Swascan
TINEXTA GROUP

Threatland Report H2 2023

www.swascan.com
info@swascan.com

SOMMARIO

Disclaimer

La ricerca svolta da Swascan è basata su dati OSINT e CLOSINT ottenuti tramite Threat Intelligence.
Questa pubblicazione non rappresenta necessariamente lo stato dell'arte – data la natura transitoria delle fonti – e Swascan si riserva la prerogativa di aggiornamento periodico.
Fonti di terze parti sono citate a seconda dei casi. Swascan non è responsabile del contenuto delle fonti esterne, compresi i siti web esterni a cui si fa riferimento in questa pubblicazione.
La presente pubblicazione ha uno scopo puramente informativo. Essa deve essere accessibile gratuitamente.
Né Swascan né alcuna persona che agisca per suo conto è responsabile dell'uso che potrebbe essere fatto delle informazioni contenute in questa pubblicazione.

Chi siamo

Swascan

Swascan è una Cyber Security Company nata da un'idea di Pierguido Iezzi e Raoul Chiesa. La prima azienda di Cyber Security Italiana proprietaria di una piattaforma di Cyber Security Testing e Threat Intelligence, oltre ad un centro di eccellenza di Cyber Security Research; centro premiato con numerosi riconoscimenti nazionali e internazionali dai più importanti player del mercato IT e non solo. Da ottobre 2020, Swascan è parte integrante di Tinexta Cyber (Tinexta S.P.A), diventando protagonista attiva del primo polo nazionale di Cyber Security: non solo una azienda, ma un gruppo italiano, un nuovo hub nazionale specializzato nei servizi di identità digitale e sicurezza digitale.

Tinexta

Tinexta è un Gruppo industriale che offre soluzioni innovative per la trasformazione digitale e la crescita di imprese, professionisti e istituzioni. Quotata all'Euronext STAR Milan (MIC: MTAA), è inserita nell'indice europeo Tech Leader come azienda tech ad alto tasso di crescita. Basata in Italia e presente in 12 Paesi tra Europa e America Latina con oltre 2500 dipendenti, Tinexta è attiva nei settori strategici del Digital Trust, Cyber Security e Business Innovation. Al 31 dicembre 2022, il Gruppo ha riportato ricavi consolidati pari a € 357,2 milioni, EBITDA Adjusted pari a € 94,8 milioni e Utile netto pari a € 78,1 milioni. Attraverso le aziende del Gruppo, Tinexta promuove un'offerta integrata di servizi avanzati per l'identità e la certificazione digitale, la cybersicurezza, il digital marketing, l'accesso ai finanziamenti per l'innovazione e l'internazionalizzazione. Gestisce progetti complessi di digital transformation e realizza strategie mirate di sviluppo per supportare i piani di innovazione di piccole e medie imprese, grandi gruppi e istituzioni. Una presenza diffusa sul territorio e una vocazione internazionale, un'elevata agilità operativa e un solido presidio istituzionale, la ricchezza di risorse di grande professionalità e la valorizzazione delle competenze sono le caratteristiche distintive del Gruppo. Grazie ad esse Tinexta oggi continua a crescere sui mercati nazionali ed esteri, anticipando sfide e tendenze, innovando i processi e facendo crescere il business.

Data collection notice

Il presente rapporto è stato redatto esclusivamente dal Security Operations Center (SOC) e dal Threat Intelligence Team di Swascan, mediante l'utilizzo di tecniche di Open Source Intelligence (OSINT) e Closed Source Intelligence (CLOSINT), oltre alla piattaforma proprietaria Swascan. Le informazioni raccolte e presentate in questo documento rappresentano solo la parte emersa dell'intera situazione, poiché sono state prese in considerazione esclusivamente le aziende colpite da attacchi di ransomware che, avendo rifiutato di pagare il riscatto, hanno subito la pubblicazione dei propri dati su siti di data leak.

Si sottolinea che il numero riportato nel presente rapporto riflette un trend generale basato sulle informazioni disponibili. Tuttavia, è fondamentale comprendere che tale dato rappresenta solamente la punta dell'iceberg, in quanto il numero reale di vittime potrebbe essere significativamente superiore, considerando un fattore moltiplicativo n volte più grande.

