 3Q2020, 4Q2020, 1Q2021, 2Q2021, 3Q2021, 4Q2021, 1Q2022, 2Q2022, 3Q2022 e 4Q2022

Quanto ai grafici relativi alla distribuzione dei dispositivi IoT, si nota che tutti i numeri sono in decremento. Dai dati analizzati, infatti, risulta un decremento di 16.986 telecamere, 1.433 dispositivi medicali, 378 stampanti, 2665 firewall e 129 VoIP ed un incremento di 1.251 router per un totale di 20.340 dispositivi in meno. Secondo l'Osservatorio CyberSecurity di Exprivia, questo decremento dei dispositivi esposti rispetto al 3Q2022, è un bene in quanto decrementa la superfice di attacco. Per quanto riguarda la distribuzione delle telecamere individuate, il primato resta al Nord Italia.
In questo quarter del 2022 sono riportate le analisi effettuate sui sistemi VoIP, iniziate nell'ultimo quarter del 2021. È possibile osservare un'inversione di tendenza rispetto al 3Q2022 che aveva registrato un incremento dei sistemi, rilevando attualmente 334 dispositivi rispetto ai precedenti 463. 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.

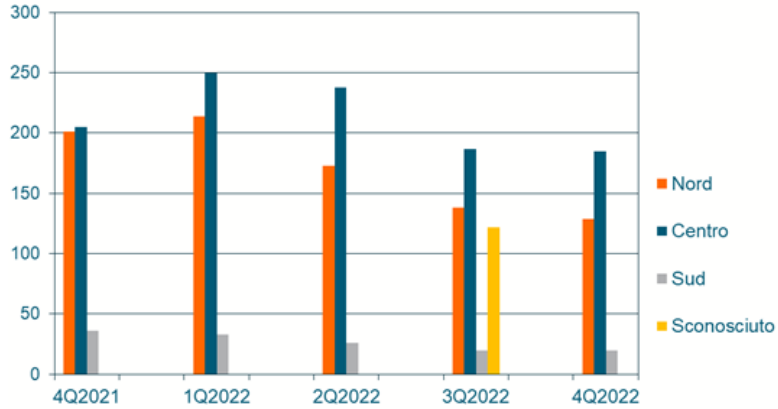

Figura 31 - Distribuzione dispositivi VoIP in Italia per area geografica 4Q2021, 1Q2022, 2Q2022, 3Q2022 e 4Q2022

La distribuzione delle telecamere mantiene sempre il primato nel nord Italia con un decremento rispetto al 3Q2022.

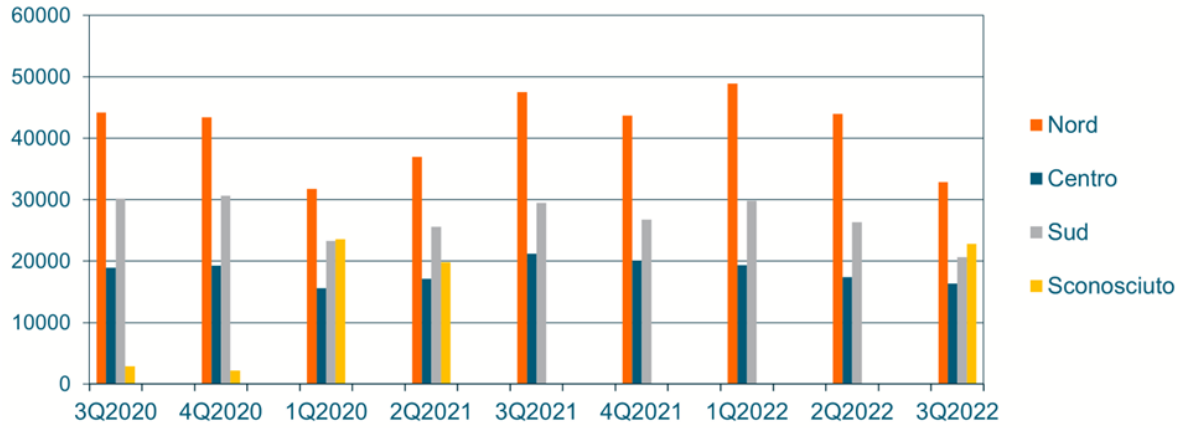

Figura 32 - Distribuzione telecamere in Italia per area geografica 3Q2020, 4Q2020, 1Q2021, 2Q2021, 3Q2021, 4Q2021 e 1Q2022, 2Q2022, 3Q2022 e 4Q2022

La distribuzione delle stampanti mantiene sempre il primato nel nord Italia con un decremento da 225 a 118 rispetto al 3Q2022. Anche nelle aeree del centro e sud Italia il numero di stampanti rilevate diminuisce.

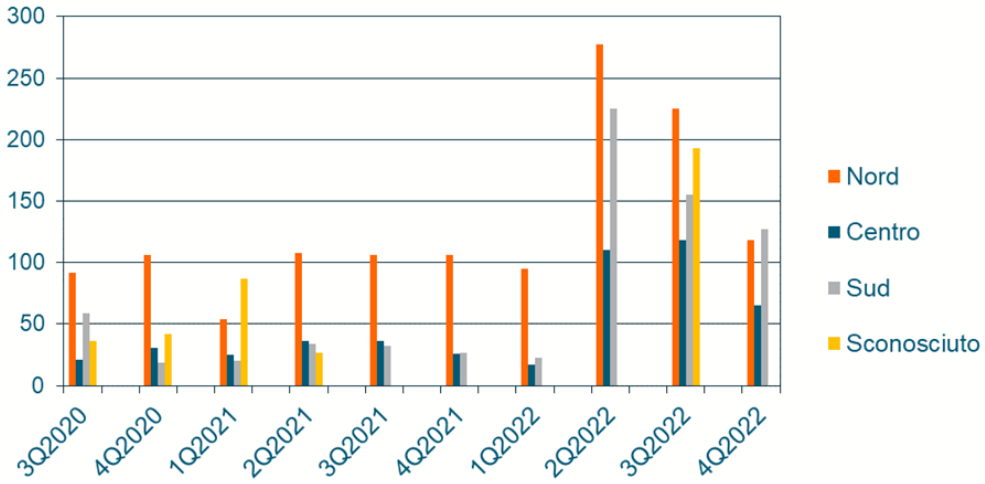

Figura 33 - Distribuzione stampanti in Italia per area geografica 3Q2020, 4Q2020, 1Q2021, 2Q2021, 3Q2021, 4Q2021 e 1Q2022, 2Q2022, 3Q2022 e 4Q2022

Anche per quanto riguarda i firewall si può notare che c'è stato un decremento dei dispositivi totali, in particolare nel nord Italia.

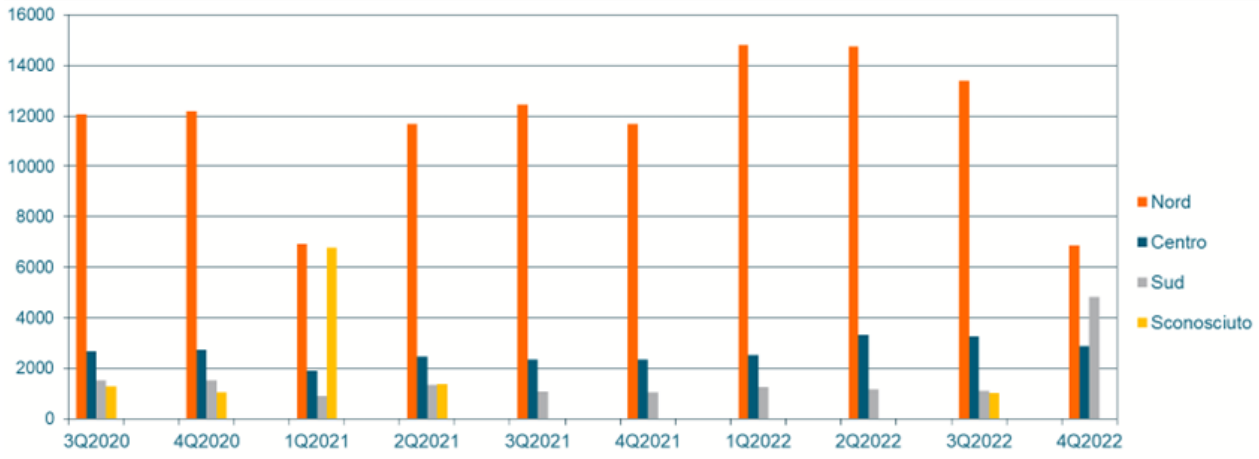

Figura 34 - Distribuzione firewall in Italia per area geografica 3Q2020, 4Q2020, 1Q2021, 2Q2021, 3Q2021, 4Q2021 e 1Q2022, 2Q2022, 3Q2022 e 4Q2022

Per i router, si evidenzia un aumento dei dispositivi individuati per quanto riguarda nord (da 6.394 a 6.883), centro (da 2.076 a 2.873) e sud (da 1.951 a 4.822) per un totale di 1251 dispositivi in più rispetto al 3Q2022.

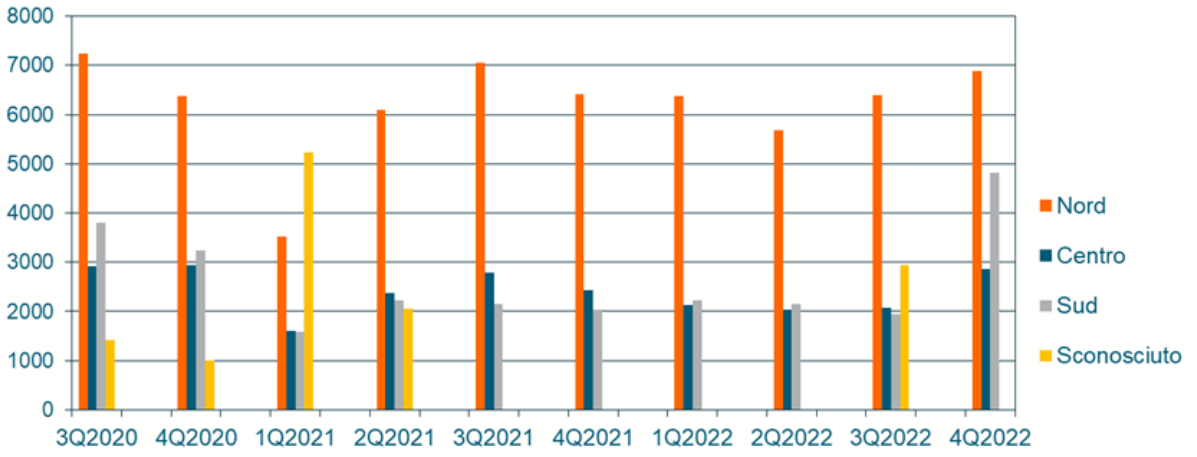

Figura 35 - Distribuzione router in Italia per area geografica 3Q2020, 4Q2020, 1Q2021, 2Q2021, 3Q2021, 4Q2021 e 1Q2022, 2Q2022, 3Q2022 e 4Q2022

Nel 4Q2022 sono riportate le analisi effettuate sui dispositivi medicali, iniziate nel quarter precedente. Come è possibile osservare dalla figura si nota una notevole diminuzione di tali dispositivi che passa dai 2.106 rilevati nel 3Q2022 ai 673 rilevati nel 4Q2022. Si può notare, inoltre una maggiore presenza di questi dispositivi a nord, seguiti da centro e sud.

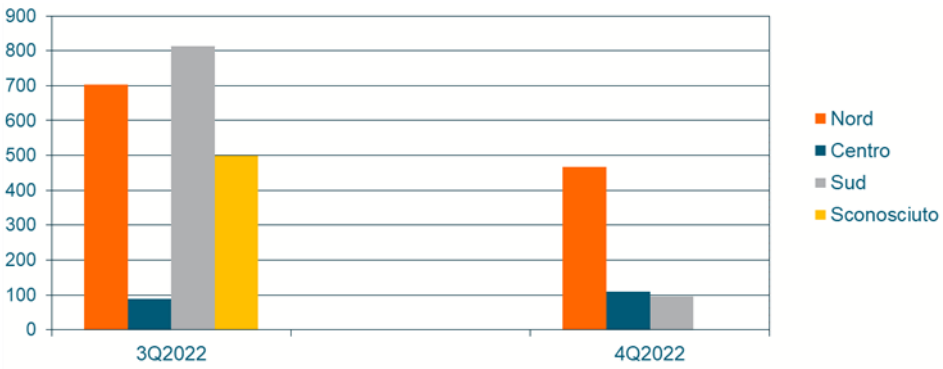

Figura 36 - Distribuzione dispositivi medicali in Italia per area geografica 4Q2022

Stato della sicurezza dei dispositivi IoT 4Q2022

In questa rubrica si illustra l'evoluzione del livello di sicurezza dei dispositivi IoT osservati nel 4Q2022. Per valutare questo livello di sicurezza l'azienda Exprivia ha 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 4Q2022:

	4Q2022
N°Protocolli Vulnerabili	4.656
N° Protocolli Totali	127.656
N° dispositivi IoT vulnerabili	24.198
N° dispositivi IoT totali	83.191
Unsecurity_IoT_Index	0,01061

Tabella 1 - Unsecurity IoT Index Totale

Il valore ottenuto è riportato graficamente in figura 37:

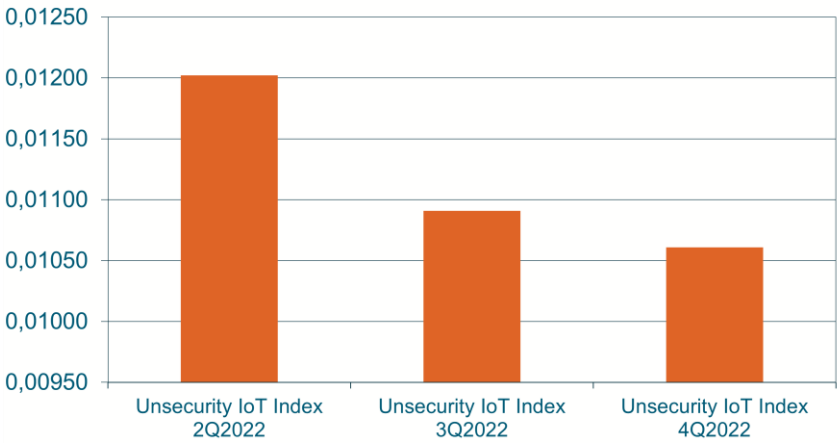

Figura 37 - Unsecurity IoT Index nel 2Q2022, 3Q2022 e 4Q2022

Come si può osservare dalla figura 37 il valore dell'UII nel 4Q2022 è leggermente inferiore. Ciò è dovuto principalmente ad una lieve riduzione del tasso di vulnerabilità dei protocolli che passa da circa il 4% nel 3Q2022 al 3,6% nel 4Q2022.

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 4Q2022 sono riportati in tabella 2:

	Nord	Centro	Sud	Sconosciuto	Totale
N°Protocolli Senza Autenticazione	2305	1344	1007	0	4.656
N° Protocolli totali	71.929	34.362	21.365	0	127.656
N° dispositivi IoT vulnerabili	10852	5565	7781	0	24.198
N° dispositivi IoT totali	39953	19685	23553	0	83.191
Unsecurity_IoT_Index	0,00870	0,01106	0,01557	0,00000	0,01061

Tabella 2 - Unsecurity IoT Index per Area Geografica

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

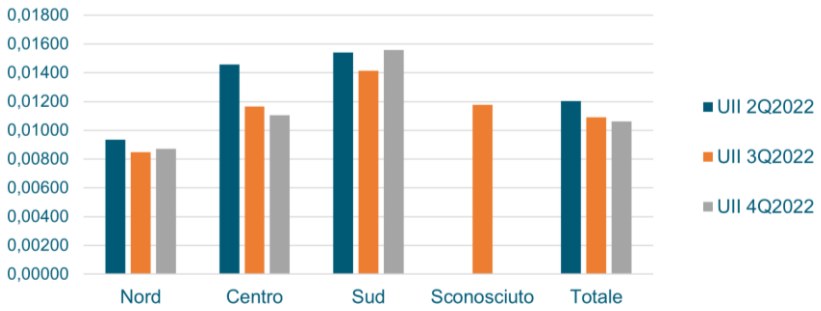

Figura 38 - Unsecurity IoT Index per Area Geografica

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 al nord. 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, come si evidenzia al centro in cui si ha un rischio moderato e al sud rispettivamente un rischio elevato.
È evidente come il decremento del valore dell'UII nazionale si riflette sulle varie aree geografiche italiane, ad esclusione del sud.

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. A partire dal 3Q2022 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
4Q2022	0,03153	0,01138	0,00000	0,00056	0,00742	0,00699	0,01061

Tabella 3 - Unsecurity IoT Index per Dispositivo

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

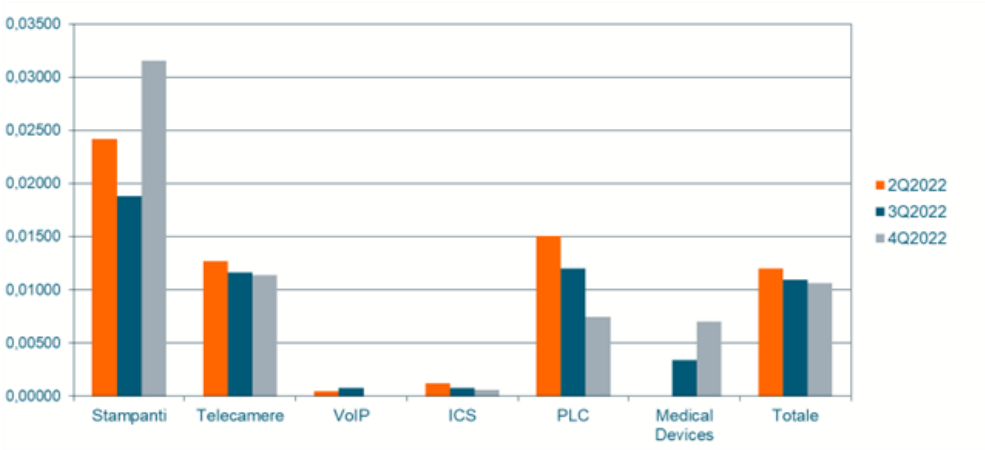

Figura 39 - Unsecurity IoT Index per dispositivo

Dall'analisi si evince che i dispositivi a maggior rischio sono le stampanti. Questo è evidente se si considera che 268 stampanti su un totale di 310 sono vulnerabili (circa l'86%). Inoltre, come si può vedere, il valore dell'indice delle stampanti è superiore di circa il 67% rispetto al totale.
Per quanto riguarda i dispositivi medicali e i PLC, si ha che solo il 19% ed il 20% dei dispositivi è vulnerabile, pertanto questi presentano un basso rischio.
Una considerazione analoga può essere fatta per i dispositivi ICS che presentano un rischio molto basso poiché solo l'1,5% 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 75.470 telecamere totali, 23.549 sono risultate vulnerabili pari ad una percentuale di vulnerabilità di circa il 31%.