Swascan non può garantire l'esattezza o la completezza delle informazioni fornite nel rapporto, poiché tali dati sono soggetti a cambiamenti e possono essere influenzati da vari fattori esterni. Gli utenti sono pertanto invitati a considerare attentamente il contesto e la complessità della situazione prima di trarre conclusioni definitive o prendere decisioni basate su queste informazioni.

Si declina ogni responsabilità per eventuali conseguenze derivanti dall'uso delle informazioni contenute nel presente rapporto. Swascan si impegna a mantenere la massima riservatezza e professionalità nelle proprie attività di analisi e fornisce questo rapporto a scopo informativo senza assumersi alcuna responsabilità legale o di altro genere.

SOC
Swascan
TINEXTA GROUP

H2 2023 – il primo sguardo

Il secondo semestre del 2023 ha visto un aumento significativo di attacchi informatici mirati al furto di dati e alla richiesta di riscatti in cambio del ripristino dei sistemi colpiti. Il SOC e Threat Intelligence Team di Swascan ha condotto un'analisi approfondita sugli scenari ransomware, malware e phishing, fornendo un quadro dettagliato delle minacce emergenti e delle tendenze in evoluzione.

Durante l'H2 sono state osservate numerose campagne ransomware, caratterizzate dalla diffusione di software malevoli che criptano i dati delle vittime e richiedono poi un riscatto per ripristinarli. Questi attacchi hanno colpito una vasta gamma di settori, inclusi quelli finanziari, sanitari, governativi, mettendo a rischio la sicurezza delle informazioni e la continuità operativa.

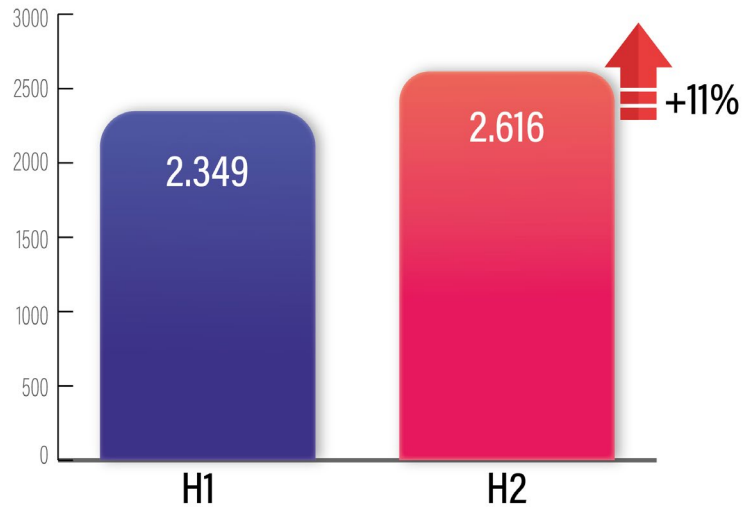
L'evoluzione delle tattiche utilizzate dai criminali informatici, soprattutto nell'H2, è stata particolarmente preoccupante. I ransomware sono diventati sempre più sofisticati e mirati e sono emerse numerose nuove gang ransomware.

Parallelamente agli attacchi di ransomware, il phishing ha continuato a rappresentare una minaccia significativa per la sicurezza informatica. Gli attaccanti hanno utilizzato metodi sempre più sofisticati per ingannare gli utenti, creando e-mail, siti web e messaggi di testo ingannevoli che sembrano provenire da fonti legittime. Attraverso queste tecniche, gli attaccanti cercano di ottenere informazioni sensibili come password, dati finanziari e credenziali di accesso, al fine di compiere frodi e danneggiare le vittime.

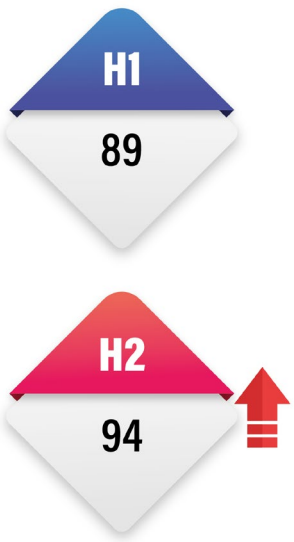
In questo report, analizzeremo i principali attacchi ransomware e phishing registrati, evidenziando le modalità operative, le vittime, le regioni colpite e le tendenze emergenti, ed esamineremo le misure di sicurezza consigliate per mitigare il rischio di tali minacce.

H1 e H2 cos'è cambiato – Ransomware

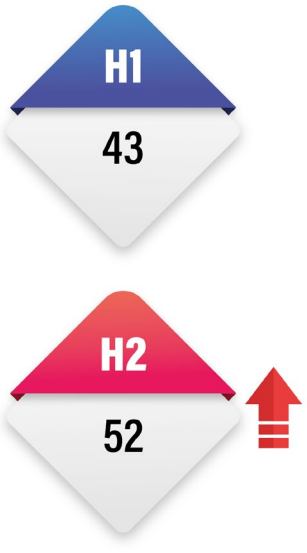
Attacchi Ransomware



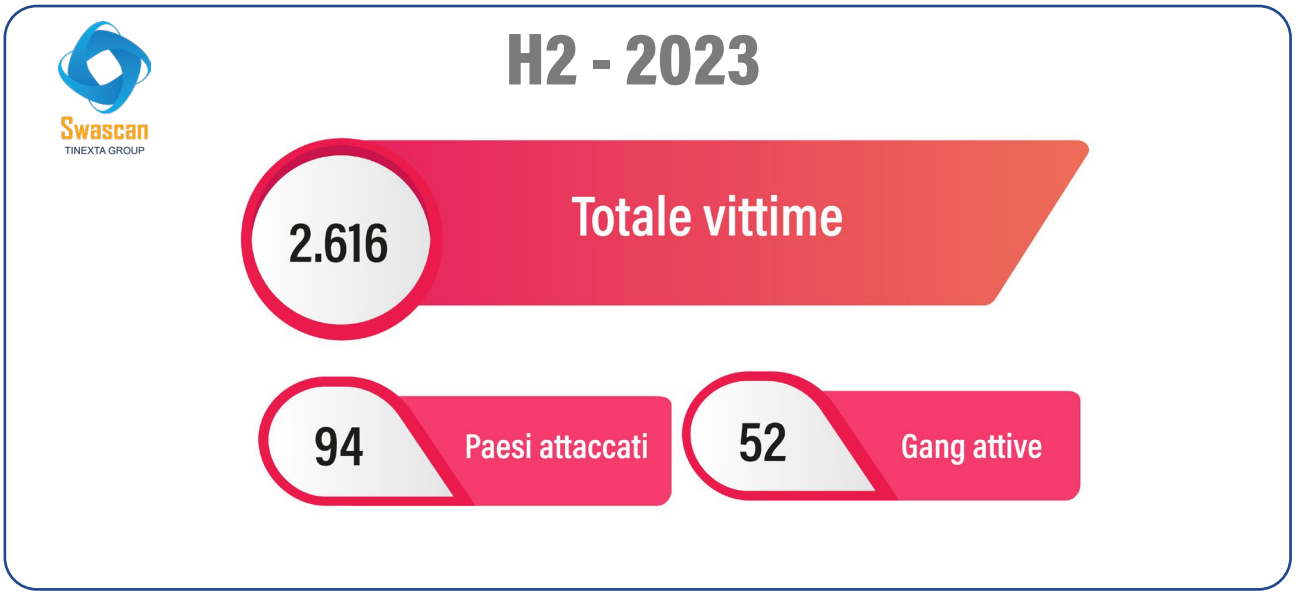
Paesi colpiti

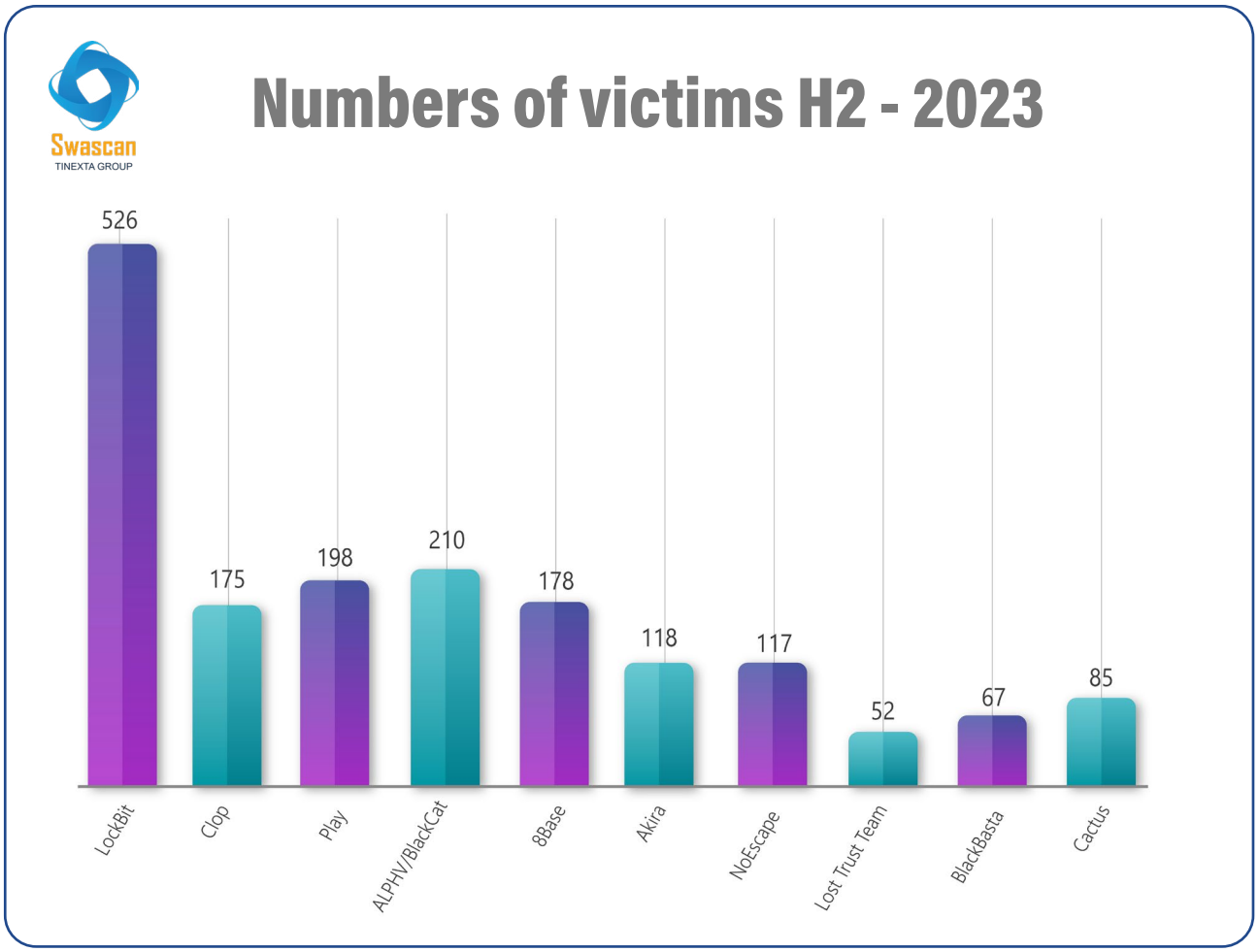


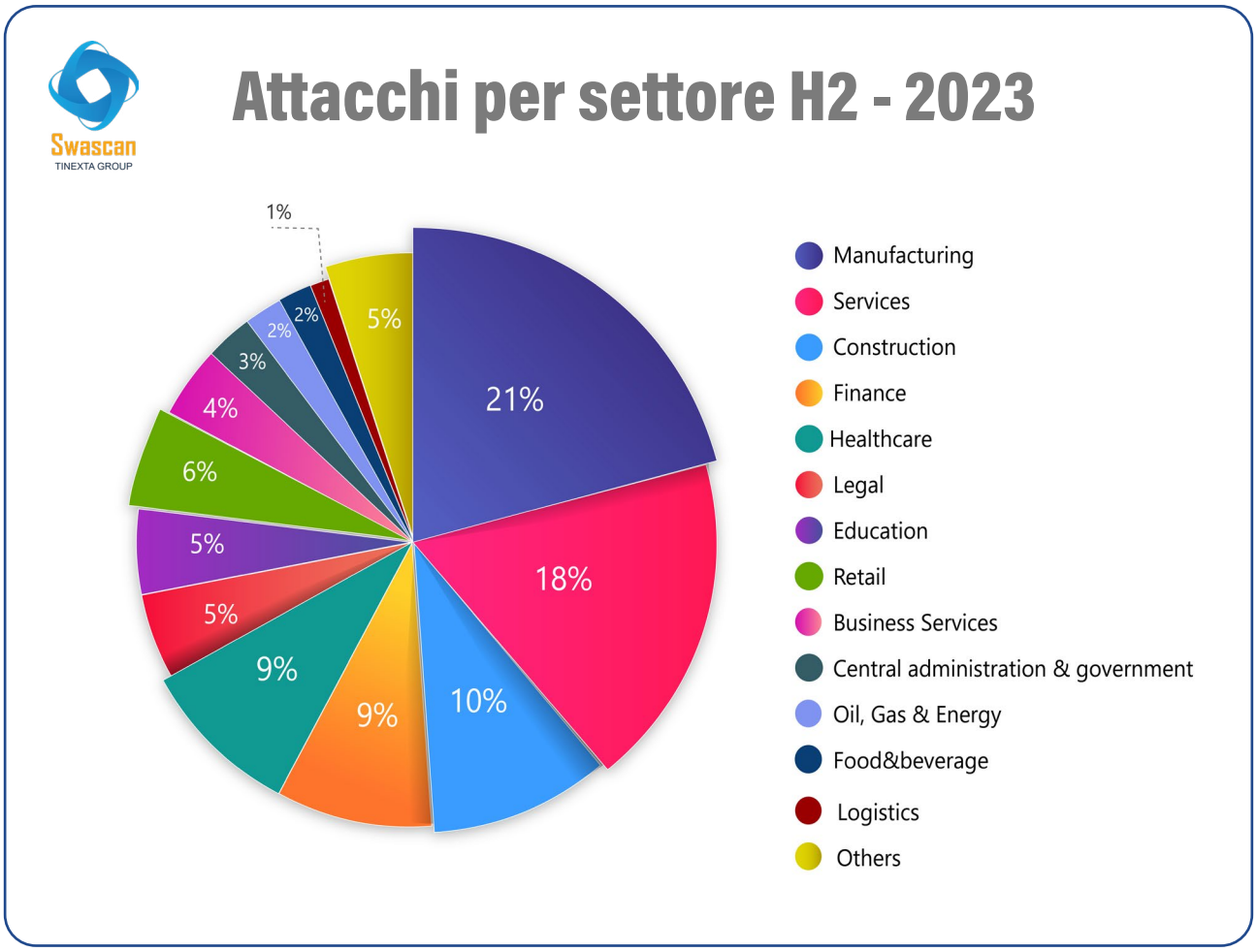
Gruppi attivi



H2 in dettaglio - Ransomware







Cosa ci dicono i numeri?

La classifica delle vittime di ransomware suddivise per settore fornisce una panoramica significativa delle aree più colpite da questa minaccia cibernetica in rapida crescita. Analizziamo attentamente i dati per comprendere le tendenze emergenti e le possibili implicazioni per la sicurezza informatica nelle diverse industrie.

Manifatturiero (Manufacturing): 21%

La predominanza del settore manifatturiero potrebbe essere attribuita alla sua crescente interconnessione digitale, con la presenza di infrastrutture complesse e la dipendenza da sistemi automatizzati. L'industria manifatturiera dovrebbe concentrarsi ulteriormente sulla sicurezza informatica per mitigare rischi futuri.

Servizi (Services): 18%

Il settore dei servizi, essendo ampio e diversificato, presenta una vasta gamma di obiettivi per gli attacchi di ransomware. Le aziende del settore dovrebbero implementare strategie di difesa avanzate, considerando la diversità dei servizi offerti.

Costruzioni (Construction): 10%

Nonostante la percezione comune che il settore delle costruzioni possa essere meno vulnerabile, il 10% indica una presenza significativa di ransomware. Potrebbe essere dovuto alla crescente digitalizzazione nel settore e alla dipendenza da sistemi di gestione dati.

Finanza (Finance): 9%

Le istituzioni finanziarie sono fra i bersagli principali. Nonostante gli sforzi per implementare misure di sicurezza avanzate, il settore finanziario rimane vulnerabile a causa dell'alto valore delle informazioni gestite.