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
01/12/2022	0,00064

Tabella 4 - IoT Vulnerability Entropy Index

I risultati ottenuti vengono mostrati graficamente in figura 40:

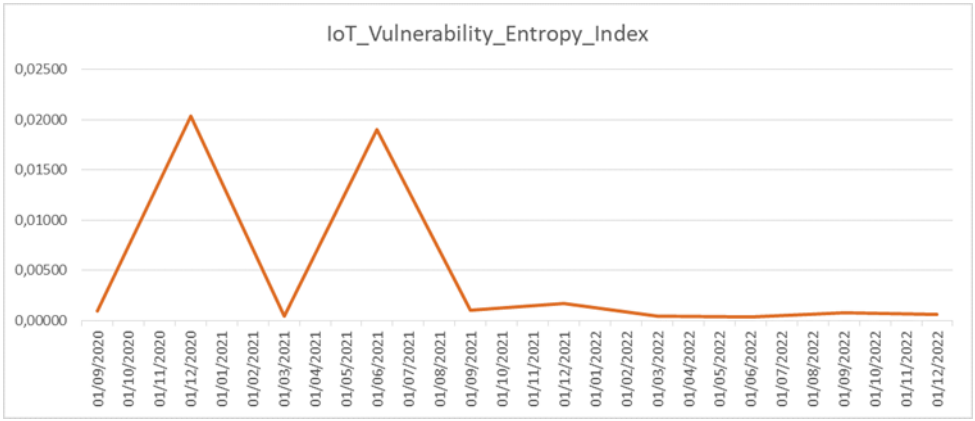

Figura 40 - IoT Vulnerability Entropy Index

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 4Q2022. 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 4Q2022

In questo approfondimento si osserva l''evoluzione del livello di sicurezza dei settori economici italiani in riferimento al 4Q2022.
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 4Q2022:

	Investment Index 2Q2022	Investment Index 3Q2022	Investment Index 4Q2022
Automotive	9,8973	9,9349	9,9306
Consulting	9,4898	9,5440	9,3646
Critical Infrastructure	9,5781	9,5427	9,4993
Education	9,8347	9,8346	9,8162
Entertainment	7,2762	7,7040	7,6799
Finance	9,9526	9,9692	9,9594

Healthcare	9,9895	9,9925	9,9906
Hospitality	9,9881	9,9863	9,9830
Industrial	9,9986	9,9989	9,9987
ONG	9,9862	9,9844	9,9933
PA	9,9876	9,9896	9,9848
Religion	9,9994	9,9991	9,9993
Retail	9,2437	9,8880	9,9847
Security	9,9977	9,9984	9,9981
Software	9,9982	9,9984	9,9981
Telco	9,8224	9,9005	9,8706

Tabella 5 - Investment Index media di ogni settore economico analizzato nel 4Q2022

I risultati ottenuti vengono mostrati graficamente in figura 41:

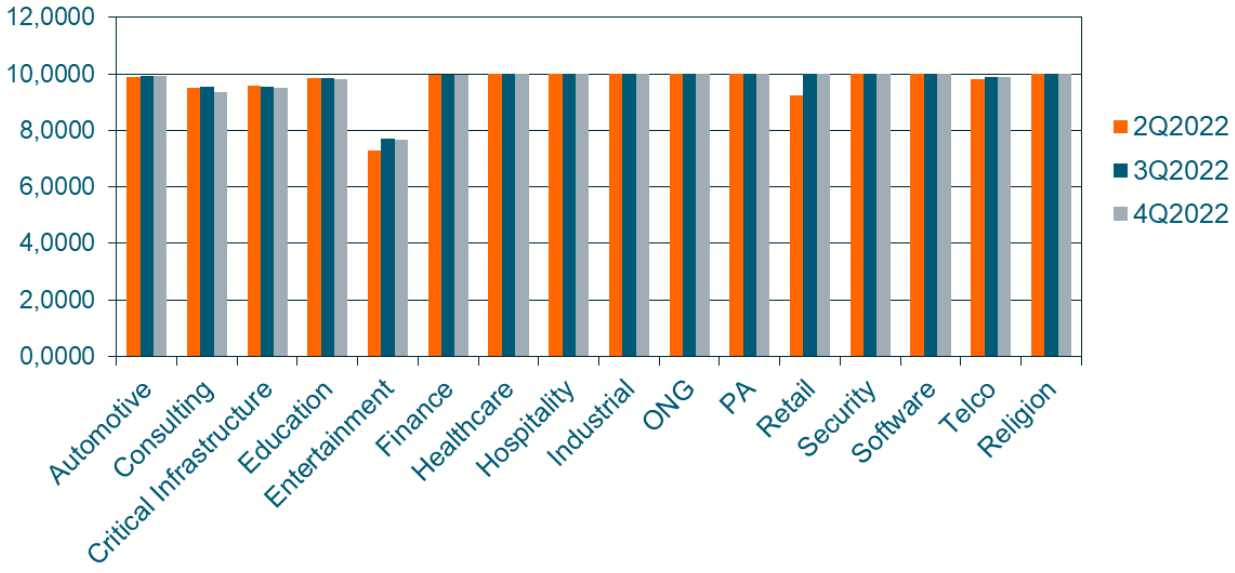

Figura 41 - Rappresentazione grafica dell'Investment Index media per ogni settore economico analizzato

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 9,9993), in lieve incremento rispetto a quello del 3Q2022.

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 7,6799 (in decremento rispetto a quello del 3Q2022 in cui era stato rilevato un II pari a 7,7040).
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 e 3Q2022:

	Investment Index 2Q2022	Investment Index 3Q2022	Investment Index 4Q2022
Nord	9,6108	9,7051	9,6925
Centro	9,7891	9,8492	9,8270
Sud	9,9897	9,9921	9,9912

Tabella 6 - Investment Index per Area Geografica

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

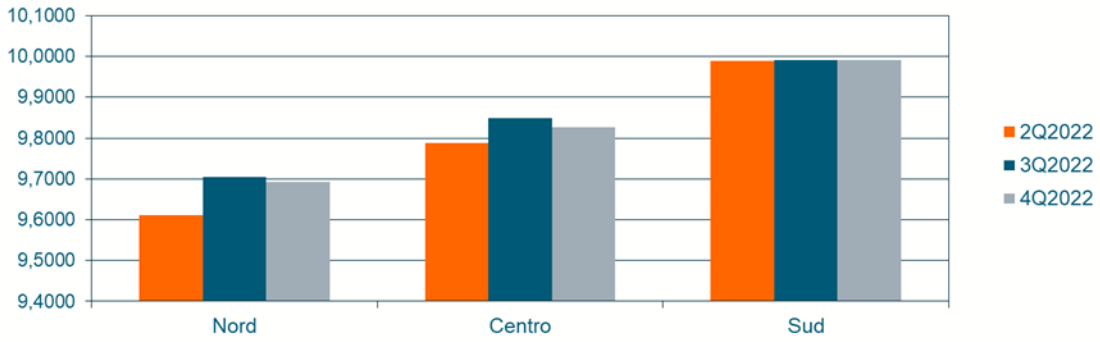

Figura 42 - Investment Index per Area Geografica

Dalla figura si evince come, rispetto al quarter precedente, ci sia stato un lieve peggioramento dell'efficienza degli investimenti a Nord e Centro e sia rimasto quasi costante 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 4Q2022

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 ottobre, novembre e dicembre hanno toccato differenti aeree del territorio italiano creando non poche problematiche. In questo quarto quarto del 2022 è stato registrato un andamento relativamente decrescente rispetto ai tre mesi precedenti, 17% in meno. 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 riguardano i *sistemi operativi,* quasi il 26% del totale delle vulnerabilità riscontrate in questo ultimo quarto del 2022. Un sistema vulnerabile può causare qualsiasi genere di disservizio e danno

Anche nel 4Q2022 sono state individuate un gran numero di vulnerabilità in ambito "*Security*", il 20%. Valore costante rispetto il quarto precedente. 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.

Come per le vulnerabilità in ambito "*Security,*" sono state individuate lo stesso numero di vulnerabilità in ambito "*Industria*", anche in questo caso abbiamo un valore costante rispetto il 3Q2022. 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.

In questo quarto è stato riscontrato un leggero decremento delle vulnerabilità in ambito "*Browser",* una in meno rispetto i tre mesi precedenti. 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.

Nel 4Q2022 si è riscontrato un andamento costante delle vulnerabilità relative alle *telecomunicazioni* rispetto al quarto precedente. 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 4Q2022 rispetto il 3Q2022 sono state riscontrate anche vulnerabilità relative al *Cloud* e alle *infrastrutture critiche.* Le prime permettono ai cybercriminali di accedere ad aree riservate agli utenti prendendo possesso

di informazioni sensibili. Le seconde, non per importanza, potrebbero causare danni sia all'ente stesso, che ne è affetto, ma anche alla collettività, in quanto questi enti erogano servizi di prima necessità.

Da evidenziare il dato relativo alle vulnerabilità legate ai software che permettono la *conservazione di documenti,* sempre più presenti. 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.

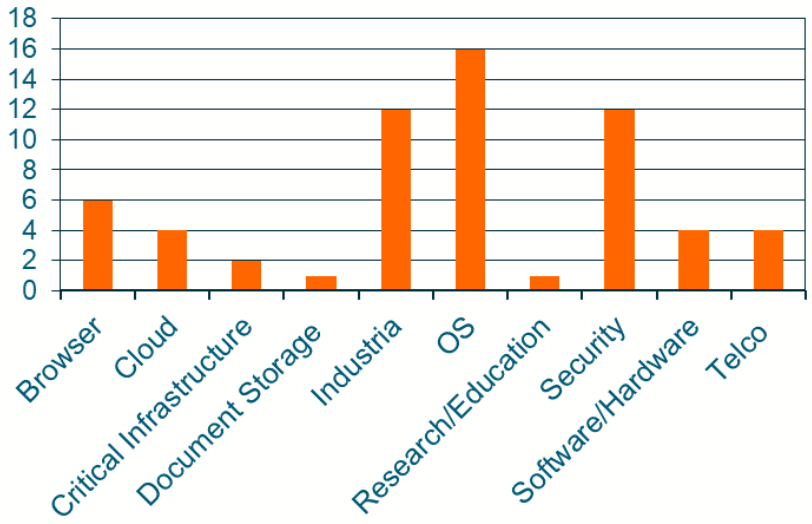

Figura 43 - Tipologia Vittima 4Q2022

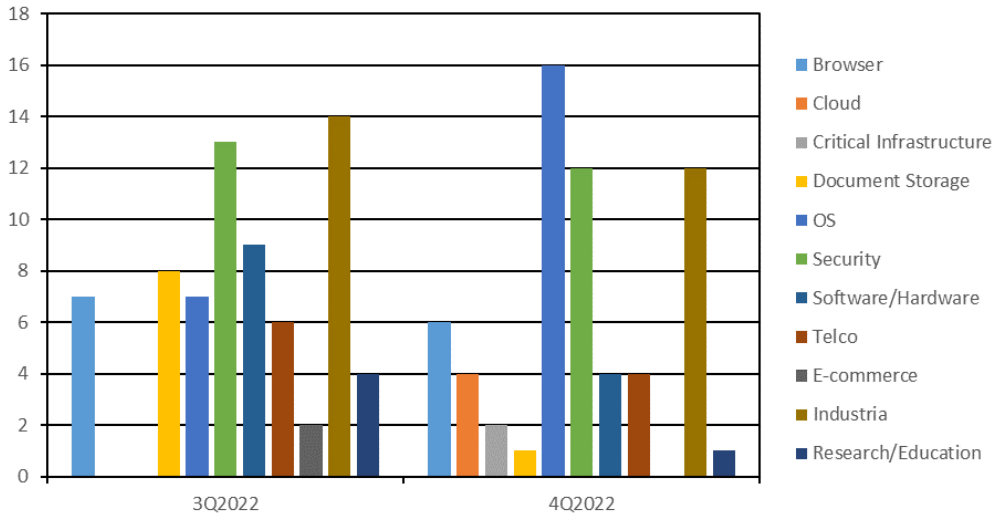

Figura 44 - Tipologia vittima 3Q2022 e 4Q2022

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

In questo quarto quarto del 2022 la tipologia di danno più riscontrata è di tipo "*Remote code execution*", il 22% sul totale. 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 4Q2022 è stato registrato un decremento delle vulnerabilità che causano danni di tipo "*Denial of Service*", il 50% in meno. Dato da non sottovalutare perché questa vulnerabilità crea importanti disservizi all'intero sistema rendendolo inutilizzabile.

Anche le vulnerabilità che provocano *Service interrupt* hanno registrato una diminuzione, quasi la metà rispetto il 3Q2022. 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

Nel 4Q2022 è stato registrato un decremento delle vulnerabilità che causano danni di tipo di "*Privilege escalation*". 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.

In quest'ultimo quarto è stato registrato un netto incremento per quanto riguarda le vulnerabilità che causano danni alla *privacy,* più di cinque volte rispetto i tre mesi precedenti. 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.

L'andamento delle vulnerabilità che causano danno di tipo "*C&C*" è costante rispetto il quarto precedente. 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.

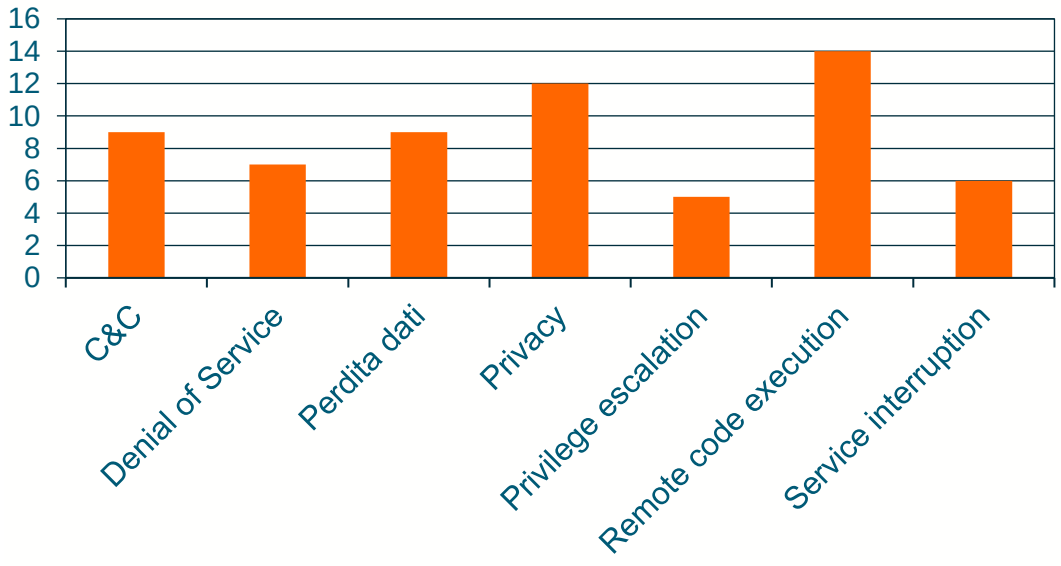

Figura 45 - Tipologia danno 4Q2022

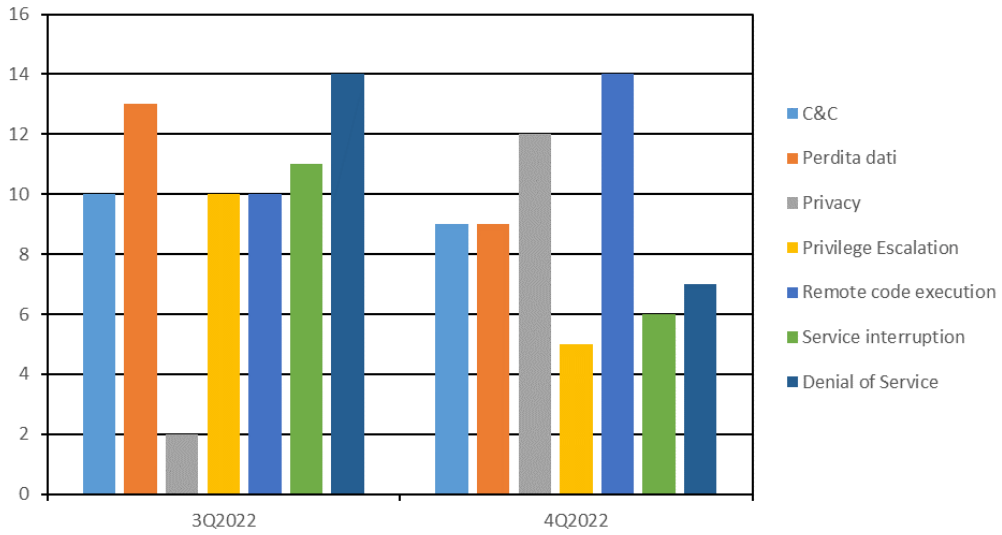

Figura 46 - Tipologia danno 3Q2022 e 4Q2022

Tutte le vulnerabilità individuate dal nostro Osservatorio nel 4Q2022 hanno criticità abbastanza elevata. Sono state riscontrate esattamente 12 critiche, 39 alte e 11 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.

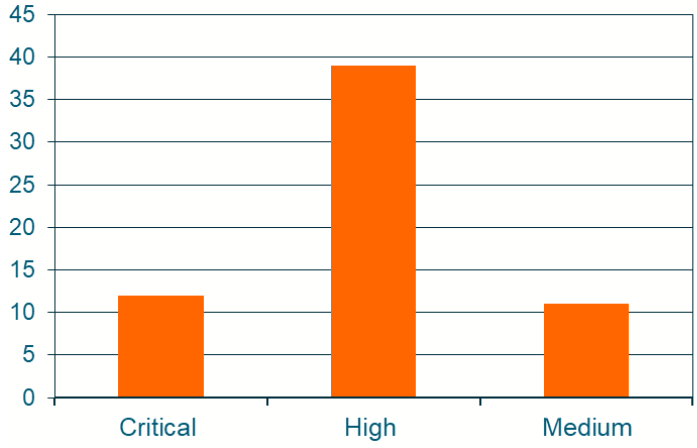

Figura 47 - Severity vulnerabilità 4Q2022

Analizzando i dati nel loro complesso, è possibile mettere a confronto le informazioni riguardante il 2021 con i dati del 2022. La tipologia di vittima presente in entrambi gli anni in modo massivo è quella relativa "*Software/Hardware".* Questo ribadisce la pericolosità di queste falle.

In entrambi gli anni sono presenti vulnerabilità che interessano la *Security*, le *telecomunicazioni,* le *industrie* e vulnerabilità relative ai "*Browse"r e i sistemi operativi* anche se in numero notevolmente maggiore nel 2022.
Nel 2022 sono state riscontrate tipologie di vittime nuove come "*E-commerce*" e "*Research/Education*".

Analizzando invece la tipologia dei danni generati a seguito delle vulnerabilità del 2021 e del 2022 si evidenzia che i danni più ricorrenti sono "*Perdita dati*" e "*Privacy*". Questo ad evidenziare l'importanza dei dati. Inoltre, nell'ultimo anno è stato registrato una crescita di vulnerabilità che causano danni di tipo "*Privilege Escalation*" e "*Remote code execution*". A testimonianza dell'importanza di mettere in sicurezza i sistemi utilizzati.
Nel 2022 sono state riscontrate tipologie di danno nuove come "*Denial of Service*".

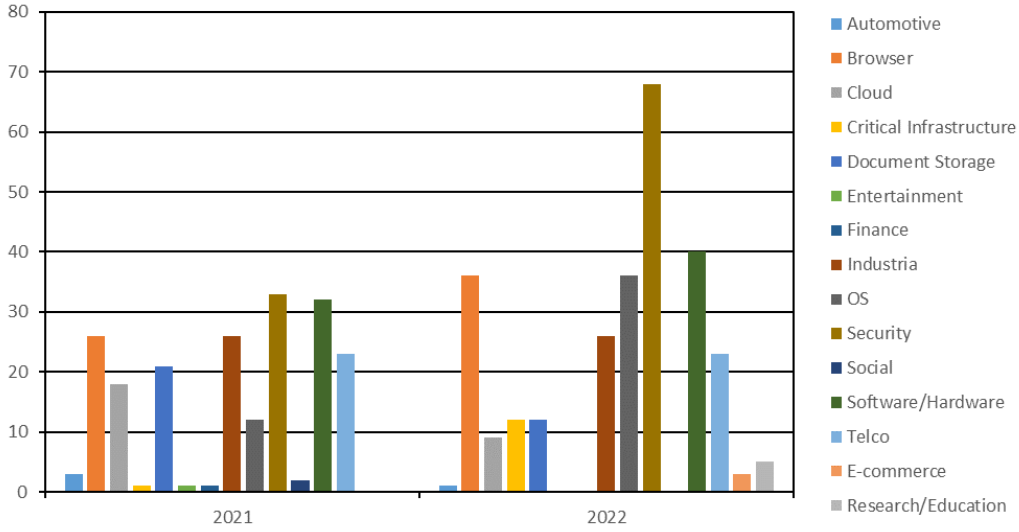

Figura 48 - Tipologia vittima 2021/2022

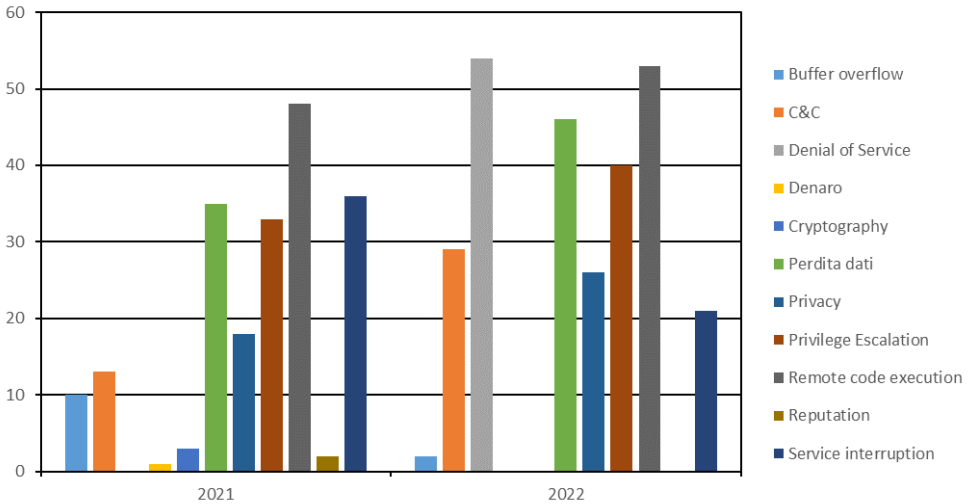

Figura 49 - Tipologia danno 2021/2022

Approfondimenti

Perché è fondamentale per tutti proteggere le Utenze Privilegiate?