Sanità (Healthcare): 9%

La presenza del ransomware nel settore sanitario è allarmante, considerando la sensibilità dei dati personali e sanitari. La necessità di implementare misure di sicurezza robuste è imperativa per garantire la continuità delle cure e proteggere la privacy dei pazienti.

Legale (Legal): 5%

Anche il settore legale non è immune agli attacchi di ransomware, con il 5% di vittime. L'accesso a informazioni sensibili e riservate lo rende un obiettivo attraente per gli aggressori.

Educazione (Education): 5%

L'educazione, con il 5%, può essere bersaglio a causa della crescente digitalizzazione delle istituzioni accademiche. La protezione dei dati degli studenti e delle informazioni accademiche è essenziale.

Vendite al dettaglio (Retail): 6%

Il settore retail, con il 6%, può essere vulnerabile a causa dell'ampia presenza online e delle transazioni finanziarie. Le aziende devono focalizzarsi su soluzioni di sicurezza per proteggere sia i dati dei clienti che le operazioni aziendali.

Servizi Aziendali (Business Services): 4%

La varietà dei servizi aziendali contribuisce al 4%. Le aziende devono implementare misure di sicurezza avanzate per garantire la protezione dei dati aziendali e dei clienti.

Amministrazione Centrale e Governo: 3%

La presenza del ransomware nel settore governativo sottolinea l'importanza di garantire la sicurezza delle informazioni sensibili e dei servizi pubblici.

Petrolio, Gas ed Energia: 2%

Anche il settore energetico è coinvolto, evidenziando la necessità di proteggere le infrastrutture critiche contro gli attacchi informatici.

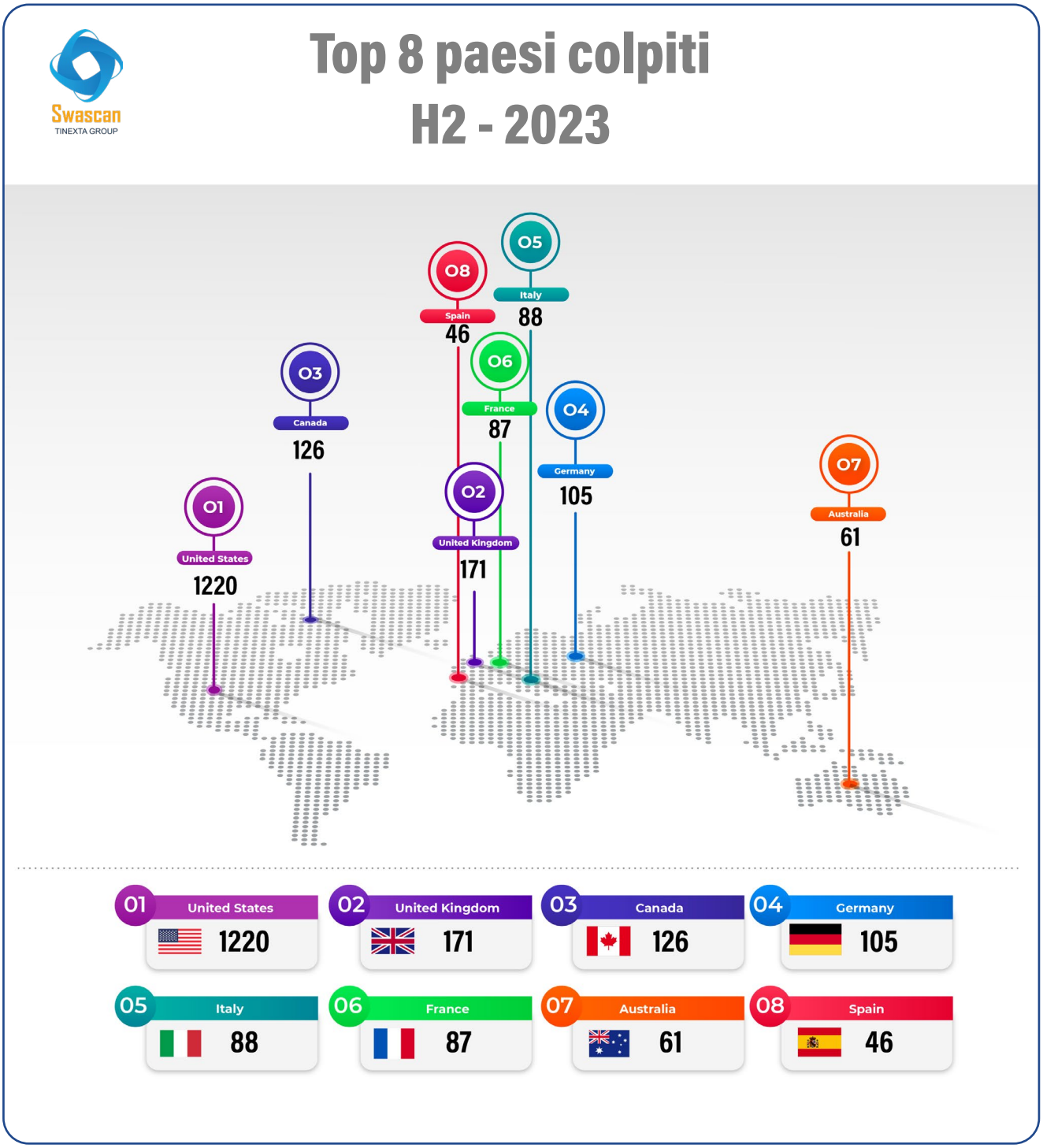
Alimentare e Bevande: 2%

Nonostante la percentuale relativamente bassa, il settore alimentare e delle bevande è un obiettivo interessante per via della catena di approvvigionamento complessa e della sensibilità dei dati.