Carlo Falciola, *Senior Security Technical Advisor – Exprivia*

Per ogni organizzazione sa che è fondamentale proteggere le Utenze Privilegiate, perché proprio i privilegi sono al centro di tutti gli attacchi.
Il più delle volte è proprio attraverso l'utilizzo malevolo delle utenze privilegiate che i malware e gli attaccanti più in generale raggiungono i propri obbiettivi: danneggiare i sistemi attaccati o rubarne i dati. Le statistiche più recenti (ricerca Cyberark 2021) indicano come più del **95%** degli attacchi avvenga avvalendosi dell'abuso e della escalation di privilegi.
La protezione del perimetro di una organizzazione che è pur sempre **necessaria**, ormai non è più **sufficiente**, a causa della evoluzione digitale che porta ad una sempre più massiccia interazione con sistemi e servizi di terzi, alla dispersione e mobilità dei lavoratori e alla adozione del cloud nelle sue differenti declinazioni.
Occorre anche ricordare che anche i più raffinati sistemi di protezione EDR e XDR, così come i servizi di detection più potenti ecc. agiscono **sempre e solo a valle di azioni malevoli o mentre** un attacco è in corso.
Quindi un approccio proattivo e preventivo di protezione dei privilegi è un tassello fondamentale per qualsiasi organizzazione, non sostituisce o esclude i sistemi di protezione classici, bensì li rafforza!

Quali sono le utenze privilegiate?

Analizziamo in maggiore dettaglio le Utenze Privilegiate (UP), che sono tutte quelle utenze che possiedono privilegi nei confronti dei sistemi di una organizzazione. Si suddividono in quattro classi: utenze privilegiate umane, utenze privilegiate non-umane, utenze privilegiate personali e utenze privilegiate condivise.
Le utenze umane sono, ovviamente quelle utilizzate dal personale di una organizzazione, quelle non-umane sono invece utilizzate da sistemi fisici o software per effettuare comunicazioni automatiche. È fondamentale l'applicazione del criterio che in nessun caso deve essere permessa ed accettata la commistione nell'utilizzo delle medesime utenze da parte di persone e sistemi, in quanto la tracciabilità e la identificabilità di utenze in uso misto diventa eccessivamente complessa ed i tempi di analisi di anomalie troppo lunghi per una efficace protezione.
Le utenze privilegiate condivise sono di solito il gruppo più ampio di utenze presenti in una organizzazione, in quanto le troviamo built-in in ogni apparato, sia esso fisico che virtuale, in ogni workload, ed in ogni istanza di middleware, DBMS o appliance per permetterne l'amministrazione a livello apicale da parte del personale preposto, ovvio in questo caso l'esigenza di ottenere l'identificazione stretta di ogni utilizzo, la minimizzazione della conoscenza diretta di tali credenziali da parte del personale e l'applicazione di opportune tecniche di rotazione periodica automatica.
Anche le applicazioni posseggono utenze privilegiate per la loro amministrazione e ne utilizzano altre per accedere ai dati, in questo caso le criticità sono la conservazione sicura delle credenziali senza dispersione, la possibilità di rotazione periodica e la possibilità di limitarne l'uso effettivo alle sole effettive istanze applicative. In condizioni non protette le utenze applicative sono sicuramente un "soft spot" per gli attaccanti in quanto tipicamente possiedono diritti elevati su risorse sensibili (es. DBMS), inoltre, affinché le applicazioni possano fruirne sono conservate in modalità standardizzate e note (es. file di configurazione), poco o per nulla protette, e vengono utilizzate dalle applicazioni con elevata frequenza rendendo il

tracciamento degli accessi difficile, se non impossibile. Anche in questo caso l'utilizzo misto da parte di applicazioni e personale è assolutamente da evitare per le ragioni sopra discusse.
Le utenze privilegiate personali, nelle quali il privilegio è associato in modo permanente ad una utenza sono i punti preferiti di ingresso degli attaccanti e le best practices di sicurezza suggeriscono ormai univocamente di limitare al massimo l'adozione o meglio eliminarle del tutto dalle organizzazioni sostituendole con approcci Just-in-Time o (R)ABAC, approcci che proprio le soluzioni PAM possono e devono implementare con efficacia.

Quante sono le utenze privilegiate?

Le Utenze privilegiate sono tantissime in ogni organizzazione, in quanto in qualunque organizzazione esistono conosciute o sconosciute molte più utenze “privilegiate” che utenze “normali”. Questo accade per varie ragioni concomitanti:
Ogni sistema fisico o virtuale possiede almeno una credenziale apicale, built-in nel sistema, cosi come ogni piattaforma applicativa on-prem o SaaS possiede almeno una utenza amministrativa apicale. Inoltre ogni Istanza di tenant Cloud possiede una utenza apicale e un numero elevatissimo di utenze predefinite con ruoli amministrativi, per esempio a tutto settembre 2022 I tre principali cloud provider mondiali contavano cumulativamente circa 7000 ruoli amministrativi differenti fra funzionalità e tools (*fonte survey 2022 - Cyberark*), da moltiplicare ovviamente per ogni tenant. Infine ogni applicazione possiede una o più utenze non-umane, spesso definite come “utenze tecniche“condivise, atte a permettere ai vari componenti della applicazione di interagire con i vari middleware ad essa rilevanti, quali DBMS, Message Server ed ad altre applicazioni. Tipicamente queste utenze "tecniche" avendo funzione di accesso “application wide" sono intrinsecamente privilegiate.

Regole base di protezione

Quali sono le regole basilari di protezione a cui attenersi: in breve vale l'affermazione: Non si può rubare che non si può raggiungere o quello che proprio non c’è!
L’uso di una soluzione PAM permette di rendere difficile o impossibile il furto di credenziali privilegiate mediante l'implementazione di differenti strategie generali, come già accennato in precedenza:

1. Evitare che esistano utenze privilegiate personali in uso continuo al personale
2. Provvedere affinché non sia necessaria la conoscenza delle password delle UP personali o impersonali da parte degli amministratori di sistema/dba/operatori di applicazioni sensibili
3. La rimozione delle password delle UP impersonali dai codici sorgenti e dai file di configurazione delle applicazioni e degli script
4. Il disaccoppiamento fisico e logico tra gli ambienti e il conseguente isolamento ed intermediazione delle sessioni amministrative

Infine, in termini generali occorre, durante l'implementazione di una soluzione PAM, porre estrema attenzione alle esigenze della utenza impattata, curando sia gli aspetti di user experience che devono rispettare il più possibile, se non migliorare, il flusso di lavoro che gli aspetti di comunicazione e "fiducia" della piattaforma, che in taluni casi andrà a sostituire una pregressa "assunzione di responsabilità" da parte del personale stesso nella gestione di tali UP.
Il personale dovrà quindi essere coinvolto fin da subito nella implementazione della piattaforma, le modalità reali di lavoro analizzate e l'implementazione ottimizzata di conseguenza. Inoltre, la stratega di resilienza complessiva della piattaforma e delle sue principali funzionalità dovrà essere condivisa con il personale interessato sia in ottica di gestione della fiducia che in quella di massimizzare la disponibilità operativa in condizioni di degrado.

Come è nata la tecnologia delle soluzioni PAM?

È interessante ricordare come la tecnologia delle soluzioni PAM sia nata all'inizio degli anni 2000, proprio da richieste dirette degli utenti amministratori che hanno iniziato ad avvalersi di strumenti di protezione dati esistenti ed hanno iniziato a intravvedere la possibilità di implementare su di questi alcune funzioni automatiche di gestione che proprio in quel periodo, caratterizzato dalla introduzione nei sistemi informativi di un sempre maggior numero di sistemi "open".

Quali sono gli impatti sulla organizzazione?

L'adozione di un PAM ha degli impatti rispetto alle modalità di lavoro e ai processi del passato.
In alcuni casi l'adozione di una piattaforma PAM, quale che essa sia, potrebbe rendere il lavoro degli amministratori un poco più scomodo, in altri invece più facile, ma nella maggior parte dei casi è solo differente.
Tuttavia, è fondamentale ricordare che l'opzione lavoro senza protezioni non è più da prendere in considerazione in nessun caso, il pericolo e in ultima analisi l'impatto anche personale sugli operatori è ormai troppo elevato.
Nella interazione con le organizzazioni che amministrano i sistemi è sempre necessario che il confronto operativo "as-is *vs* to-be" sia effettuato non nei confronti delle modalità "tradizionali" che non tengono conto di alcun criterio di sicurezza, ma nei confronti di quello che si dovrebbe fare comunque, anche senza l'adozione di un PAM. Occorre che strutture di sicurezza ed utenti amministratori collaborino assieme per trovare il miglior approccio, scegliendo l'approccio più opportuno, fra le molte opzioni possibili!

Come si Implementa una soluzione PAM?

Implementazione di una soluzione PAM di successo è una attività, come abbiamo visto, importante e presenta sempre impatti organizzativi ed operativi, che non devono essere trascurati o rimandati, ma vanno gestiti con la necessaria attenzione e condivisione. Una implementazione PAM affrettata e non condivisa spesso si arena in veti reciproci e non ottiene il desiderato e necessario esito di mitigazione del rischio.
Da parte della organizzazione responsabile della implementazione PAM sarà anche necessaria l'applicazione di attenzione ed accortezza nella definizione in collaborazione con le funzioni aziendali di compliance delle corrette misure ed opzioni di sicurezza da attivare nella piattaforma nei confronti della utenza finale, modulando i numerosi strumenti ed opzioni normalmente presenti nelle piattaforme PAM più evolute in funzione delle necessari livelli di controllo, senza tuttavia eccedere nei requisiti attivati imposti all'utenza magari anche in casi ove questi non fossero non strettamente necessari. L'applicazione di controlli anche banali, p.es. di scrivere una motivazione ad una azione, dovrebbero essere sempre validati da un lato in merito alla effettiva utilità che ne deriverebbe, dall'altro dall'impatto operativo sulla utenza e nel caso applicati solo in contesti di effettiva necessità e se possibili sempre mitigati da opportune azioni di pre-configurazione (nel caso specifico predisponendo in piattaforma una serie di messaggi precompilati di uso più comune.

Pianificazione della Resilienza della piattaforma PAM

Le credenziali privilegiate sono il cuore operativo di una organizzazione e si deve porre la massima cura nella loro conservazione e nella disponibilità della piattaforma è quindi essenziale.
Inoltre, l'adozione e l'uso pervasivo di una soluzione PAM è accettata e valida solo se in grado di offrire servizio nello spettro più ampio delle condizioni di degrado che un sistema informativo possa venire a trovarsi
Ciò avviene curando i seguenti aspetti in una implementazione:

Alta Disponibilità

La piattaforma che sia on prem o in cloud deve sempre essere Alta disponibilità e la progettazione delle architetture dovrebbe prevedere una “graceful performance degradation”, sempre commisurata al contesto.
Analisi, Minimizzazione e mitigazione degli SPoF

E' sempre anche necessaria una attenta analisi dei "Single point of failure" relativa alla piattaforma nel suo complesso e delle interazioni con gli altri servizi del sistema informativo e dovrà essere prodotto e condivisa l'elenco delle corrispondenti azioni di mitigazioni possibili.

Disponibilità, validità e addestramento su tutte le procedure di Failover, Last Resort e Recovery

È necessaria la massima attenzione nella definizione di tutte le procedure di mitigazione dei malfunzionamenti, la condivisione delle strategie con l'utenza ed il test periodico delle stesse che ne permetta una continua validazione e familiarità da parte del personale coinvolto siano questi gli amministratori PAM che le varie tipologie di utenti finali.

Sicurezza in sanità: un case study per la telemedicina

Rosita Galiandro, *Responsabile Osservatorio Cybersecurity - Exprivia*
Gaetano De Gennaro, *Process Analyst - Exprivia*

Numerosi sono i vantaggi che si introducono nella società con l'avvento dell'e-health e della telemedicina. Si pensi a quanto sia stata utile durante la pandemia da COVID-19, periodo in cui i medici mediante apposite tecnologie hanno potuto seguire i propri pazienti a distanza, monitorando i parametri vitali ed eventualmente somministrando le giuste cure.
Il vantaggio prodotto dall'uso della tecnologia è stata sicuramente la riduzione della congestione nelle strutture ospedaliere, in difficoltà sin da subito.

Le nostre informazioni sono davvero al sicuro?

Oggi si convive con il costante pensiero che i nostri dati vengono custoditi in enormi database e che le nostre informazioni restino effettivamente nostre e di nessun altro.
Ignoriamo molto spesso una voce interiore, quella più prudente, che ci allontanerebbe dall'idea di custodire informazioni tanto importanti online.
Si può affermare, quindi, che la digitalizzazione in sanità è qualcosa di rivoluzionario e che sta cambiando il modo di concepire l'assistenza sanitaria stessa.
A fronte di cambiamenti positivi c'è anche da tener conto di ulteriori aspetti che necessitano di particolare attenzione: assicura la security e la safety.
Problemi di sicurezza, infatti, possono causare forti disagi sia ai pazienti che ai care-providers, con conseguenze quasi sempre gravi.

Paziente	Care-provider
Furto d'identità	Indisponibilità dei sistemi
Frodi fiscali	Perdita di dati
Vendita di dati a terzi	Corruzione di dati

Tabella 7 - Possibili minacce ai pazienti e ai care-provider

Sfide per la sicurezza in ambito sanitario

Si riportano di seguito alcuni famosi attacchi in ambito healthcare:

- **Medjack**: exploit che dirotta i dispositivi IoT per creare delle backdoor nelle reti ospedaliere. I dati medici rubati sono stati utilizzati per perpetrare frodi fiscali o furti d'identità, oltre che per tracciare la prescrizione di farmaci;
- **Ransomware**
  - Europa e nord America: WannaCry
  - ASL Torino: il 19/08/2022 si è verificato un tentativo di attacco ransomware, procurando un rallentamento dei sistemi informatici

Si noti in ambito ospedaliero quanto sia importante la disponibilità dei sistemi informatici (e di conseguenza informativi).
L'indisponibilità dei sistemi in fase di accettazione in un pronto soccorso, causa un notevole ritardo nell'erogazione di cure a chi le necessita, aumentando così il livello di congestione delle strutture e aggravando lo stato di salute dei pazienti.
È possibile quindi racchiudere le sfide per la sicurezza in ambito sanitario in cinque parole chiave:

- Anonimizzazione
- Robustezza
- Resilienza
- Data Breach
- Privacy

Quando porre maggiore attenzione alla sicurezza nelle reti ospedaliere?

Molto spesso, le reti ospedaliere sono protette da determinate accortezze sistemistiche, come ad esempio un firewall.
La situazione però diventa critica nel momento in cui le informazioni escono dall'ambiente protetto (rete della struttura ospedaliera) e viaggiano attraverso Internet.
Si pensi ad un paziente monitorato a distanza mediante dispositivi IoT (Internet of Things), i quali inviano periodicamente alla struttura ospedaliera i dati sanitari rilevati.
In questo caso risulta impossibile implementare determinati criteri di sicurezza, rendendo il tutto più complicato.

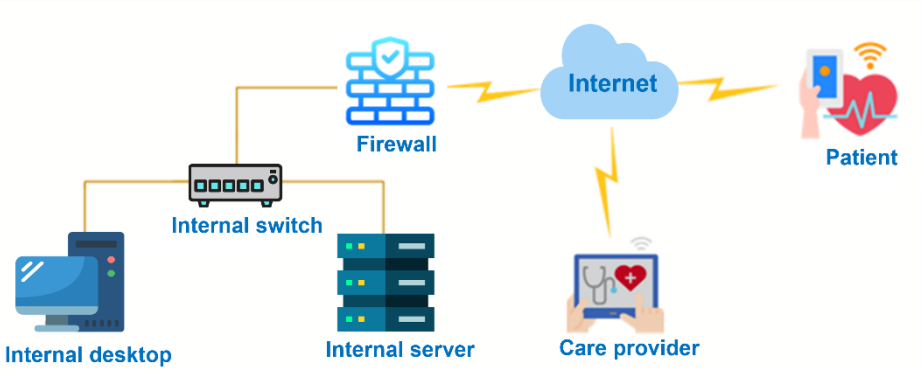

Figura 50 - Use case in e-health

Quale soluzione adottare? In questo scenario, si pensi ad un possibile ruolo della **Blockchain**.

Blockchain: overview

Blockchain è una rete di nodi interconnessi tra loro mediante tecnologia P2P (Peer-to-Peer). Consiste nella condivisione di un registro comune, dove si tiene traccia di tutte le transazioni avvenute nella rete, dove per transazione s'intende l'aggiunta di un nuovo blocco alla catena esistente.
Prima che avvenga, una transazione deve essere validata: la maggior parte di nodi partecipanti deve assicurare che le regole del protocollo vengano seguite e che tutti i partecipanti siano d'accordo sull'attuale stato di Blockchain.

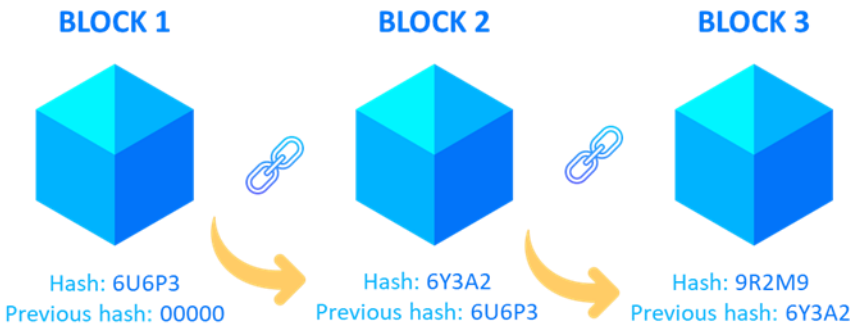

Figura 51 - Esempio di Blockchain

Blockchain: è la soluzione ideale?

C'è da dire che sono numerosi i casi di pazienti monitorati remotamente. Come accennato precedentemente, essi sono collegati a dispositivi medici che comunicano periodicamente o costantemente in rete e sono connessi ad una centrale operativa pronta ad intervenire in caso di necessità.
Questo tipo di assistenza, utilizzato in parte durante la pandemia da COVID-19 possiede però delle criticità: si pensi alla quantità di informazioni che tali dispositivi producono e che devono memorizzare. Un sistema centralizzato porterebbe inevitabilmente alla creazione di un collo di bottiglia e faciliterebbe un attacco mirato a rendere indisponibile il sistema. La tecnologia distribuita consente di avere più punti di accesso al dato, garantendone la disponibilità in qualsiasi momento.
Tuttavia, in questo contesto, Blockchain si rivela particolarmente utile anche per tracciare lo storico degli eventi, che vengono memorizzati in modo immutabile per la tecnologia in essere.
Per le proprietà intrinseche di Blockchain, è possibile ricostruire la storia dei record e la loro proprietà, fungendo come una specie di log certificato che attesti il susseguirsi di determinati eventi.

	Immutabilità	Applicazione distribuita	Sicurezza
Blockchain	Registro contenente la storia delle transazioni	L'accesso alle informazioni non avviene in unico punto, riducendo eventuali colli di bottiglia. Logiche ben codificate atte a ridurre frodi, errori e costi	Trasmissione e memorizzazione di dati sensibili in maniera sicura Dati immutabili garantendo autenticità
VS			
DB Centralizzato	I dati possono essere compromessi: unico point of failure	Un DB centralizzato potrebbe richiedere un grande effort per creare le connessioni con ogni client. La disponibilità dei dati può non essere sempre garantita	Unico point of failure dove può avvenire un data breach La trasmissione di dati potrebbe essere compromessa

Tabella 8 - Blockchain vs DB Centralizzato

C’è da dire che, come accennato, in ambito IoT gli attori che accedono alle informazioni fruiscono dei sistemi dall’esterno della struttura ospedaliera, che può essere protetta mediante apposite accortezze sistemistiche. In questo caso, risulta più difficile controllare la sicurezza dei dispositivi e Blockchain apporta determinati vantaggi, consentendone anche la pseudonimizzazione (separando le informazioni anagrafiche da quelle sanitarie).

Sicurezza della Blockchain

La Blockchain **rappresenta un approccio innovativo alla cyber security** poiché è una tecnologia che permette di progettare sistemi rispettando il principio security by design.
La sicurezza della tecnologia Blockchain si basa principalmente su tre elementi fondamentali:

- **Riservatezza**: la Blockchain offre funzionalità estese per garantire l’anonimato dell’utente. Le chiavi utente sono l’unico collegamento tra un utente e i suoi dati. Tuttavia, queste chiavi sono facili da rendere anonime. L’utilizzo della Blockchain deve garantire l’accesso ai dati corretti solo alle parti interessate e autorizzate. Proteggere l’accesso alla rete Blockchain è importante per garantire l’accesso ai dati, soprattutto per la Blockchain privata.
  La riservatezza dei partecipanti alla rete Blockchain è elevata a causa della crittografia a chiave pubblica che autentica gli utenti.
- **Integrità dei dati**: le Blockchain sono progettate come libri mastri (ledge) in cui ogni blocco è collegato a blocchi vicini utilizzando funzioni hash crittografiche. Pertanto, una volta che una transazione è stata registrata sulla Blockchain, non può essere modificata o eliminata. Eventuali modifiche apportate ai dati già registrati vengono elaborate come nuove transazioni.
- **Disponibilità**: avere un numero elevato di nodi garantisce la resilienza della Blockchain anche quando alcuni nodi non sono disponibili. E poiché ogni nodo della rete ha una copia del registro distribuito, la Blockchain corretta rimane accessibile ad altri peer anche nel caso di un nodo compromesso.

Figura 52 - I parametri RID della Sicurezza Informatica

Blockchain e Cybersecurity

Le soluzioni basate su Blockchain si stanno rilevando particolarmente efficaci e promettenti al fine di aumentare la sicurezza informatica e prevenire attacchi informatici. In particolare, applicare la Blockchain alla CyberSecurity permette di avere i seguenti vantaggi:

- Blockchain *decentralizza i dati sensibili*. L'informazione che circola oggi sul web ha un valore enorme; per questo motivo è spesso oggetto di attacchi informatici.
  - Pertanto, anziché utilizzare l'archiviazione centralizzata, le soluzioni basate su Blockchain archiviano i dati su molti nodi. Ciò complica notevolmente la vita dei criminali informatici, che non possono più accedere a interi database da un unico punto di accesso.
- Un altro modo in cui la Blockchain trasformerà la CyberSecurity sarà attraverso i *dispositivi IoT "più intelligenti"*
  - I dispositivi in un sistema possono prendere decisioni sulla sicurezza in modo indipendente, senza l'esigenza di un'autorità centrale.

Ad esempio, possono formare un consenso condiviso su eventi normali all'interno di una rete e bloccare i nodi che si comportano in modo diverso e quindi sospetto. Ciò renderebbe più difficile per i cyber criminali sfruttare le vulnerabilità dei dispositivi periferici per penetrare in una rete.

- Blockchain consente di prevenire *attacchi DNS.*
  - Il DNS è per lo più centralizzato; è più facile interrompere la connessione tra il nome del sito Web e l'indirizzo IP. In effetti, gli attaccanti sfruttano questa debolezza per rendere i siti inutilizzabili o reindirizzare le persone a siti truffa. In un sistema basato su Blockchain, il decentramento consentirebbe di archiviare le informazioni sul dominio su un ledger distribuito.
    L'implementazione della tecnologia Blockchain decentralizzerebbe completamente il DNS, distribuendo i contenuti a un numero maggiore di nodi rendendo così quasi impossibile l'hackeraggio per i cyber-attaccanti.
- Riservatezza
  - L'utilizzo della Blockchain deve garantire l'accesso ai dati corretti solo alle parti interessate e autorizzate. Proteggere l'accesso alla rete Blockchain è importante per garantire l'accesso ai dati, soprattutto per la Blockchain privata.

La riservatezza dei partecipanti alla rete Blockchain è elevata a causa della crittografia a chiave pubblica che autentica gli utenti.

La Blockchain è stata mai hackerata?

Mentre la tecnologia Blockchain produce un registro delle transazioni a prova di manomissione, le reti Blockchain non sono immuni da attacchi informatici e frodi. Gli aggressori malintenzionati possono manipolare le vulnerabilità note nell'infrastruttura Blockchain e sono riusciti in vari attacchi e frodi nel corso degli anni.
La Blockchain è particolarmente attraente per gli attaccanti perché le transazioni fraudolente non possono essere annullate come spesso possono essere nel sistema finanziario tradizionale. Oltre a ciò, sappiamo da tempo che proprio come la Blockchain ha caratteristiche di sicurezza uniche, ha anche vulnerabilità uniche.

Alcune minacce in ambito Blockchain riguardano:

- Indisponibilità del servizio (che renderebbe inutilizzabili i servizi basati su Blockchain);
- Indisponibilità di Internet (ad esempio, se un'applicazione su Blockchain lancia un attacco DDoS);
- Controllo fraudolento della Blockchain (ad esempio, furto dei wallet digitali).

Modelli di servizio per la Cybersecurity – Cloud & MSSP

Carlo Falciola, Service Delivery Manager Exprivia
Graziano Specchierla, ICT Security Consultant Exprivia

Molte aziende si trovano a dover pianificare investimenti sempre crescenti in ambito cybersecurity, a protezione del business, dei dati e della reputazione.
Nel panorama cybersecurity attuale, vi è una vasta scelta di prodotti, servizi e modalità di accesso agli stessi, e il mercato è molto segmentato. Nascono ogni giorno nuove startup, e questo spesso crea delle nicchie interessanti per i fornitori di servizi, sempre a caccia di novità.
Dal punto di vista dell'utente finale, il CISO o l'IT manager della situazione, la faccenda è complicata.
Spesso è difficile effettuare scelte, vista la quantità di elementi a disposizione, e il timore di finire in una nicchia e vanificare investimenti in skill e tecnologie è sempre alto. È pur vero che i modelli di acquisizione delle licenze in subscription rendono più facile passare da un servizio ad un altro, ma il cambiamento non è tutto riconducibile a questa pur semplice operazione: servono tempo, risorse e competenze.
Fortunatamente si possono minimizzare le problematiche di gestione diretta delle tecnologie necessarie e delle scelte da effettuare. È necessario affidarsi ad un fornitore che possa essere partner vero in queste scelte, e possa intermediarle efficacemente, perché conosce il problema e non si focalizza su una unica soluzione.

I vantaggi di un modello "Managed Security Service Provider"

Il modello MSSP presenta numerosi vantaggi in quanto permette di sopperire ad evidenti difficoltà nel reperire e sostenere economicamente la disponibilità in azienda di figure di esperienza negli ormai molti sottosettori. Quindi la grande organizzazione potrà evitare una eccessiva frammentazione delle competenze e contemporaneamente essere in grado di avvalersi delle più recenti soluzioni di sicurezza disponibili sul mercato. Di contro le piccole organizzazioni potranno comunque avvalersi a costi contenuti ed in tempi più rapidi del supporto di competenze nel contesto, senza dover far dolorose scelte di priorità o rinunciare a servizi essenziali a causa della inevitabile necessità di adattarsi ai flussi di budget annuali.

L'importanza di scegliere il partner giusto le proprie necessità

È bene scegliere un cybersecurity partner al quale affidarsi che non fornisca solamente un SOC, con servizi di pura gestione degli eventi di sicurezza di primo livello e secondo livello. Oltre alle attività di Detection e Response ci si potrà avvalere di un Managed Security Service Provider su tutto lo spettro della classificazione NIST, quindi anche Identify, Prevention e Recovery.
Un Managed Security Service Provider è in grado di governare end-to-end le tematiche di sicurezza, e di offrire servizi basandosi su una framework di riferimento, e su architettura che non siano strettamente dipendenti dall'una o dall'altra tecnologia, ma che si possano adattare alle richieste ed alle esigenze del Cliente finale.
Quindi un "SOC MSSP", oltre all'analisi degli eventi e delle minacce, dovrà poter fornire anche un servizio globale di gestione della sicurezza, sia tecnologico sia comprensivo dei processi di Risk Management, Incident Management, Continuous Improvement, e con le competenze per governare le normative ed i regolamenti che concorrono all'implementazione delle misure tecniche organizzative in ambito cybersecurity.
Adottando un'architettura di riferimento realizzata in cloud, ad esempio, un Managed Security Service Provider può fornire servizi minimizzando le attività di configurazione nei datacenter del Cliente, limitando la richiesta di infrastrutture on premises o nel cloud del cliente stesso. Il Managed Security Service Provider è in grado di mantenere e gestire un suo ambiente tecnologico, partendo da una corretta scelta dei vendor e delle partnership, ed essere in grado di fornire servizi che richiedono al massimo solo la distribuzione di agenti on premises al cliente, per realizzare servizi di Breach and Attack Simulation, Microsegmentazione,

Patch Management, da un unico punto ed essere così in grado di offrire una combinazione di tecnologie anti-ransomware interamente dal cloud. Tecnologie che potrà controllare e gestire per il cliente avvalendosi di competenze di alto livello che sarebbero altrimenti inaccessibili per costo.
Inoltre, avendo a disposizione tutti gli strumenti per la gestione della sicurezza, potrebbe farsi carico dell'intero ciclo di vita delle attività pianificate per la mitigazione dei rischi cyber, e dei processi di healthcheck periodici per garantire la compliance dei sistemi ad una baseline di sicurezza, offrendo quindi non soltanto un supporto tecnologico come servizio ma la vera e propria implementazione di un controllo di sicurezza, sollevando il cliente dall'onere di gestirne la complessità infrastrutturale, organizzativa e operativa.
Questa è la direzione che un Managed Security Service Provider dovrebbe percorrere nel prossimo futuro: poter offrire l''intero stack di competenze, framework di sicurezza e architetture per poter essere continuamente allineato nella risposta ai requisiti di sicurezza dei propri Clienti, mantenendo sempre un allineamento con le soluzioni di mercato.
La disponibilità di Managed Security Services è sicuramente una delle soluzioni in grado di risolvere le problematiche di carenza di personale nel settore cybersecurity e l'eccesso di complessità e costi da parte dei clienti per poter avere una buona protezione, a fronte della crescente complessità dell' offerta CyberSecurity , ma anche un'efficace risposta ai rischi posti in essere dalla continua evoluzione degli attaccanti.

Risk analysis by design: il metodo CRISP

Antonio Capodieci – Dipartimento di Ingegneria dell'Innovazione – Università del Salento
Roberto Paiano – Dipartimento di Ingegneria dell'Innovazione – Università del Salento
Luca Mainetti – Dipartimento di Ingegneria dell'Innovazione – Università del Salento

Abstract

La diffusione delle reti di sensori e attuatori IoT richiede una sempre maggiore attenzione alla sicurezza informatica e, di conseguenza, implica l'adozione di metodologie di analisi dei rischi cyber. Le reti IoT hanno una funzione sempre più importante sia nelle Smart City sia nei contesti industriali, diventando agenti attivi la cui manomissione potrebbe compromettere il funzionamento di interi sistemi. L'infrastruttura IoT può essere considerata, in sostanza, come un'infrastruttura critica. Nel contesto dei processi industriali e dell'automazione, e in particolare nella cosiddetta Industria 4.0, l'applicazione ormai intensiva di sistemi di controllo in reti interconnesse ha portato a un aumento delle minacce alla sicurezza delle informazioni per i sistemi di supervisione e acquisizione dati (SCADA) e per i sistemi di controllo distribuiti (DCS). Con la dovuta attenzione, si possono trovare interessanti parallelismi tra i sistemi di controllo remoto tipici dell'ambiente industriale e le reti di sensori IoT, rispetto ai quali i classici metodi di valutazione del rischio potrebbero non essere sufficienti. Di fatto si sta assistendo al superamento della storica dicotomia IT/OT e si sta andando verso un unico ambiente operativo interconnesso che necessita di specifici approcci strutturati.
Illustriamo, di seguito, una metodologia denominata CRISP (Cyber Risk Analysis in Industrial Process System Environment) che, attraverso un approccio "by design", permette di valutare sistematicamente il rischio legato alla manipolazione dei componenti connessi in rete. CRISP definisce un metodo in grado di guidare l'analisi strutturata (cioè legata ai processi) sia per il rischio legato alla manipolazione di un singolo elemento del sistema sia per determinare le conseguenze sull'intero sistema o su una porzione limitata dello stesso.

Introduzione

Il termine Industria 4.0 indica una tendenza dell'automazione industriale che integra alcune nuove tecnologie di produzione per migliorare le condizioni di lavoro, creare nuovi modelli di business e aumentare la produttività e la qualità degli impianti. Il termine si riferisce anche alla quarta rivoluzione industriale. Questa visione prevede che i sistemi cyber-fisici comprendano macchine intelligenti, sistemi di stoccaggio e impianti di produzione in grado, attraverso dispositivi IoT connessi, di scambiare autonomamente informazioni, attivare azioni e controllarsi a vicenda in modo indipendente. In questo scenario per l'analisi del rischio è fondamentale in una moderna gestione di sistemi interconnessi.
Definendo il rischio come "una funzione della probabilità che una determinata fonte di minaccia sfrutti una potenziale vulnerabilità e dell'impatto che ne deriverebbe in caso di sfruttamento riuscito della vulnerabilità", abbiamo definito una metodologia di valutazione del rischio nei sistemi cyber-fisici, al fine di contribuire alla progettazione di sistemi sicuri ed alla definizione di adeguate politiche di sicurezza e di prevenzione dei rischi. La valutazione del rischio risponde alle seguenti tre domande:

(I) Cosa può andare storto?
(II) Qual è la probabilità che vada storto?
(III) Quali sono le conseguenze?

Nel corso degli anni è stata elaborata un'ampia gamma di standard e documenti normativi relativi alla gestione e alla valutazione del rischio per i sistemi informatici. La norma ISO 31000:2009 (ISO, 2009) delinea linee guida generiche e non specifiche del settore sulla gestione del rischio. Il NIST SP 800-30 contiene una guida sulla gestione del rischio per i sistemi IT. Il NIST 800-37 fornisce un quadro di gestione del rischio per i sistemi informativi federali. La norma ISO/IEC 27005:2011 è, invece, uno standard per la gestione del rischio della sicurezza delle informazioni. Tuttavia, questi approcci non si prestano ad affrontare

integralmente scenari dove i sistemi IT si integrano con sistemi OT come quelli industriali e, soprattutto, non aiutano a rivedere i processi di business con un approccio di sicurezza by design.

Esistono altresì innumerevoli metodi di valutazione del rischio, in contesti strettamente industriali, legati ai sistemi cyber-fisici connessi (SCADA e IDS). Per ragioni di spazio non si possono illustrare dettagliatamente in questo contesto; tuttavia, un approccio certamente interessante sono le diverse metodologie che si richiamano ad una valutazione probabilistica dei rischi (PRA), associati a un'entità tecnologica ingegneristica complessa.
Nella PRA le conseguenze negative che possono derivare da un'azione malevola sono espresse numericamente, mentre il loro verificarsi è espresso in termini di probabilità. Vi sono diversi approcci che si rifanno a stime PRA valutando la probabilità di un insieme di scenari e stimando le loro conseguenze (FMEA, FMECA, FTA), oppure partendo dai guasti risalire alle loro conseguenze. Tuttavia, questi approcci o sono carenti di una visione complessiva delle conseguenze di un guasto su un solo componente oppure non prevedono una valutazione della combinazione dei guasti.
Un approccio PRA completo, come quello illustrato, dovrebbe utilizzare sia l'approccio induttivo sia quello deduttivo per ottenere un insieme completo di sequenze di incidenti. Walker sostiene la necessità di utilizzare tali approcci fin dalla fase iniziale di tutti i progetti di ingegneria per determinare il rischio tecnico del progetto.

La metodologia CRISP in sintesi

In un'infrastruttura IoT e negli impianti Industria 4.0, i processi sono guidati da un'unità di calcolo che fornisce i comandi necessari al corretto funzionamento dell'impianto e ne monitora lo stato. Le unità operative sono costituite da controllori interfacciati con sensori e attuatori di dispositivi meccanici. Questi possono essere gestiti da sistemo Cloud e/o da sistemi Edge, in grado di scambiare informazioni. In altre parole, non esiste un unico nodo controllore per l'intero sistema, ma diversi controllori dislocati per sezioni dell'infrastruttura: le informazioni scambiate dai sottosistemi vengono raccolte da appositi centralizzatori di supervisione.

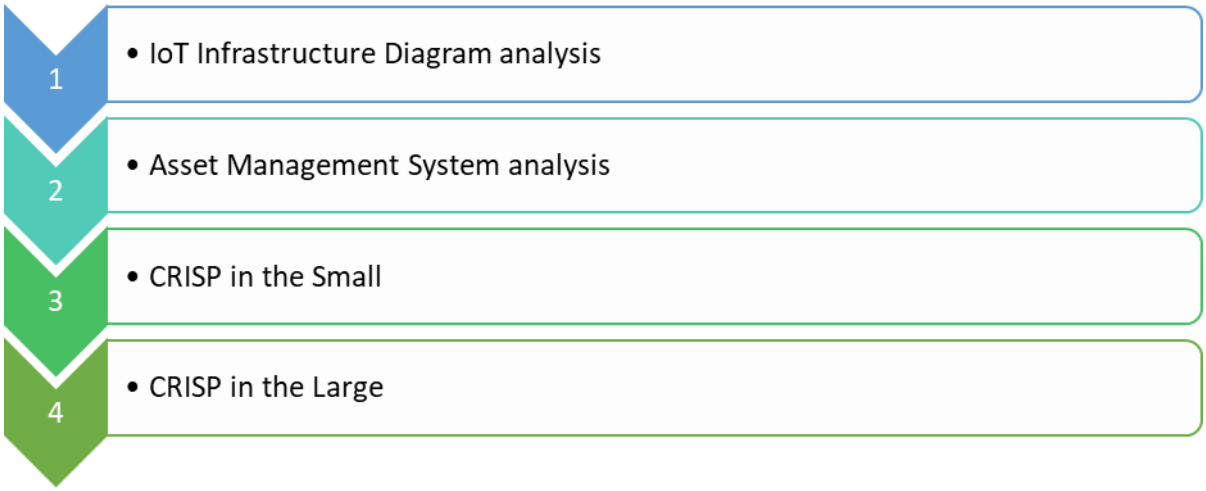

Figura 53 - CRISP - Cyber Risk Analysis in IoT Infrastructure

Sappiamo analizzando le kill chain che in una prima fase di un cyberattacco l'attaccante ottiene l'accesso al sistema e a un dispositivo collegato alla rete del sistema controllabile da remoto. In una seconda fase l'attaccante manipola il sistema, ad esempio modificando i valori forniti dai sensori o lo stato degli attuatori.
La CRISP si concentra sulla seconda fase: supponendo che si verifichi un'intrusione (è impossibile ridurre a zero il rischio di intrusione), è fondamentale cercare di ridurre i possibili danni. La CRISP mira a identificare,

in modo sistematico, come suggerito da Walker, le conseguenze della manomissione dell'impianto a seguito di un cyberattacco, analizzando sia le conseguenze globali, ovvero all'intero sistema (fase CRISP in Large) sia quelle locali, ovvero relative ad una singola sezione del sistema (fase CRISP in Small). In entrambe le fasi sono utilizzati come punto di partenza per la valutazione del rischio:

- L'IoT Infrastructure Diagram, ovvero i diagrammi dell'infrastruttura della rete di IoT da analizzare,
- l'Asset Management System, ovvero l'inventario dettagliato dei dispositivi installati nell'infrastruttura.

L'attuale evoluzione degli strumenti di asset management potrebbe aiutare ad affrontare il problema, ma sono insufficienti. Non considerano gli interi sistemi o impianti, ma solo i singoli elementi, non hanno una visione complessiva dei sistemi e delle interdipendenze tra i singoli componenti, né affrontano le conseguenze che i malfunzionamenti possono avere sui sistemi a livello globale.
La fase CRISP in Small è la prima analisi, fatta su tutti gli elementi "passibili di attacchi informatici" presenti nel sistema, al fine di valutare le conseguenze di manipolazioni su singoli dispositivi dell'infrastruttura o di un sistema relativamente semplice e modulare. In sostanza si basa su una struttura simile alla FMECA (Failure Modes, Effects and Critical Analysis), appositamente adattata all'analisi degli attacchi informatici.
La fase CRISP in the Large è l'analisi successiva, in grado di valutare le ripercussioni che le manipolazioni su uno o più dispositivi possono avere sull'intera infrastruttura. La metodologia si basa su una struttura simile a quella di una "Reverse HazOp" (Reverse Hazard and Operability analysis): partendo dall'identificazione di un potenziale "Top Event", traccia l'intera catena di causa-effetto fino a identificare le variabili che devono essere manipolate durante l'attacco. L'applicazione richiede come input la documentazione tipica dell'infrastruttura e il sistema di gestione degli asset. La CRISP può essere legata ai processi di business per i quali il sistema o l'impianto è stato ideato e, nella sua ultima formulazione, contiene anche uno specifico profilo BPMN 2.0 per disegnare processi di business "risk aware" con strumenti standard di Business Process Modeling.

In sintesi

La metodologia CRISP è composta da due fasi complementari, "in the Small" e " in the Large". La prima permette di individuare gli eventi pericolosi e le loro cause e conseguenze su ogni singolo componente, mentre la seconda permette di identificare gli eventi critici per ogni nodo. I risultati dell'applicazione della CRISP in the small individuano ai singoli componenti che sono, e/o possono essere, l'obiettivo di un attacco in grado di generare gli eventi critici.
L'adozione del CRISP consente di analizzare sistematicamente e puntualmente un intero sistema sia in termini di componenti installati sia in termini di possibili conseguenze di deviazioni indesiderate.
La CRISP ha alcune caratteristiche operative che vanno considerate:

(i) La complessità e il costo dell'applicazione del metodo per sistemi di grandi dimensioni.
(ii) Lo sforzo in termini di risorse richiesto per l'aggiornamento dell'analisi e dei processi con l'evoluzione dei sistemi.

Tuttavia, questi aspetti possono essere uno stimolo per migliorare la gestione dell'infrastruttura anche in relazione agli aspetti manutentivi e normativi.
In conclusione, è importante ribadire che la sicurezza è un processo - insieme di attività, ruoli e responsabilità, approcci e metodologie - e non solo l'uso di tecnologie o di un approccio esclusivamente tecnologico. Inoltre, la sicurezza deve evolvere insieme all'organizzazione e ai sistemi, e deve essere orientata al monitoraggio continuo e razionale dei processi aziendali. Da questo punto di vista, la CRISP supporta l'analisi dei rischi determinando in dettaglio le vulnerabilità di ciascun componente e, contemporaneamente, di un intero sistema complesso al fine di implementare una adeguata strategia di protezione.

BIBLIOGRAFIA

[1] M. Henrie, "Cyber security risk management in the SCADA critical infrastructure environment," Engineering Management Journal, vol. 25, no. 2, pp. 38–45, 2013.
[2] NIST, Special Publication 800-82. Guide to Industrial Control Systems (ICS) Security, 2011.

[3] M. Cheminod, L. Durante, and A. Valenzano, “Review of security issues in industrial networks,” IEEE Transactions on Industrial Informatics, vol. 9, no. 1, pp. 277–293, 2013.
[4] S. Kaplan and B. J. Garrick, “On The Quantitative Definition of Risk,” Risk Analysis, vol. 1, no. 1, pp. 11–27, 1981.
[5] Walker, Mark, and Ravi Kapadia. "Integrated Design of On-line Health and Prognostics Management." Annual Conference of the Prognostics and Health Management Society. 2009.
[6] A. Capodieci, V. Capalbo, G. Filitti and A. Caruso, " C.Ri.S.P. - Cyber Risk Analysis in Industrial Process System Environment", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 8, Issue 4, July - August 2019, pp. 001-009, ISSN 2278-6856.

Quantum Computing in Automotive Security

Vita Santa Barletta, Danilo Caivano, Mirko De Vincentiis
Dipartimento di Informatica, Università degli Studi di Bari Aldo Moro
{vita.barletta, danilo.caivano, mirko.devincentiis}@uniba.it

Abstract

L'attuale contesto di innovazione tecnologica e trasformazione digitale richiede di garantire la sicurezza dei sistemi preservandone la riservatezza, l'integrità e la disponibilità. In tale scenario la mobilità intelligente rappresenta un elemento fondamentale e pone nuove sfide per la definizione di modelli come quello della Mobility-as-a-Service. Pertanto, per rispondere alle esigenze di sicurezza derivanti dall'integrazione di tecnologie emergenti e necessarie per la realizzazione del processo di digitalizzazione e trasformazione che l'industria automobilistica sta vivendo è necessario analizzare e investigare nuovi sistemi di intrusion detection (IDSs) che permettano di ridurre il tempo di elaborazione per l'identificazione di attacchi e di rispondere adeguatamente alla minaccia. Di seguito, vengono presentati i primi risultati di una sperimentazione eseguita con tecnologie quantistiche per poter definire nuovi modelli di detection in ambito automotive ma soprattutto di mobilità intelligente.

Introduzione

Si stima che entro il 2030 il numero di auto connesse raggiungerà i 700 milioni e il numero di veicoli autonomi i 90 milioni [1]. Da un lato ciò offre la possibilità di migliorare le funzionalità, i servizi forniti e facilitare una guida sicura; dall'altra parte, invece, ogni punto di connessione rappresenta un punto di accesso al veicolo che può essere sfruttato da un attaccante, insieme ad errori presenti nel codice, per compromettere le funzionalità critiche del veicolo. Kim et al. [2] identificano tre categorie per classificare gli attacchi (
Figura 54):

- attacchi al sistema di controllo autonomo e che riguardano le ECUs (Electronic Control Units) e i vari protocolli di comunicazione come il CAN (Control Area Network), LIN (Local Interconnect Network), Flexray e Radio Frequency [3]–[5];
- attacchi alle componenti del sistema di guida autonoma, come ad esempio GPS (Global Positioning System), Video Camera, LIDAR (Light detection and ranging), Central computer e sensori [6]–[8];
- attacchi al veicolo connesso, Vehicle-to-Everything (V2X), che riguardano l'Infotainment e la sicurezza del veicolo e delle persone durante la guida [9], [10].

Diverse le soluzioni implementate per poter difendersi da tali attacchi e riguardano principalmente sistemi per il rilevamento delle intrusioni e delle anomalie, e la sicurezza dei protocolli inerenti alla comunicazione delle varie componenti.
Emerge, però, la necessità non solo di rilevare possibili vulnerabilità ma anche di poter definire risposte adeguate a tali minacce in modo da preservare la sicurezza fisica dei passeggeri. Ciò comporta, inevitabilmente, l'applicazione di controlli di sicurezza nelle tre unità operative di sicurezza (Detection, Response, Prevention - Figura 54), ma anche la possibilità di analizzare i diversi fattori derivanti da un contesto come quello della Smart City per migliorare la sicurezza dei veicoli a guida autonoma e offrire servizi efficienti all'interno della mobilità intelligente.

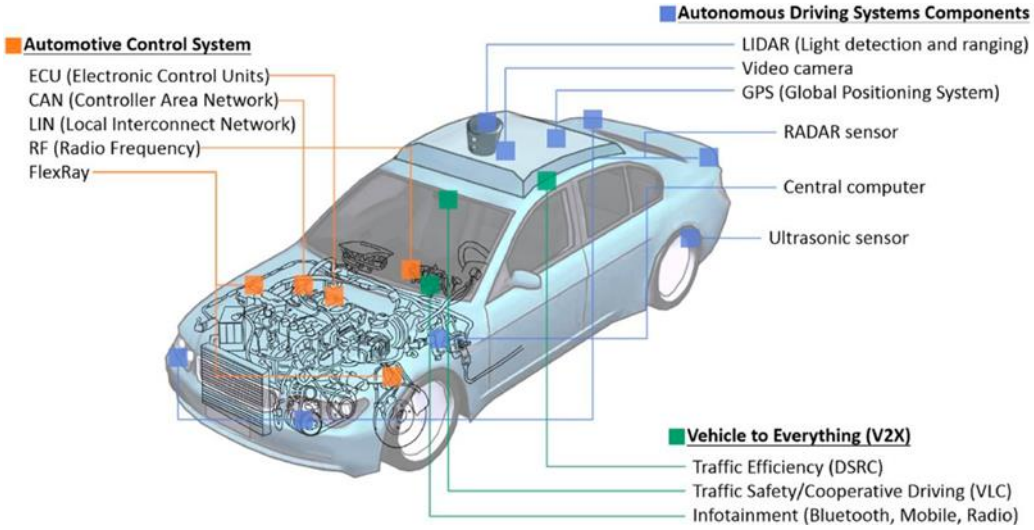

Figura 54 - Struttura dei veicoli a guida autonoma [2]

Pertanto, considerando, la mole di dati dei veicoli connessi nella prossima sezione presentiamo una prima analisi dell'integrazione di tecnologie quantistiche per poter migliorare la fase di detction, ma soprattutto per iniziare a focalizzarci sulla definizione di attività di risposta. In particolare, durante questa prima fase, sono state prese in considerazione le vulnerabilità sul protocollo CAN al fine di valutare come tale tecnologia possa migliorare le attività di difesa.

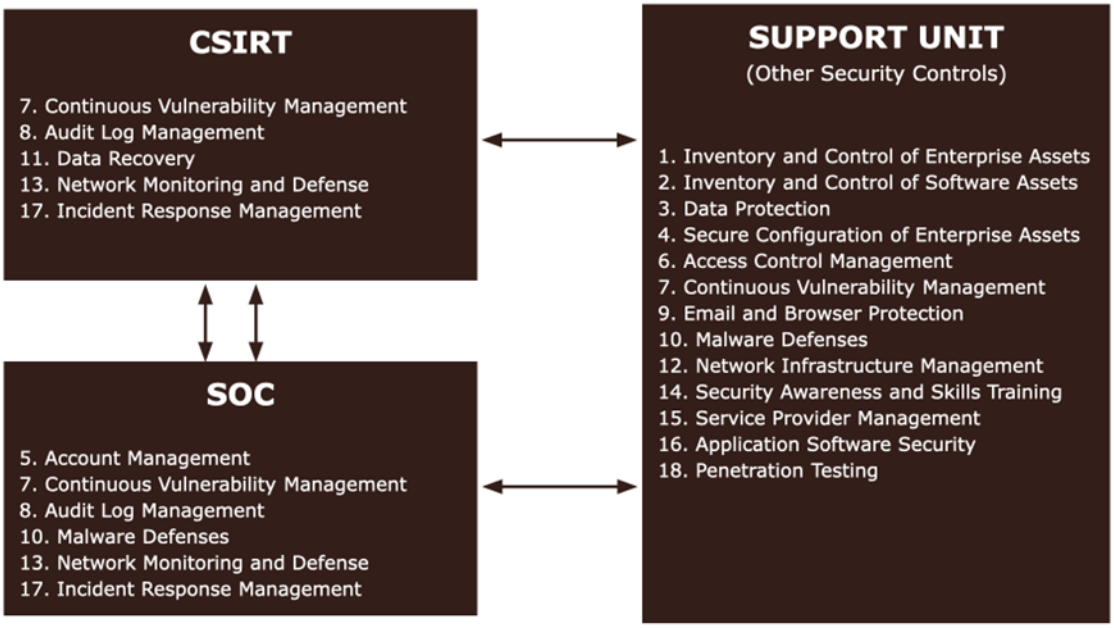

Figura 55 - Unità operative di sicurezza [11]

Quantum Computing per la detection di attacchi sul CAN bus

Il protocollo Controller Area Network (CAN) [12] è responsabile della comunicazione tra le varie centraline (Electronic Control Unit). Le ECU si scambiano messaggi critici e che potrebbero essere sfruttati da attaccanti per causare comportamenti inattesi al veicolo oppure ottenere informazioni sul guidatore (tipo di guida, destinazione, ecc.). Ciò accade a causa della mancanza di meccanismi crittografici come, ad esempio, l'autenticazione e la cifratura dei messaggi che vengono scambiati tra le diverse ECU. Il risultato comporta la possibilità di effettuare attacchi di tipo *Denial of Service (DoS)*, *Eavesdropping, Injection* e *Replay* [8].
L'attacco DoS sfrutta la mancanza di meccanismi di autenticazione per poter inviare messaggi ad alta priorità con l'obiettivo di congestionare il bus negando l'invio di messaggi da parte di ECU legittime. Un eavesdropper, invece, avendo un accesso ad una ECU (oppure tramite porta OBD-II) potrebbe ottenere il traffico inviato da altre ECU.
La letteratura, considerando tali necessità di sicurezza, presenta diversi lavori di ricerca con l'obiettivo di identificare attacchi informatici e prevenire l'insorgere di questi. Per quanto concerne la detection, vengono utilizzati gli Intrusion Detection Systems (IDSs) che sfruttano algoritmi di Machine Learning (ML) o Deep Learning (DL). Tali soluzioni pongono diversi limiti nel contesto automotive a causa della bassa potenza computazionale e del basso consumo elettrico della ECU.
Viceversa, le tecniche di prevenzione riguardano la creazione di algoritmi crittografici e di autenticazione così da porre rimedio alle carenze di sicurezza del protocollo CAN. Anche in questo caso, però, è necessario sviluppare algoritmi considerati *lightweight* che quindi abbiano un basso consumo e una bassa potenza computazionale. Ad esempio, in [13] i ricercatori hanno sviluppato un sistema di tipo challenge-based nel quale una ECU, prima di inviare un messaggio sul bus CAN, deve autenticarsi ad un'altra ECU predisposta per questo compito. Altre tecniche, invece, consistono nell'utilizzare sistemi crittografici al fine di rendere il messaggio CAN sicuro. Tuttavia, la chiave che viene utilizzata per cifrare il messaggio potrebbe essere identificata tramite tecniche di reverse engineering sulla ECU, nel momento in cui non vengono applicate corrette tecniche difensive.
Oggigiorno, però, il Quantum Computing sta aprendo la strada per lo sviluppo di tecniche difensive sempre più sofisticate. La velocità dei computer quantistici potrebbe essere sfruttata per creare IDS che riducano il tempo di training e prediction. Nel contesto della mobilità intelligente, ciò risulta fondamentale per poter identificare e prevenire specifiche tipologie di attacco ma anche nuovi pattern di attacco a tale contesto. Ciò nasce anche dalla concezione del veicolo come sistemi critico in quanto, un attacco potrebbe compromettere la vita del guidatore e/o passeggeri.
È stato condotto un primo lavoro di ricerca, "*Quantum Optimization for Fast CAN Bus Intrusion Detection*" [14], per comprendere in termini quantitativi come tecnologie basate su l'ottimizzazione quantistica potessero aiutare ad implementare nuovi modelli di sicurezza e ridefinire il ciclo di detection, response e prevention, in accordo agli obiettivi del progetto "*Secure Safe Apulia - Regional Security Center*".
In particolare, il seguente lavoro mostra come, prendendo in esame QBoost [15], classificatore binario che sfrutta il Quantum Annealing, e un algoritmo di ML ampiamente utilizzato per identificare attacchi, la Support Vector Machine (SVM) [16].
Quantum Annealing è utilizzato per identificare la miglior soluzione con minore energia, ed è applicato per problemi di ottimizzazione e di samplig probabilistico.
Di seguito vengono riportati i risultati dei due classificatori (QBoost e SVC) utilizzando due tipologie di attacco sul CAN bus: DoS e Fuzzy. QBoost surclassa in termini di tempo di predizione e di addestramento il classificatore SVC (Tabella 9), e nello specifico considerando il DoS Dataset (Tabella 10). Inoltre, anche la predizione degli attacchi è migliore rispetto alla SVM.

Tabella 9 - Risultati performance classificatori - DoS Dataset

Classifier	Average training time (s)	Average prediction time (s)
SVC	68.6735	2.5609
QBoost	26.1415	0.0275

Tabella 10 - Risultati performance classificatori - Fuzzy Dataset

Classifier	Average training time (s)	Average training time (h)	Average prediction time (s)	Average prediction time (m)
SVC	5933.2840	1.6481	431.4609	7.191
QBoost	25.7134	0.0071	0.1462	0.0024

Considerando invece, le metriche di accuracy, precision, recall ed F1-Score, dalla Tabella 11 possiamo notare che i due classificatori raggiungono lo stesso risultato sul DoS dataset, ma cambiano in termini di training e prediction sul dataset Fuzzy. I risultati migliori sono evidenziati in grigio.

Tabella 11 - Risultati performance classificatori - DoS e Fuzzy Dataset

Dataset	Set	Classifier	Accuracy	Precision	Recall	F1-score
DoS	Train	SVC	1.0	1.0	1.0	1.0
		QBoost	1.0	1.0	1.0	1.0
	Test	SVC	1.0	1.0	1.0	1.0
		QBoost	1.0	1.0	1.0	1.0
Fuzzy	Train	SVC	0.9858	0.9945	0.9891	0.9918
		QBoost	0.9778	0.9988	0.9757	0.9871
	Test	SVC	0.9716	0.9785	0.9892	0.9838
		QBoost	0.9756	0.9959	0.9760	0.9858

Conclusioni

In questo primo lavoro condotto per migliorare i modelli di sicurezza all'interno della mobilità intelligente, i risultati mostrano che l'applicazione di tecniche quantistiche potrebbe migliorare notevolmente i tempi di detection di un attacco e di conseguenza ridurre i tempi di risposta e l'impatto sulla sicurezza dei passeggeri e del veicolo.
Naturalmente, lavorando su questa direzione, abbiamo la necessità di sviluppare componenti quantistiche da integrare all'interno degli attuali sistemi per il monitoraggio delle Smart City e della mobilità intelligente, e di ridefinire e/o proporre controlli di sicurezza.

Riferimenti

[1] N. Huq, C. Gibson, V. Kropotov, and R. Vosseler, "Cybersecurity for Connected Cars".
[2] K. Kim, J. S. Kim, S. Jeong, J.-H. Park, and H. K. Kim, "Cybersecurity for autonomous vehicles: Review of attacks and defense," Comput. Secur., vol. 103, p. 102150, 2021, doi: https://doi.org/10.1016/j.cose.2020.102150.
[3] J. Takahashi et al., "Automotive attacks and countermeasures on lin-bus," J. Inf. Process., vol. 25, pp. 220–228, 2017.
[4] J. M. Ernst and A. J. Michaels, "LIN Bus Security Analysis," in IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society, 2018, pp. 2085–2090. doi: 10.1109/IECON.2018.8592744.
[5] M. Wolf, A. Weimerskirch, and C. Paar, "Security in automotive bus systems," in Workshop on Embedded Security in Cars, 2004, pp. 1–13.
[6] S. Chandrasekaran, K. Ramachandran, S. Adarsh, and A. K. Puranik, "Avoidance of Replay attack in CAN protocol using Authenticated Encryption," in 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2020, pp. 1–6.
[7] D. Nassi, R. Ben-Netanel, Y. Elovici, and B. Nassi, "MobilBye: attacking ADAS with camera spoofing," ArXiv Prepr. ArXiv190609765, 2019.
[8] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, "Cybersecurity challenges in vehicular communications," Veh. Commun., vol. 23, p. 100214, 2020.
[9] Tencent Security Keen Lab, "Experimental Security Assessment of Mercedes-Benz Cars." [Online]. Available: https://keenlab.tencent.com/en/2021/05/12/Tencent-Security-Keen-Lab-Experimental-Security-Assessment-on-Mercedes-Benz-Cars/
[10] Tencent Security Keen Lab, "Experimental Security Assessment on Lexus Cars." [Online]. Available: https://keenlab.tencent.com/en/2020/03/30/Tencent-Keen-Security-Lab-Experimental-Security-Assessment-on-Lexus-Cars/
[11] M. T. Baldassarre, V. S. Barletta, D. Caivano, D. Raguseo, and M. Scalera, "Teaching Cyber Security: The HACK-SPACE Integrated Model," in ITASEC, 2019.
[12] Bosh, "CAN Specification Version 2.0," Robert Bosch GmbH Postfach, vol. 50, 1991.
[13] G. Costantino, I. Matteucci, and D. Morales, "EARNEST: A challenge-based intrusion prevention system for CAN messages," in 2020 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), 2020, pp. 243–248.
[14] D. Caivano, M. De Vincentiis, F. Nitti, and A. Pal, "Quantum Optimization for Fast CAN Bus Intrusion Detection," in Proceedings of the 1st International Workshop on Quantum Programming for Software Engineering, New York, NY, USA, 2022, pp. 15–18. doi: 10.1145/3549036.3562058.
[15] H. Neven, V. S. Denchev, G. Rose, and W. G. Macready, "Training a Binary Classifier with the Quantum Adiabatic Algorithm," 2008, doi: 10.48550/ARXIV.0811.0416.
[16] C. Cortes and V. Vapnik, "Support-vector networks," Mach. Learn., vol. 20, no. 3, pp. 273–297, Sep. 1995, doi: 10.1007/BF00994018.

Enhancing Security through Explainable Threat Intelligence

Tommaso Di Noia – Laboratori di Sistemi Informativi – Politecnico di Bari
Claudio Pomo – Laboratori di Sistemi Informativi – Politecnico di Bari

Abstract

L'intelligenza artificiale (AI) svolge un ruolo fondamentale nella lotta contro gli attacchi alla sicurezza di qualsiasi istituzione, indipendentemente dal fatto che si tratti di un'azienda o di un Paese. A causa del gran numero di avvisi e segnalazioni che sommergono i team di sicurezza, oltre al rilevamento delle minacce è di fondamentale importanza la progettazione di modelli per la loro rappresentazione e comprensione. I sistemi di spiegabilità dell'intelligenza artificiale stanno guadagnando terreno, ma si può fare molto per renderli ancora più efficaci. La nostra ricerca mira a migliorare i sistemi attualmente disponibili fornendo diverse forme di spiegazione, a seconda dei diversi utenti finali, e la possibilità di manipolare interattivamente le rappresentazioni grafiche basate su tecniche di Visual Data Mining.

Introduzione

In uno scenario globale in cui le minacce ai sistemi informativi aumentano di giorno in giorno, la difesa delle infrastrutture critiche (CI) è di fondamentale importanza. Una CI è un sistema, una risorsa, un processo, un insieme di risorse o processi, la cui distruzione, interruzione o indisponibilità anche parziale o temporanea ha l'effetto di indebolire significativamente l'efficienza e il normale funzionamento di qualsiasi servizio vitale per il Paese. In quest'ultimo caso, sono a rischio anche la sicurezza e il sistema economico-finanziario e sociale, compresi gli apparati della pubblica amministrazione centrale e locale.
In questo contesto, la Cybersecurity gioca un ruolo sempre più importante nella protezione delle infrastrutture e dei loro dati. L'Intelligenza Artificiale (AI) ha un ruolo di primo piano: i sistemi utilizzati per rilevare le minacce possono essere ancora più precisi se dotati di moduli intelligenti progettati secondo le più moderne tecniche di Machine Learning (ML) e AI. Questi moduli devono essere in grado di notificare intuizioni intelligenti in grado di identificare e dare priorità alle minacce in modo accurato.
Esaminando le minacce provenienti da diverse fonti di traffico dati, l'AI può fare inferenza, aiutando così l'utente finale a determinare le anomalie e a ridurre drasticamente i tempi di reazione. L'identificazione di attacchi dannosi non è sempre banale, poiché anche gli aggressori, oltre alle tecniche classiche basate su compressione, polimorfismo, offuscamento e impersonalizzazione, utilizzano tecniche avanzate di AI che possono eludere i più moderni sistemi di rilevamento.

Oltre al rilevamento delle minacce, è di fondamentale importanza la progettazione di modelli per la loro rappresentazione e comprensione. Nel rapporto annuale di Cisco sulla Cybersecurity del 2022 emerge che in media il 44% degli avvisi di sicurezza presi in carico dai dipartimenti di sicurezza aziendali non vengono approfonditi. Ciò è certamente dovuto al gran numero di avvisi e segnalazioni che sommergono i team di sicurezza, i quali devono scegliere con cura quali avvisi valgono la pena di essere esaminati e quali invece possono essere tralasciati, sulla base della spiegazione delle ragioni di quell'avviso. In questo scenario, l'adozione di tecniche di Explainable AI, per una spiegazione esaustiva delle minacce, può essere uno strumento utile per supportare i team di sicurezza nel prendere le giuste decisioni.
La spiegabilità, quindi, ha un ruolo fondamentale, in quanto illustra il motivo del rilevamento. L'utente può così scegliere in modo più consapevole le azioni difensive da intraprendere. Tuttavia, la maggior parte dei sistemi di Explainability sono progettati per utenti esperti di ML, in grado di comprendere l'output restituito da tali sistemi, che può essere anche in formato tabellare o grafico.

In questo report presentiamo un approccio, che mira a migliorare gli attuali sistemi fornendo spiegazioni personalizzate e dando all'utente la possibilità di interagire con esse, al fine di favorire il processo di senso e di decisione [5].

Approccio

Nel settore della sicurezza informatica, i sistemi di spiegabilità dell'intelligenza artificiale sarebbero più efficaci se l'utente potesse:

1) cogliere facilmente il significato della spiegazione;
2) interagire con una rappresentazione visiva della spiegazione delle minacce identificate.

Inoltre, occorre considerare le diverse competenze degli utenti che interagiscono con il sistema, nonché i compiti che svolgono. Si pensi, ad esempio, alla Quarta Rivoluzione Industriale, in cui le aziende stanno subendo una trasformazione digitale, con un ampio uso della rete per fornire servizi, comunicare e condividere risorse distribuite, favorendo e aumentando anche l'interazione tra i vari soggetti a fini sociali, economici e lavorativi. Questa digitalizzazione apre il fronte ad attacchi criminali volti a compromettere la riservatezza, l'integrità e la disponibilità delle risorse e delle informazioni. Le tradizionali misure di sicurezza informatica non sono sufficienti, in quanto le minacce non sono più limitate a pochi dispositivi e richiedono più delle competenze di un dipartimento IT Security. È necessario un team dedicato di Cybersecurity in cui ogni membro ha il proprio know-how e i propri compiti.
La figura del Security Incident Manager potrebbe così monitorare e analizzare continuamente, con una visione a 360 gradi, tutti i problemi di sicurezza dell'infrastruttura IT. Il Penetration Tester, noto anche come "hacker etico", trova e sfrutta le vulnerabilità di un sistema informatico. Lo specialista in rischi informatici e conformità assicura che l'azienda sia sempre aggiornata su tutti i requisiti normativi e di licenza. Il Cybersecurity Strategist è responsabile della definizione della roadmap strategica per la Cybersecurity, interfacciandosi con le funzioni aziendali principali e i team tecnologici.

Questi sono solo ruoli esemplificativi secondo l'azienda Stichkman Cybersecurity[1], ma mostrano come questi quattro utenti sfrutterebbero un sistema di ML dotato di un modulo AI Explainability per il loro lavoro in base ai diversi obiettivi, compiti e know-how. Pertanto, hanno bisogno di diverse rappresentazioni dei risultati restituiti dal sistema e di diversi strumenti di analisi dei dati.
A causa dell'uso diffuso della rete e delle risorse distribuite condivise, anche i dipendenti dell'azienda, non direttamente coinvolti nella gestione della sicurezza, rappresentano un punto debole di difesa dagli attacchi. Questi dipendenti di solito ricevono direttamente un avviso che li avverte che stanno per compiere un'azione potenzialmente non sicura, ma potrebbero trascurarlo perché la sua formulazione è troppo tecnica e non corrisponde alla loro security awareness.
Riassumendo, come primo obiettivo verso i sistemi di spiegabilità dell'intelligenza artificiale più usabili ed efficaci, i risultati dovrebbero essere espressi da spiegazioni che implementino le proprietà suggerite da Grice[1]. Inoltre, per consentire agli utenti di approfondire le ragioni di un avviso, devono essere supportati nell'esplorazione dei dati di spiegabilità.
La maggior parte degli attuali sistemi di spiegabilità dell'intelligenza artificiale non dispone di una potente interfaccia utente per fornire spiegazioni con visualizzazioni diverse, a seconda dell'utente che interagisce con essi. Questo tipo di strumenti e tecniche per assistere le persone durante l'analisi dei dati, che in realtà è un compito gravoso, sono studiati dal campo di ricerca interdisciplinare Visual Data Mining (VDM), che comprende, tra l'altro, tecniche di Data Mining e di Information Visualization [2]. Il VDM combina i punti di forza dei metodi automatici e la capacità umana di percepire visivamente modelli e tendenze per aiutare le persone ad analizzare dati complessi di grandi dimensioni. Il VDM si riferisce, inoltre, a metodi per

[1] https://www.stickman.com.au/services/strategy/cyber-security-by-design/

supportare l'esplorazione di grandi insiemi di dati, consentendo agli utenti di interagire direttamente con le rappresentazioni visive dei dati e di modificare dinamicamente i parametri per vedere come influiscono sui dati visualizzati. Lo scopo è quello di dare un senso a insiemi di dati molto grandi e complessi, combinando "l'analisi automatizzata dei dati con le visualizzazioni interattive per una comprensione, un ragionamento e un processo decisionale efficaci sulla base di insiemi di dati molto grandi e complessi" [3]. La presentazione grafica dei dati consente agli utenti di scoprire modelli specifici, nonché proprietà nuove e utili nei dati, le loro correlazioni e anche di rilevare eventuali deviazioni dai valori previsti.

Per perseguire questa strategia, il sistema di detection poterebbe essere dotato delle seguenti componenti:

- **Intelligent inference module**: è un componente di sicurezza reattivo che utilizza tecniche di AI per determinare se una minaccia è reale o meno. È in grado di analizzare il traffico proveniente da diverse fonti. Il modulo elabora il traffico di dati utilizzando tecniche di ML ed è in grado di rilevare le intrusioni sulla base di informazioni provenienti da file di registro e flussi di rete, al fine di determinare l'entità del danno e rintracciare l'aggressore. Il modulo è in grado di prevenire attacchi futuri simili e di riconoscere e prevenire le attività dannose attraverso metodi di ML basati sulla rete o sull'host.
- **Explainable module**: elabora i dati del modulo di inferenza, utilizzando diversi algoritmi di spiegabilità e li fornisce al modulo di interfaccia utente. A tal proposito, ad esempio, ProfWeight è un algoritmo per trasferire informazioni da una rete neurale profonda pre-addestrata con un'elevata accuratezza di test a un modello interpretabile più semplice o a una rete molto superficiale di bassa complessità e con un'accuratezza di test a priori bassa [4].
- **Threat Visualizer module**: riceve in ingresso la spiegazione generata dal modulo Explainable e le rappresenta graficamente. L'interfaccia utente può essere personalizzata proponendo diverse tecniche VDM e widget in base ai compiti e alle conoscenze dell'utente. Le spiegazioni vengono "riformulate" per creare un messaggio che possa essere colto anche da chi non è esperto di ML. Le tecniche VDM consentono all'utente di analizzare i dati alla base del rilevamento, aiutandolo così a decidere se ignorarlo o meno.

In sintesi

Le tecniche tradizionali di rilevamento delle intrusioni, come i firewall, i meccanismi di controllo degli accessi e i meccanismi di crittografia, presentano limiti. Tali sistemi non sono più in grado di proteggere completamente sistemi complessi da attacchi sempre più sofisticati. Inoltre, la maggior parte dei sistemi basati su queste tecniche soffre di un alto tasso di rilevamento di falsi positivi e falsi negativi e di una mancanza di adattamento continuo ai cambiamenti del comportamento dannoso. In questo contesto, il ML ha fornito un grande supporto, in quanto le tecniche di ML sono state applicate al problema del rilevamento delle intrusioni per migliorare i tassi di rilevamento e l'adattabilità.

Siamo certi che l'approccio proposto consentirebbe agli utenti finali di essere più efficaci in nell'identificazione della minaccia, ricevendo informazioni dettagliate sul processo decisionale dell'algoritmo di spiegabilità, che è anche una componente chiave per promuovere la fiducia nei sistemi di intelligenza artificiale.

[1] Herbert P Grice. Logic and conversation. *In Syntax and semantics 3: Speech arts, pages 41–58.*, New York: Academic Press, 1975.
[2] Simeon Simoff, Michael H Bo¨hlen, and Arturas Mazeika. *Visual data mining: theory, techniques and tools for visual analytics*, volume 4404. Springer Science & Business Media, 2008.
[3] Daniel Keim, Jo¨rn Kohlhammer, Geoffrey Ellis, and Florian Mansmann. Mastering the information age: solving problems with visual analytics. 2010.

[4] Amit Dhurandhar, Karthikeyan Shanmugam, Ronny Luss, and Peder A Olsen. Improving simple models with confidence profiles. In *Advances in Neural Information Processing Systems*, pages 10296–10306, 2018.
[5] Vigano, Luca, and Daniele Magazzeni. "Explainable security." *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2020.

2022 Devo SOC Performance Report™ - Sommario

Il quarto “Devo SOC Performance ReportTM” annuale mostra che i problemi che le organizzazioni hanno dovuto affrontare dall’inizio della pandemia globale all’inizio del 2020 continuano a influenzare le prestazioni del SOC, comprese le sfide nell’assunzione e nel mantenimento dei talenti del SOC. Basato su un sondaggio indipendente condotto nel settembre 2022 su oltre 1.000 professionisti della cybersecurity a livello globale, commissionato da Devo, il report esamina le tendenze e le sfide attuali dei SOC.

Il report 2022 analizza i risultati del sondaggio presentando le risposte dei leader e dei membri del personale SOC fianco a fianco. Le disparità in alcune aree chiave dimostrano chiaramente che i problemi che le organizzazioni hanno dovuto affrontare dall’inizio della pandemia globale all’inizio del 2020 continuano a influenzare le prestazioni del SOC, comprese le difficoltà nell’assumere e trattenere i talenti SOC durante la Grande Dimissione in corso.

Quasi tutti i professionisti intervistati ritengono che il SOC sia importante per la strategia di cybersecurity della loro organizzazione. Infatti, il 77% degli intervistati afferma che il SOC è “molto importante” o “essenziale” per la propria organizzazione. Questo dato rappresenta un leggero aumento rispetto al sondaggio del 2021, in cui il 73% degli intervistati teneva in grande considerazione il proprio SOC.

Inoltre, quasi il 90% degli intervistati giudica il proprio SIEM da “efficace” a “molto efficace” e il 25% lo valuta con un punteggio di 9 o 10 su una scala di 10 punti. Questi risultati, compreso il fatto che solo il 3% degli intervistati lavora per
organizzazioni che non hanno implementato un SIEM evidenziano il ruolo significativo e centrale che questa tecnologia svolge per la stragrande maggioranza dei SOC.

La cattiva notizia? Quasi un terzo degli intervistati cita la mancanza di visibilità sull’infrastruttura di sicurezza informatica come un ostacolo al successo. La visibilità è l’ingrediente di base più cruciale per il successo della cybersecurity: è necessario vedere cosa sta accadendo prima che sia troppo tardi, in modo da poter rispondere efficacemente.

La formazione, l’assunzione e il mantenimento di personale qualificato sono un altro punto dolente. Non ci sono abbastanza esperti di sicurezza e questo mette sotto pressione gli analisti SOC, che sono esausti a causa dei crescenti carichi di

lavoro e dei troppi allarmi. Secondo gli intervistati, il tempo medio necessario per coprire una posizione è di sette mesi, mentre il 15% dei leader SOC afferma che ci vogliono due anni o più per coprire un ruolo SOC.

Ma gli intervistati indicano anche l'automazione della forza lavoro come un modo efficace per alleviare il dolore degli analisti SOC. Le funzionalità SIEM su scala cloud per l'ingestione dei dati, le funzionalità di interrogazione ad alte prestazioni e un'interfaccia utente intuitiva sono strumenti che possono aiutare gli analisti a lavorare più velocemente e a individuare più rapidamente le minacce.

In sintesi, le risposte al sondaggio 2022 dimostrano che i membri del personale SOC continuano a soffrire notevolmente durante lo svolgimento del loro lavoro di importanza critica e altamente stressante. I risultati indicano che i leader dei SOC e i loro team continuano a lottare con diverse sfide in corso, tra cui:

- Allineamento degli obiettivi del SOC e delle esigenze aziendali
- Ostacoli al successo del funzionamento del SOC
- I motivi dell'inefficacia del SOC
- Le continue sofferenze dei lavoratori SOC e le cause che le determinano
- I lavoratori SOC che si licenziano o prendono seriamente in considerazione l'idea di farlo, e la difficoltà di sostituirli

Si legga il rapporto completo per comprendere più a fondo le sfide che i SOC e i lavoratori SOC devono affrontare. C'è ancora molto lavoro da fare per affrontare le prestazioni dei SOC e i numerosi problemi di fondo che le influenzano negativamente. Questo report fornisce ai leader e al personale dei SOC, nonché ai responsabili del programma generale di cybersecurity della loro organizzazione, una grande quantità di informazioni da tenere in considerazione per migliorare le prestazioni dei SOC e ridurre le sofferenze degli analisti.

2022 Devo SOC Performance Report™ - INGLESE

Devo
255 Main Street
Suite 702
Cambridge, MA 02142

Devo is the only cloud-native logging and security analytics platform that releases the full potential of your data to empower bold, confident action. With unrivaled scale to collect all of your data without compromise, speed to give you immediate access and answers, and clarity to focus on the signals that matter most, Devo is your ally in protecting your organization today and tomorrow. Devo is headquartered in Cambridge, Mass. Learn more at www.devo.com.

THREAT INTELLIGENCE AUTOMOTIVE: Secure Safe tra AI e collaborazione

Mario Direnzo – Responsabile sviluppo software & sistemi informativi

La Threat Intelligence nel mondo IT e quella nel mondo Automotive hanno alcune somiglianze, ma anche alcune importanti differenze: l'ambito IT si concentra sulle minacce informatiche che riguardano i sistemi informatici, come i computer, i server e le reti, mentre l'ambito automotive si concentra sulle minacce che riguardano i veicoli connessi e le infrastrutture connesse, come i sistemi di bordo, le reti di comunicazione e le infrastrutture di ricarica, con particolare attenzione alla raccolta, analisi e utilizzo delle informazioni su minacce potenziali, incluse le vulnerabilità software e hardware presenti nei sistemi di bordo dei veicoli, il monitoraggio delle minacce emergenti e la creazione di strategie di difesa proattive per prevenire gli attacchi.
Una delle maggiori sfide nell'ambito della Threat Intelligence nel dominio automotive è data dal continuo aumento del numero e della complessità dei sistemi di bordo, oltre che delle infrastrutture connesse che determinano un vertiginoso aumento della quantità di dati generati in un ambito estremamente distribuito, con una conseguente maggiore superficie di attacco per i criminali informatici ed una aumentata complessità di raccolta di dati dal campo.
Per le aziende del settore automotive affrontare questo scenario identificando e prevenendo le minacce è reso ulteriormente più difficile dalle aziende fornitrici di componentistica e sistemi automotive che spesso non collaborano tra loro per la cybersecurity: se le aziende fornitrici non condividono informazioni sulle vulnerabilità e sulle minacce emergenti, potrebbero sviluppare soluzioni di sicurezza parziali o incomplete, che potrebbero non essere sufficienti a proteggere i veicoli connessi. È importante che le aziende del settore collaborino e lavorino insieme per garantire una solida difesa contro le minacce alla sicurezza dei veicoli connessi.
In questo contesto complesso, variegato e distribuito, in cui non esiste un accentratore di dati per la Threat Intelligence, ma esistono diverse fonti di informazioni (tra cui organizzazioni di sicurezza informatica, istituti di ricerca, agenzie governative e organizzazioni di settore) le case costruttrici devono necessariamente implementare una propria Threat Intelligence che includa anche componenti e sistemi acquisiti tramite i propri fornitori.
Questa base di osservazione deve essere migliorata costantemente anche tramite la rilevazione e dall'analisi dei dati dal campo: a tale scopo l'intelligenza artificiale può risultare strategica nella definizione della soluzione.
Il machine learning può aiutare ad automatizzare la raccolta e l'analisi di grandi quantità di dati sulla sicurezza, rendendo più efficiente e precisa la identificazione delle minacce. Inoltre, il machine learning può essere utilizzato per sviluppare modelli di rilevamento di anomalie e di intrusione, che possono aiutare a identificare comportamenti sospetti e prevenire gli attacchi.
Ad esempio, i modelli di machine learning possono essere utilizzati per analizzare i dati sulle comunicazioni dei veicoli connessi, identificare comportamenti anomali e prevenire gli attacchi ai sistemi di bordo. Inoltre, i modelli di machine learning possono essere utilizzati per analizzare i dati sulle vulnerabilità e sugli attacchi del passato, al fine di prevedere le minacce future e di sviluppare soluzioni di sicurezza più efficaci.
In sintesi, il machine learning può migliorare la Threat Intelligence nell'industria automobilistica automatizzando e rendendo più efficiente la raccolta e l'analisi dei dati sulla sicurezza, e aiutando a identificare comportamenti anomali e prevenire gli attacchi.
Ma il machine learning richiede una quantità sufficiente di dati di alta qualità per addestrare modelli affidabili, motivo per cui sarebbe auspicabile una collaborazione dell'intero comparto Automotive: dai produttori di componenti elettronici, a quelli di sistemi complessi, fino a costruttori, passando dagli sviluppatori firmware e software ed arrivando al cloud che acquisisce e gestisce le informazioni.
Questa base di osservazione e comprensione delle esigenze del settore Automotive ha guidato la ricerca di Macnil nel novero del progetto "Secure Safe Apulia". Macnil ha così disegnato una soluzione di prevention implementando una componente di Threat Intelligence specifica per il mondo Automotive alimentata tramite la perlustrazione costante del deep e dark web, per stare al passo con i malintenzionati.

Le approfondite informazioni ottenute per il settore Automotive aiutano nell'identificazione dei trend di minaccia, consentono di proteggere i vettori di attacco emergenti e di mitigare gli attacchi più sofisticati.

Malware 4Q2022

Alice Ransomware

Alice è tra i nuovi ransomware in vendita sui forum di criminalità informatica che figura sotto il progetto di "Alice in the Land of Malware".
Una volta scaricato, consente di generare file binari ransomware con la possibilità di inviare una richiesta di riscatto personalizzata. La sua esecuzione cripta i file della vittima aggiungendo l'estensione ".alice". Tra le note di riscatto spesso viene inserita in più cartelle la nota "How to Restore Your Files.txt".
Funziona dunque secondo il modello commerciale Ransomware-as-a-Service (RaaS).
Al momento non vi sono ancora indicatori di compromissione noti.

AXLocker

AXLocker è un nuovo tipo di ransomware che, una volta entrato nella macchina della vittima, non solo riesce a crittografare i file (utilizzando l'algoritmo di crittografia AES) rendendoli completamente inutilizzabili, ma riesce anche a rubare i token Discord e altre informazioni sensibili come nome utente o indirizzo IP della macchina, per inviarli al server.
Dopo aver crittografati i file, AXLocker mostra una finestra pop-up contenente la richiesta di riscatto con le istruzioni per ottenere lo strumento di decrittazione utile per recuperare i file crittografati.
A differenza di altri ransomware, AXLocker non modifica il nome o l'estensione dei file crittografati e prende di mira solo estensioni di file specifiche, escludendo un elenco di directory dal processo di crittografia.
Le imprese dovrebbero essere all'avanguardia rispetto alle tecniche utilizzate dai cybercriminali e implementare le best practice e i controlli di sicurezza richiesti, altrimenti diventeranno vittime di ransomware sempre più sofisticati e aggressivi

Dtrack

Il malware Dtrack utilizza uno strumento di amministrazione remota (RAT) in grado di controllare il dispositivo dell'utente. I creatori sono il gruppo APT Lazarus e operano dal 2009. Le attività malevoli da loro messe in atto continuano a sviluppare varianti sempre più pericolose, in grado di raggiungere obiettivi e vittime diverse. Negli ultimi mesi hanno preso di mira numerose aziende Europee, di cui anche italiane.
Anche la sua diffusione, mediante i canali di crack e download non certificati di software da installare sul proprio PC, fa riflettere su quanto questi canali, privi di ogni garanzia di sicurezza, siano ancora oggi molto utilizzati a livello globale, sia per estorcere denaro che per effettuare attacchi mirati di tipo geo-politico.
L'obbiettivo degli attacchi è quello di caricare, scaricare, lanciare o eliminare file. Nonostante i continui aggiornamenti effettuati sul malware, la backdoor è rimasta invariata: la vittima scarica un software normale che nasconde una serie di malware. Dtrack sfrutta la crittografia, un keylogger ed effettua screenshot per raccogliere informazioni sul sistema dell'utente.
Per proteggersi da eventuali attacchi, è indispensabile usare software capaci di monitorare il traffico, utilizzare soluzioni di sicurezza completa con tecnologie di rilevamento, come gli EDR.

DuckTail

DuckTail è un ransomware che utilizza come linguaggio di programmazione PHP, che solitamente è applicato per lo sviluppo Web. Lo script dannoso si attiva quando il programma è installato sul dispositivo, inconsapevolmente dalla vittima.
Questo ransoware colpisce le vittime attraverso piattaforme Ads&Business di Facebook per prendere il controllo di Facebook Business e Linkedin
In questo modo, i criminali informatici hanno l possibilità di accedere ai dati sensibili aziendali, contenenti spesso informazioni di tipo economico. Una volta che il ransomware ha preso il controllo del broswar, i criminali informatici, eseguendo codice arbitrario con l'aiuto di questo script PHP dannoso.
Per comunicare, gli aggressori hanno sviluppato un sito Web che archivia e ospita i dati in formato JSON. A differenza di servizio di messaggistica istantanea e broadcasting, come Telegram, il sito è in grado di recuperare le informazioni sul browser installato nel sistema, estrarre informazioni memorizzate dei cookie del browser dal sistema e raccogliere il tutto per inviare i dati al server di comando e controllo (C&C)

Industrial Spy

Industrial Spy nuovo è una nuova gang di criminali informatici che ha messo in atto azioni illegali e realizzando una doppia estorsione per gli utenti malcapitati.
Il gruppo si distingue da altri perché ha La gang ha strutturato il suo business illegale su tre livelli. Ad Ad ogni livello, i dati rubati all'azienda vittima vengono rivenduti:

- Nel livello premium, in aste online a prezzi elevati. In cambi di milioni di bitcoin, si ottengono i dati e la cancellazione degli stessi dai server dei criminali.
- Nel secondo livello, ad altri gruppi criminali in cambio di altri dati o di bitcoin
- Nel livello di accesso libero i dati possono essere downloadati gratuitamente da qualunque malintenzionato.

Le vittime attualmente colpite sono poche aziende, ma Industrial Spy è riuscita ad ottenere ingenti profitti, grazie al vero e proprio e-commerce realizzando per lo scambio di informazioni segrete delle aziende vittime. L'attività del gruppo è estremamente pericolosa per chi viene colpito perché perde l'accessibilità ai dati, che diventa di dominio di molti.

MedusaLocker

MedusaLocker fa parte della famiglia di ransomware. Si tratta di un software malevolo, che circola da circa due anni e che risulta essere in continua evoluzione infatti, tattiche, tecniche e procedure (TTP) cambiano di volta in volta.
Inizialmente, per iniettare questo ransomware all'interno della memoria del sistema target, si utilizzava un file batch iniziale ed un documento di testo. Oggi sfrutta il codice PowerShell, che inietta in modo riflessivo il suo codice, in modo che sia lo stesso PowerShell ad eseguire l'attività malevola. In questo modo, attraverso l'utilizzo della chiave di registro "EnableLinkedConnections" presente all'interno della macchina malevola, si diffonde su tutta la rete.
MedusaLocker è spesso veicolato da campagne phishing e spam su posta elettronica ed è utilizzato per alterare il sistema rimuovendo in modo permanente le copie shadow di Windows ed eliminando i servizi di sistema attraverso la crittografia AES-256 standard.

Questo consente ai criminali di accedere ai dispositivi delle vittime tramite configurazioni vulnerabili del Remote Desktop Protocol e di richiedere loro pagamenti di riscatto di importi rilevanti. Ad oggi, ne sono stati individuati circa 21, diversi tra loro, che presentano transazioni che vanno dai 50mila ai 3 milioni di dollari.
Per cercare di mitigare attacchi di questo tipo, sarebbe bene: segmentare la rete limitando così la diffusione del ransomware in caso di attacco, eseguire regolarmente il backup per l'infrastruttura che si vuole proteggere, effettuare costantemente aggiornamenti di sicurezza dei sistemi operativi e applicativi installati, impostare l'autenticazione a più fattori e, in caso di organizzazioni, formare continuamente il personale dipendente operativo.

Octocrypt

Tra le nuove famiglie di ransomware, apparse negli ultimi mesi del 2022, è stato scoperto Octocrypt, un ransomware scritto in Golang ed utilizzato come Ransomware-as-a-Service che ha come obiettivo quello di prendere di mira tutte le versioni di Windows per criptare i dati del PC su cui si installa e richiedere poi un riscatto alla vittima.
Octocrypt si presenta con una semplice interfaccia web al fine di costruire il crittografo, il decrittografo e il pannello web, che mostra i dettagli della vittima. Grazie a quest'interfaccia del generatore del pannello web i criminali riescono a generare eseguibili binari ransomware, inserendo opzioni come URL, API, indirizzo mail, indirizzo crittografico e importo crittografico.
Cliccando sull'URL, il ransomware si diffonde in tutte le cartelle rilasciando la richiesta di riscatto con un file nominato "INSTRUCTIONS.html" e modifica lo sfondo del desktop della vittima, la quale visualizzerà un messaggio di minaccia con un importo di riscatto da inviare ad uno specifico indirizzo.
Per prevenire attacchi di questo genere è bene eseguire regolarmente backup, aggiornare costantemente i dispositivi, utilizzare noti pacchetti software antivirus e di sicurezza e porre estrema attenzione ai link e agli allegati presenti nelle mail sospette.

Royal

Si tratta di un ransomware, noto anche come Royal Zeon, il cui obiettivo è chiedere un notevole riscatto alle grandi realtà.
Il primo attacco Royal risale a giugno 2022; la metodologia scelta come vettore di attacco è il cosiddetto callback phishing. L'attaccante quindi tramite mail contatta la sua vittima, incitandola a pagare un finto abbonamento su servizi o di food delivery o servizi software.
Nel testo della mail mandata alla vittima, viene aggiunto un numero di telefono da chiamare se si desidera ricevere informazioni in merito. A tale numero risponderà un complice dell'attaccante che convincerà la vittima ad installare un programma, al fine di ottenere il controllo remoto ai computer.
A questo punto viene chiesto il riscatto notevole alla vittima.

ViperSoftX

È un'estensione malevola del browser Google Chrome, avente l'obiettivo di rubare le informazioni riportate negli appunti. Si tratta di un JavaScript-based RAT (Remote Access Trojan), nato nel 2020 e registra le sue vittime negli Stati Uniti, Brasile, India e Italia.
Il vettore di attacco utilizzato è un file torrent malevolo per videogiochi o licenze malevole per programmi a pagamento. Come già anticipato, il RAT si maschera come un'estensione di un'applicazione nota come "Google Sheet 2.1".
Modifica il codice HTML del siti Web e dirotta le transazioni di criptovaluta ai portafogli degli attaccanti. Inoltre, il malware è in grado di sottrarre illecitamente le password delle vittime.

Malware 1Q2022

Chaos

Si tratta di un ransomware avente matrice italiana. Sui sistemi compromessi viene impostato come sfondo del desktop due agenti della Polizia di Stato, vengono cifrati i file e viene depositato un file "polizia.exe".
I criminali informatici dietro questa campagna ransomware rilevano sul computer compromesso la presenza di materiale pedopornografico. Per non denunciare l'illecito penale alle forze dell'ordine viene richiesto, entro 72 ore, il pagamento di un riscatto in bitcoin del corrispettivo di 250 euro, cifra decisamente minore rispetto ai soliti riscatti ransomware a cui si è abituati.
Tuttavia la vittima non tornerà più in possesso dei file compromessi perché, al fine di snellire la procedura di crittografia, vengono effettivamente cifrati solo i file minori di 2 MB, gli altri file vengono sovrascritti con dati casuali.
Chaos ha la capacità di propagarsi su tutte le unità di archiviazione collegate al sistema compromesso, ampliando così la portata dei danni arrecati.

CryptoRom

CryptoRom è il nuovo malware che colpisce gli utenti di iPhone e Android attraverso app di dating come Bumble e Tinder, utilizza tecniche di social engineering e induce le vittime ad effettuare investimenti in servizi fasulli di trading di criptovalute.
Si tratta di una vera e propria truffa finanziaria che fa leva su rapporti sentimentali nati online, il cui scopo è convincere le vittime ad investire in criptovalute, promettendo enormi guadagni. Spesso i cybercriminali contattano direttamente gli utenti, dopo aver trovato le informazioni sui social media.
Alle vittime che non possono pagare, inoltre, viene addirittura proposto un prestito, attraverso finti siti web.
Ovviamente riappropriarsi delle monete digitali investite è impossibile.

Electron-bot

Electron-bot è un malware presente nell'App store di Microsoft, che si impossessa del controllo degli account dei social media delle sue vittime, registra nuovi account, accede, commenta e mette like ad altri post. Il malware, infatti, ha infettato gaming app molto popolari come Temple Run e Subway Surfer. Si stima che questa campagna malware abbia avuto origine in Bulgaria e la maggior parte delle vittime finora conteggiate si trova in Spagna, Svezia, Bermuda e Israele.

L'attacco con Electron-bot parte con l'installazione di un'app non autentica presente nel Microsoft Store. In questo modo l'attaccante scarica i file ed esegue gli script che attivano il malware, il quale prende il controllo del sistema ed esegue comandi inviati dal server C&C dell'attaccante. La maggior parte degli script vengono eseguiti direttamente dai server degli attaccanti per evitare che un software antimalware rilevi la presenza di un file malevolo.
Per imitare il comportamento dell'utente durante la navigazione, il malware sfrutta il framework Electron evitando così le protezioni dei siti web. Inoltre, gli operatori modificano il payload del malware e variano continuamente il comportamento dei bot così da non fornire alcun elemento identificabile di attacco.

Tutte le varianti riscontrate tra il 2019 e il 2022 sono state caricate su un cloud storage pubblico dal nome "mediafire.com", mentre l'account Sound Cloud e il canale YouTube che il bot promuove sono sotto il nome di "Ivaylo Yordanov", un popolare wrestler e calciatore bulgaro.

Per proteggere gli account da questo tipo di malware, gli esperti di sicurezza esortano ad utilizzare password complesse e, ove possibile, attivare l'autenticazione a due fattori.

HermeticWiper

Il nuovo malware Hermetic Wiper, realizzato a Dicembre 2021, genera un attacco DoS con l'obiettivo di distruggere i dati e rendere inutilizzabili i sistemi interrompendone l'attività. È un malware particolarmente pericoloso in quanto una volta cancellati i file, questi non sono più recuperabili. Lo scopo di Hermetic Wiper non è quindi rubare informazioni, ma semplicemente distruggere i dati presenti sui computer infettati, mettendoli fuori uso.

Per compiere tale operazione e corrompere i dati presenti in memoria, il virus sfrutta abusivamente i driver di un normale software per la gestione delle partizioni del disco. Tali driver sono presenti in forma compressa all'interno delle risorse del malware stesso e, dopo essere stati estratti e decompressi, vengono rilasciati sul disco.

Per ridurre al minimo i rischi derivanti da un attacco informatico di questa tipologia, le azioni, rivolte in modo particolare alle aziende, sono:

- misure organizzative e procedurali come:
    - verifica della disponibilità offline dei backup necessari al ripristino delle attività di core business
    - designazione di un team per la gestione di eventuali crisi informatiche;
    - esercitazione di tutto il personale nella risposta a incidenti informatici.
- operazioni da compiere come:
    - monitoraggio degli account di servizio e degli account amministrativi per rilevare eventuali attività anomale;
    - richiesta dell'autenticazione a più fattori per tutti gli accessi remoti, in particolare per servizi VPN, extranet aziendali e posta elettronica;
    - verifica delle interconnessioni tra la rete IT e le reti OT prediligendo la massima segregazione possibile tra le stesse.

Jester Stealer

Jester Stealer è un software dannoso progettato per estrarre un'ampia varietà di informazioni sensibili dai dispositivi infetti quali credenziali, dati di navigazione, informazioni bancarie ma anche App di messaggistica istantanea come Telegram e WhatsApp.
In genere arriva ai sistemi di destinazione tramite e-mail di phishing, mascherato da txt, mp3 o un file allegato ppt, doc o pdf. A volte utilizza canali di distribuzione casuali come contenuti piratati e strumenti di hacking tramite piattaforme come YouTube.
Jester Stealer è un malware multifunzionale che combina le funzioni di stealer, clipper, crypto-miner e botnet.
Utilizza comunicazioni crittografate AES-CBC-256, supporta i server di rete Tor, reindirizza i registri ai robot di telegramma e raggruppa i dati rubati nella memoria prima dell'esfiltrazione. Una volta terminata l'esfiltrazione, Jester Stealer si elimina dalla macchina infetta senza che la vittima si rende conto della violazione dei dati.
L'ultima versione sembra essere la 1.7.1.0, annunciata a gennaio 2022 con potenziamenti come migliori velocità di trasferimento dei file e rilevamenti di runtime ridotti.

JRAT

jRAT è un trojan di accesso remoto (Remote Access Trojan - RAT), scritto in Java, emerso per la prima volta nel 2013.
Nel 2022 è emersa una nuova variante che sembra prendere di mira in modo specifico il sistema operativo Windows e le comuni applicazioni Windows tra cui Internet Explorer e Outlook.
I RAT possono gestire (copiare, spostare, eliminare, rinominare, ecc.) i file archiviati sul computer infetto, acquisire schermate, accedere al microfono e alla webcam ed eseguire altre azioni.
Il malware viene solitamente veicolato tramite email con allegato .JAR dannoso opportunamente offuscato e nascosto tra una serie di applicazioni JAR legittime, caricate da un server remoto. Viene utilizzata la crittografia per rendere difficile il rilevamento del file JAR iniziale. Tutto ciò rende difficile rilevare attività anomale.

Lapsus$

Lapsus$ è un nuovo gruppo di ransomware che adotta tattiche insolite per il settore.
Oltre alle aziende tecnologiche e di telecomunicazione, questi cybercriminali hanno preso di mira enti governativi, compagnie manifatturiere, scuole e università, il settore energetico e la sanità.
Lapsus$ è attivo solo da qualche mese e ha già dato prova della sua creatività. Invece di sottrarre dati, criptare i sistemi e poi minacciare di diffondere le informazioni rubate a meno che la vittima non paghi un riscatto, Lapsus$ si è specializzato in data breach di materiali interni come il codice sorgente.
Il gruppo ottiene l'accesso ai sistemi dei suoi obiettivi attraverso attacchi di phishing, per poi rubare i dati più sensibili anche senza distribuire malware.
Poiché le vittime sono generalmente grandi enti distribuiti a livello globale, il possesso e il controllo dei codici sorgente potrebbe creare una grossa reazione alla catena di approvvigionamento, che può portare all'infezione e al danneggiamento di numerose organizzazioni e macchine.

Phoenix

Phoenix è un ransomware basato su il codice open source HiddenTear AES-256 per crittografare i file dell'utente vittima. Si tratta di un algoritmo di crittografia simmetrico, per cui la decrittazione senza una chiave univoca è impossibile.
Come diversi suoi simili, si diffonde mediante e-mail di spam, browser hijacker e pacchetti software infetti scaricati da siti non attendibili o reti P2P.
Una volta che il ransomware ha raggiunto il dispositivo, scansione e infettare i file presenti, mirando a quelli con dimensioni specifiche. Da qui, realizza un file sul desktop nominata Important!.txt, per chiedere all'utente il riscatto. Gli sviluppatori del virus memorizzano, all'interno di un server, la chiave per la risoluzione del codice e le vittime sono costrette a cedere al pagamento.
La vittima può non cedere al ricatto e può, quindi, rimuovere in autonomia il virus, eseguendo una scansione, tramite un antimalware, che è in grado di eliminarlo con facilità.
Dato che il virus presenta un bug ed è semplice da rimuovere, ci si aspetta che i criminali informatici svilupperanno nuove versioni più sofisticate e pericolose.
Per evitare infezioni di Phoenix o di simili, è possibile sia in via preventiva, attraverso l'uso di antivirus, antispyware e aggiornamenti continui del sistema, che attraverso la rimozione a posteriori.
È consigliato non usare programmi di terze parti, non aprire file all'interno di e-mail con indirizzi non noti e non scaricare software da fonti non ufficiali.

Snatch

Snatch è una variante di ransomware, classificato oggi tra i più gravi, realizzato da un gruppo di criminali informatici con l'obiettivo di estorsione e furto. Questa tipologia di malware è scritta con un linguaggio Google Go e risulta altamente pericoloso, perché è in grado di prendere il controllo di una macchina, anche in modalità provvisoria, by-passando ogni controllo di sicurezza e servizi di protezione Endpoint.
Come altri suoi simili, si diffonde via mail spam, connessioni RDP e software anti-ransomware free, ma risulta efficace su sistemi Windows.
Infatti, a differenza di altri virus, che come prima operazione analizzano immediatamente i file presenti, Snatch si inserisce come un servizio di sistema indispensabile da eseguire, anche in modalità provvisoria, impedendo a normali antivirus di vederlo e, quindi, bloccare l'infezione.
Una volta installato, i criminali potranno agire come amministratore del dispositivo e istalleranno BCDEDIT, strumento della riga di comando di Windows. A questo punto, verrà effettuata una forzatura di riavvio del dispositivo e, nel frattempo, indisturbato, crea una cartella in %AppData% o in LocalAppData% e inizia la sua azione di cifratura di file, prelevando e criptando dati sensibili. I file diventano inaccessibili ad altri, perché adotta il comando vssadmin.exe presente nel sistema operativo, decodifica i file con la crittografia AES e, infine, elimina le copie shadow, senza possibilità di recuperare i dati presenti su disco rigido.
La sua particolarità nasce con lo scopo di colpire vittime ben definite, grandi aziende ed enti governativi, alle quali ha già estorto somme di denaro e criptovalute e causando danni per migliaia di euro.

SysJoker

SysJoker è una backdoor multipiattaforma che prende di mira Windows, Mac e Linux.
Il Malware si maschera da aggiornamento di sistema e genera il suo C2 decodificando una stringa recuperata da un file di testo ospitato su Google Drive; è scritto in C++ e ogni sample è fatto su misura per il sistema operativo specifico che prende di mira. Il comportamento di SysJoker è simile per tutti e tre i sistemi operativi che colpisce. Ci sono indicazioni che l'attacco SysJoker venga eseguito da un cyber-attacker di livello avanzato; tra queste indicazioni, c'è il fatto che il codice sia stato scritto da zero e non sia stato visto prima in altri attacchi e soprattutto è evidente come sia raro trovare un malware Linux mai visto prima in un attacco live.

WarzoneRat

WarzoneRat è un trojan di accesso remoto e fa parte del gruppo degli strumenti di hacking più accessibili disponibili online: ci sono innumerevoli RAT gratuiti che i criminali informatici possono utilizzare per assumere il controllo dei computer delle loro vittime, ma questi possono avere funzionalità limitate. Tuttavia, ci sono anche alcuni casi speciali in cui questi RAT non sono gratuiti; un esempio di questo è proprio il Warzone RAT, un progetto che viene offerto online e promosso su vari forum di hacking. Il Trojan possiede un ampio elenco di funzionalità che consentirebbero ai suoi operatori di causare molti problemi ottenendo molte informazioni. Una volta che Warzone RAT ha infettato un computer, la copia attiva della minaccia può essere controllata tramite il pannello di amministrazione accessibile dall'aggressore e grazie ad esso è possibile: sfogliare, leggere, eliminare e modificare i file locali, terminare i processi, controllare le attività pianificate e i servizi di Windows, caricare i file e avviarli sull'host compromesso, avviare un modulo keylogger, stabilire una connessione desktop remoto e assumere il controllo del computer infetto ed infine utilizzare il prompt dei comandi per eseguirli.

Malware 2Q2022

Black Basta

Black Basta è un ransomware utilizzato per rubare i dati degli utenti e criptarli, renderli indisponibili e richiedere un riscatto. L'origine dei threat actors è probabilmente africana e hanno come scopo principale colpire le grandi organizzazioni statunitensi ed europee.
Questo ransomware sfrutta servizi leciti di Windows e presenta payload criptato ed offuscato. Questo è in grado di richiedere un riscatto tramite un documento ReadMe.it, che si posizione nella directory del computer infetto.
Le caratteristiche principali di Black Basta sono la cifratura parziale del contenuto dei files, lo sfruttamento del servizio FAX di Windows per ispezionare la cifratura e la creazione di un login id usato per accedere al dominio TOR degli attaccanti. Si comprende che cifrare solo porzioni di codice, rende l'operazione di crittografia rapida ma disintegra i dati contenuti nell'infrastruttura compromessa.
Si maschera da applicazione legittima firmando l'esecuzione di un certificato, per eludere potenzialmente diversi sistemi antivirus ed EDR e ingannare gli utenti, perché il file risulta "firmato" da una software house esistente e l'avviso di "firma non valida" non è evidente.
Il ransomware intrappola la vittima con la logica principale del sistema di encryption che aggiunge l'estensione basta ai files criptati, includendo files di collegamento .lnk per rendere inutilizzabile la macchina infetta.
Durante la fase di infezione le copie shadow vengono eliminate per rendere quasi impossibile il recupero dei files criptati.

Coper

Coper è un trojan bancario, nascosto all'interno di file APK ed è la versione avanzata di Exobot, malware di Android che crea sovrapposizioni invisibili sulle schermate delle applicazioni bancarie per prelevare le informazioni dell'utente.

E’ un malware piuttosto evoluto: è in grado di prendere il controllo completo del dispositivo compromesso (compresa gestione audio e schermo) e di interagire con i server di Command & Control per inviare informazioni, ricevere ed eseguire nuove istruzioni cifrate tramite crittografia simmetrica AES con chiave embedded.
La modalità di attacco di Coper su Android avviene tramite campagna phishing. Molti utenti sono stati tratti in inganno e hanno scaricato l’app malevola che i Threat Actors (TA) avevano diffuso facendola passare per software bancario. L’app ha diffuso nei dispositivi delle vittime il modulo dannoso. Da questo momento, il malware è in grado di attivare una sessione VNC (Virtual Network Computing), abilitare le funzionalità di keylogging, iniettare codice HTML, disinstallare, avviare e installare app.

Cuba ransomware

Cuba è un ransomware si occupa di scansionare i file sul sistema dell'utente e di iniziare a bloccarli usando un algoritmo di crittografia. I file come immagini, documenti, fogli di calcolo, video, presentazioni, database, archivi, ecc. vengono bloccati rapidamente. Dopo aver bloccato un file di destinazione, Cuba Ransomware applica una nuova estensione al suo nome: ".cuba".
Completato il processo di crittografia, Cuba Ransomware procederà all'attacco rilasciando un messaggio di riscatto sul desktop della vittima. Nella nota di riscatto, gli aggressori dichiarano che se l'utente non paga, non sarà in grado di recuperare i propri dati.
Si consiglia di non pagare la tassa di riscatto richiesta: la maggior parte degli utenti che pagano non ricevono mai le chiavi di decrittazione di cui hanno bisogno.

Eking

Eking appartiene alla famiglia Phobos ransomware, ovvero un’infezione utilizzata allo scopo di ricattare le vittime. Il principale metodo di divulgazione utilizzato è allegare alle e-mail il virus, che appare come documento di Microsoft Word.
Inserito nel dispositivo, Eking è in grado di codificare i file crittografati presenti sulla macchina infetta, rinomina aggiungendo l’ID della vittima, l’indirizzo e-mail degli aggressori e l’estensione “.eking”. I file sono resi inutilizzabili per l’utente-vittima e possono provocare un’infezione tale da alterare le voci del registro di Windows. L’algoritmo di crittografia utilizzato per renderli inaccessibili riesce a prendere di mira i file più diffusi (immagini, testo, audio, video, documenti, fogli di calcolo, presentazioni) e rende l’apertura impossibile per l’utente. Solo una chiave di decriptazione potrà dare la possibilità di accedere nuovamente ai file.
Nel momento in cui l’utente tenta di aprire un file infetto, Eking mostra una finestra pop-up “info.hta” e una nota di ricatto “info.txt”, nella quale sono indicate le metodologie di pagamento e la scadenza.
Gli aggressori utilizzano tale ransomware allo scopo di estorcere una somma di denaro alla vittima.

Kinsing

Kinsing è un malware che prende di mira le porte API configurate in modo errato su Docker. Vengono utilizzate per eseguire un container Ubuntu su cui è installato il malware Kinsing, che a sua volta distribuisce un *miner* di criptovalute in questi container compromessi.
Kinsing è basato su Linux e scritto in Golang e una volta entrato in esecuzione, cerca di replicarsi in altri container ed host, collegandosi a diversi IP, scaricando poi da ognuno le varie componenti necessarie per

funzionare: comunicazione con i server C&C, lo script iniziale per la configurazione dell'ambiente ed il download del *crypto-miner*.
Lo scopo principale del virus è creare un minatore Bitcoin. Inoltre, il malware riesce ad essere persistente.

Magniber

È un ransomware che sfrutta il kit di exploit Magnitudine per infettare gli utenti del broswer Microsoft Edge e Google Chrome attraverso JavaScript e si maschera come falso aggiornamento dello stesso.
La strategia dei criminali informatici è raggiungere il più grande numero di utenti e infatti, nascondono in un file il pacchetto dell'applicazione .APPX, firmato digitalmente con certificato valido ed infettati dal virus. In questo modo, riesce a by-passare i controlli del sistema operativo Windows, rilasciando il comando di attendibilità e consentendo la distribuzione e l'installazione del virus.
Per la diffusione rapida, i cybercriminali utilizzano campagne phishing via mail e tramite app di messaggistica. I messaggi contengono un link contenente il file malevolo, invogliando la vittima a cliccare sullo stesso o ad aggiornare il browser sfruttando tecniche dell'ingegneria sociale e della pressione psicologica.
I creatori del virus sono stati attenti a simulare in modo estremamente puntiglioso il layout della pagine di Microsoft e di Google, traendo in inganno la vittima con l'avviso di aggiornamento manuale. Una volta accettata l'operazione, il sistema scarica il download e crea una directory "C:\Programmi\WindowsApps" due nuovi file:

- wjoiyyxzllm.exe che carica il file DLL ed esegue una funzione specifica;
- wjoiyyxzllm.dll che scarica il payload codificato da Magniber, con decodifica ed esecuzione dello stesso.

Da qui il virus è libero di eseguire la crittografia dei dati sul sistema, per richiedere un riscatto per liberare i file
A differenza di altri malware, Magniber non ruba i file, ma effettua solo una crittografia del sistema, per estorcere denaro alla vittima.

Meta

Meta è il nuovo malware info-stealer distribuito mediante una campagna malspam e configurato per rubare le password archiviate nei browser Chrome, Edge e Firefox, ma anche nei portafogli di criptovalute, in modo semplice e a basso costo di acquisto.
Gli information stealer sono in grado di rubare credenziali di servizi per commettere furti (compresi quelli di criptovalute dai portafogli cripto); cookie archiviati nei browser per dirottare gli account anche dei social media delle vittime; utilizzare gli account verificati trafugati, per far girare pubblicità malevole (malvertising); distribuire malware.

La campagna di malspam utilizza trucchi di ingegneria sociale per indurre le vittime ad aprire un file Excel e abilitare le macro contenute in esso per avviare il processo di infezione.

Prynt stealer

È un nuovo malware che presenta un vasto assortimento di funzionalità sfruttate dai criminali informatici per rubare i dati presenti dei dispositivi delle vittime e contiene il tool che intercetta e memorizza ogni input che arriva sulla tastiera. Prynt Stealer è distribuito all'interno del dark web a pagamento ed è diffuso dagli acquirenti in diversi browser che all'interno di portafogli di criptovalute. Chi acquista il malware può personalizzare il tool, realizzare una versione più leggera ed effettuare attacchi mirati e distribuirlo attraverso software pirata.
Inizialmente, il malware ruba i file della vittima che hanno dimensione inferiore a 5KB, poi raccoglie password, cookie, segnalibri, cronologia di navigazione e numeri delle carte di credito memorizzate nei browser e infine analizza le app di messaggistiche, di gaming e i wallet di criptovalute. È in grado di rubare il login di FileZilla, NordVPN, OpenVPN e ProtonVPN.
I dati vengono rubati tramite un bot Telegram, copiati in una directory nascosta, insieme a varie informazioni sul sistema (processi in esecuzione, screenshot, rete, product key di Windows) e inviati a un server remoto.
Anche se altamente pericoloso, l'autenticazione a due fattori, alert via sms ed email, un check up periodico dei propri device e uso di sistemi di sicurezza endpoint, consente all'utente di non incorrere nel virus.

Quantum Locker

Scoperto per la prima volta a luglio 2021, Quantum Locker inizia con un attacco di phishing via e-mail. Secondo alcuni ricercatori di sicurezza, l'attacco dura solo 3 ore e 44 minuti dall'infezione iniziale al completamento di crittografia dei dispositivi, lasciando ai difensori poco tempo per reagire.
Gli attori delle minacce stanno utilizzando il malware IcedID come uno dei loro vettori di accesso iniziali, che implementa Cobalt Strike per l'accesso remoto e porta al furto di dati e alla crittografia utilizzando Quantum Locker. Le richieste di riscatto per questa banda variano a seconda della vittima, con alcuni attacchi che richiedono $ 150.000 per ricevere un decryptor, mentre altre sono richieste multimilionarie.

SmsGrab

SmsGrab è un malware per dispositivi Android veicolato tramite SMS contenenti link malevoli (APK) e generalmente dedicato a temi "Banking" e "Aggiornamenti".
SmsGrab veicola tramite SMS un malware (APK) per dispositivi Android, con lo scopo di sottrarre gli SMS, inviarli al C2 ospitato su Altervista e ottenere accesso ai codici 2FA, effettuando il furto di dati personali.
Nel caso degli istituti bancari viene solitamente inviata una comunicazione che sembra provenire dal servizio clienti, spingendo l'utente a cliccare sul link ricevuto tramite SMS.

SmsRat

Tra le minacce informatiche in grado di attaccare gli smartphone Android vi sono i RATsms, un trojan diffuso con lo scopo di rubare dati agli utenti.

I Remote Administration Tool, RAT, consentono di collegarsi da remoto a un qualsiasi dispositivo con connessione a Internet, consentendo al criminale informatico di impossesso del telefono della vittima. Potrà, così, fare qualsiasi cosa (scattare foto, attivare la geo-localizzazione per sapere tutti i nostri spostamenti, usare la nostra applicazione di home banking per rubarci i soldi) e vedere qualsiasi cosa l'utente effettuerà sul proprio smartphone.

Malware basati su questa tecnologia vengono sfruttati da grosse aziende o enti governativi per attività di spionaggio.

Nel momento in cui l'utente è attaccato dal RAT sms, l'utente non è in grado di comprendere che qualcuno sta spiando le sue attività e, involontariamente potrebbe mostrare informazioni estremamente riservate.

Per evitare di incorrere in queste situazioni, si consiglia di non installare app da fonti sconosciute, assicurandosi sempre dell'affidabilità dell'applicazione. Spesso i Trojan di questo tipo vengono nascosti all'interno di link sospetti contenuti in SMS, e-mail o applicazioni di messaggistica, che se cliccati fanno partire in automatico il download malevolo.

Evitare di disattivare il blocco di protezione, di cliccare su link sospetti e aggiornare il sistema operativo, previene trovarsi programmi indesiderati sul dispositivo mobile.

SpideyBot

Spidey Bot è un malware, presente sulla piattaforma di messaggistica per videogamer Discord, in grado di rubare username e password degli utenti. Riesce a copiare i primi 50 caratteri della clipboard di Windows, dove l'utente può contenere importanti dati personali. Non si limita a rubare i dati delle vittime, ma modifica il client Discord di Windows e lo trasforma in una blackdoor per consentire l'installazione di altri tipi di virus e malware. Discord è composto da tutte le funzionalità che derivano da HTML, CSS e JavaScript, consentendo al malware di modificare i file in modo che il client esegua un comportamento dannoso.
Al momento non esiste alcun modo per proteggersi e l'unica soluzione è prestare estrema attenzione a non aprire file di dubbia provenienza, come ad esempio chat per giochi. Infatti, il malware agisce solo nel momento in cui si effettua l'apertura del link malevolo

Spidey Bot ha come obiettivo due file:

- %AppData%\Discord\[version]\modules\discord_modules\index.js
- %AppData%\Discord\[version]\modules\discord_desktop_core\index.js

Per capire se si è stati infettati dal virus, bisogna aprire i file con l'applicazione Notepad. Se entrambi i file contengono una sola singola linea di codice, non si è stati infettati, mentre, al contrario, se è presente più di una riga di codice, installazione di Discord è stata contaminata. Bisogna procedete a disinstallarla ed effettuare la scansione antivirus.

SpyNote

SpyNote è un malware RAT (Remote Access Tool), emerso per la prima volta nel 2016, in grado di garantire il controllo assoluto del dispositivo Android attraverso un collegamento TCP.

Più che un classico malware, SpyNote potrebbe sembrare uno strumento di spionaggio remoto per attacchi mirati. Il trojan, nella versione 8.0, non necessita di accesso root, ma al momento dell'installazione richiede la concessione di numerosi permessi, tra cui quelli per modificare i messaggi e accedere alla scheda SD.
Una volta installato, SpyNote si rende invisibile nascondendo la sua icona e apre una porta di comunicazione TCP attraverso cui comunica con un server Command and Control, garantendo il controllo completo del dispositivo. Può controllare il registro chiamate, modificare qualsiasi impostazione, intercettare e registrare le telefonate effettuate col dispositivo, copiare i file memorizzati, utilizzare la videocamera e il microfono a piacimento, accedere alle informazioni relative al GPS e anche effettuare chiamate telefoniche.

Stormous

Stormous è un gruppo ransomware che agisce indisturbato sull'app di messaggistica per diverso tempo ed stato scoperto solo all'inizio del 2022, quando il gruppo ha realizzato un nuovo sito web sotto la rete Tor, creato un nuovo indirizzo onion e dichiarato lo schieramento politico nel conflitto russo-ucraino. Per quest'ultima ragione, il gruppo è monitorato dell'intelligence informatico.

Nonostante la creazione del nuovo sito, il gruppo continua ad utilizzare Telegram come principale mezzo di comunicazione. Le principali vittime sono aziende di grandi dimensioni occidentali o statunitense, dalle quali sono stati prelevati milioni di dati. Il gruppo di hacker malevoli ha reso noto che i dati rubati verranno totalmente venduti, ma l'attività criminale non è cessata e si aspetta un nuovo attacco contro i paesi occidentali.

SVCReady

SVCReady si propaga attraverso documenti Word, scoperto attraverso attacchi phishing. Una volta eseguito lo shellcode nelle proprietà del documento, questo viene caricato in memoria andando ad intaccare il funzionamento API di Windows, ottenendo pieno accesso al sistema operativo.
A questo punto, il computer è da ritenersi a tutti gli effetti infettato dal malware. Ciò significa non solo che il suo funzionamento è compromesso, ma anche che tutte le informazioni e i file contenuti sono nelle mani dei pirati informatici.

Turla

Turla è uno degli APT (Advanced Persistent Threat) più avanzati al mondo. Conosciuto anche come Snake, Venomous Bear, Uroburos, Group 88, Waterbug e Turla Team, è oggi una delle campagne di cyber-spionaggio più sofisticate. Lo spyware, infatti, è in grado di accedere alla fotocamera e al microfono dei dispositivi, registrare chiamate e messaggi e tracciare la posizione delle vittime.

Il malware Turla, sviluppato per smartphone Android, circola sotto forma di file APK (file di installazione delle app per il sistema operativo smartphone/tablet Android). L'APK contiene un'applicazione spyware Process Manager che, una volta installata sul dispositivo target, appare come la classica icona di "Impostazioni" e richiede una serie di autorizzazioni che solitamente gli utenti confermano senza dare troppa importanza, permettendo così alla nuova app di ottenere il controllo completo del dispositivo infetto.

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.

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
114. https://www.orticalab.it
115. https://www.html.it
116. https://www.punto-informatico.it
117. https://techfromthenet.it
118. https://www.giornalettismo.com

Sponsor