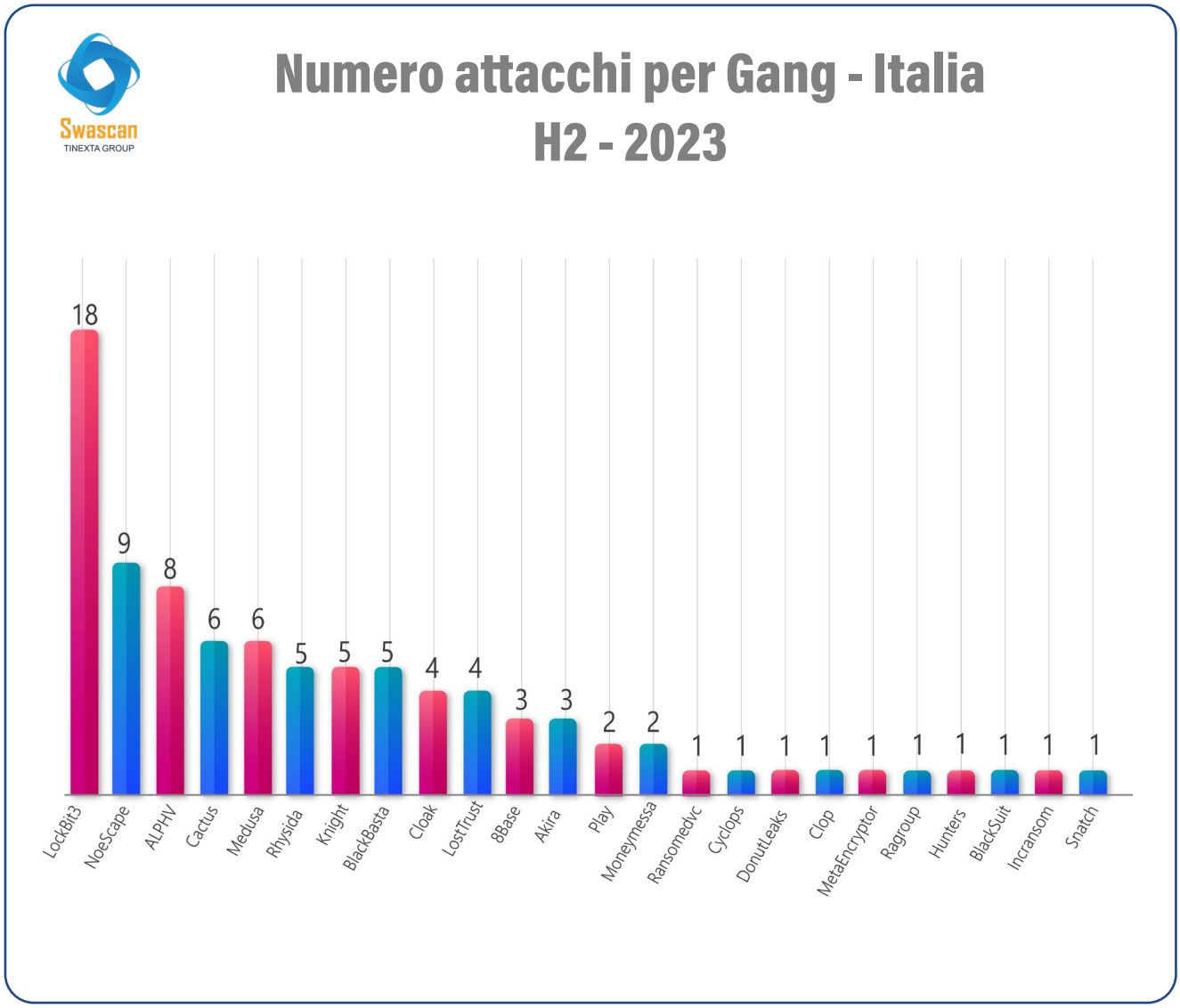
Logistica: 1%

Anche se il settore logistico rappresenta solo l'1%, la sua importanza nella gestione della supply chain lo rende un obiettivo significativo.

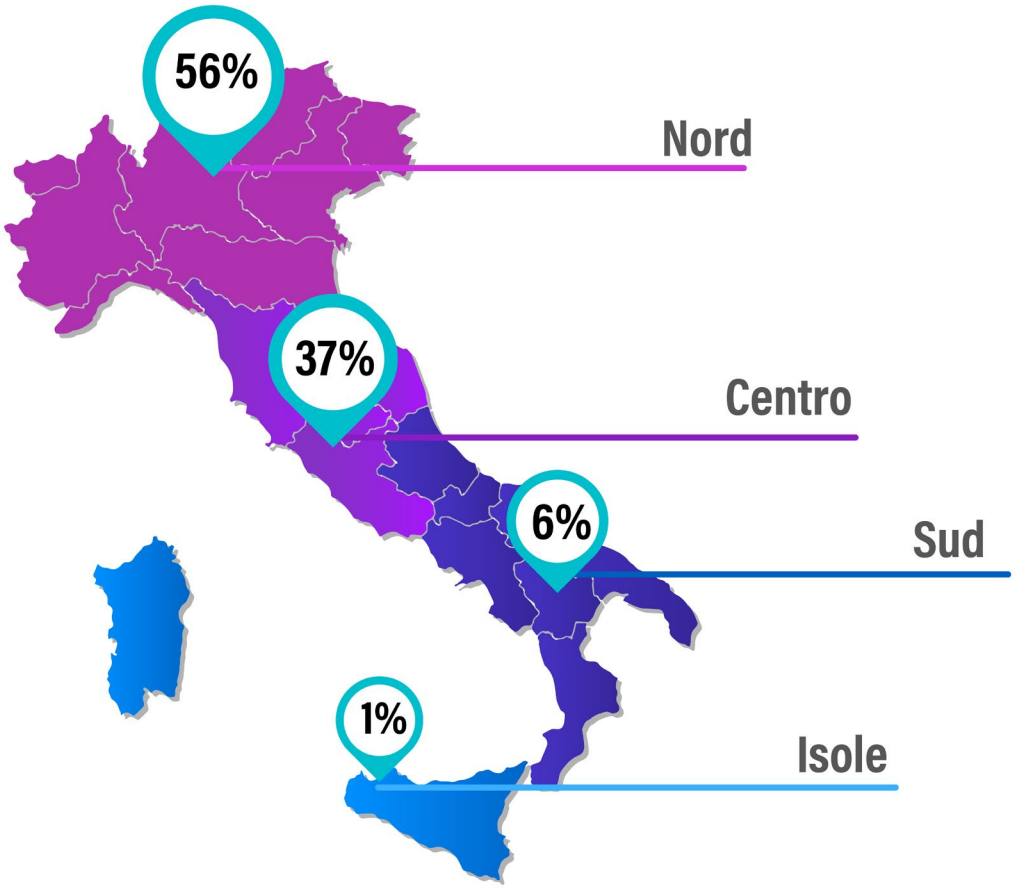
La geografia delle vittime



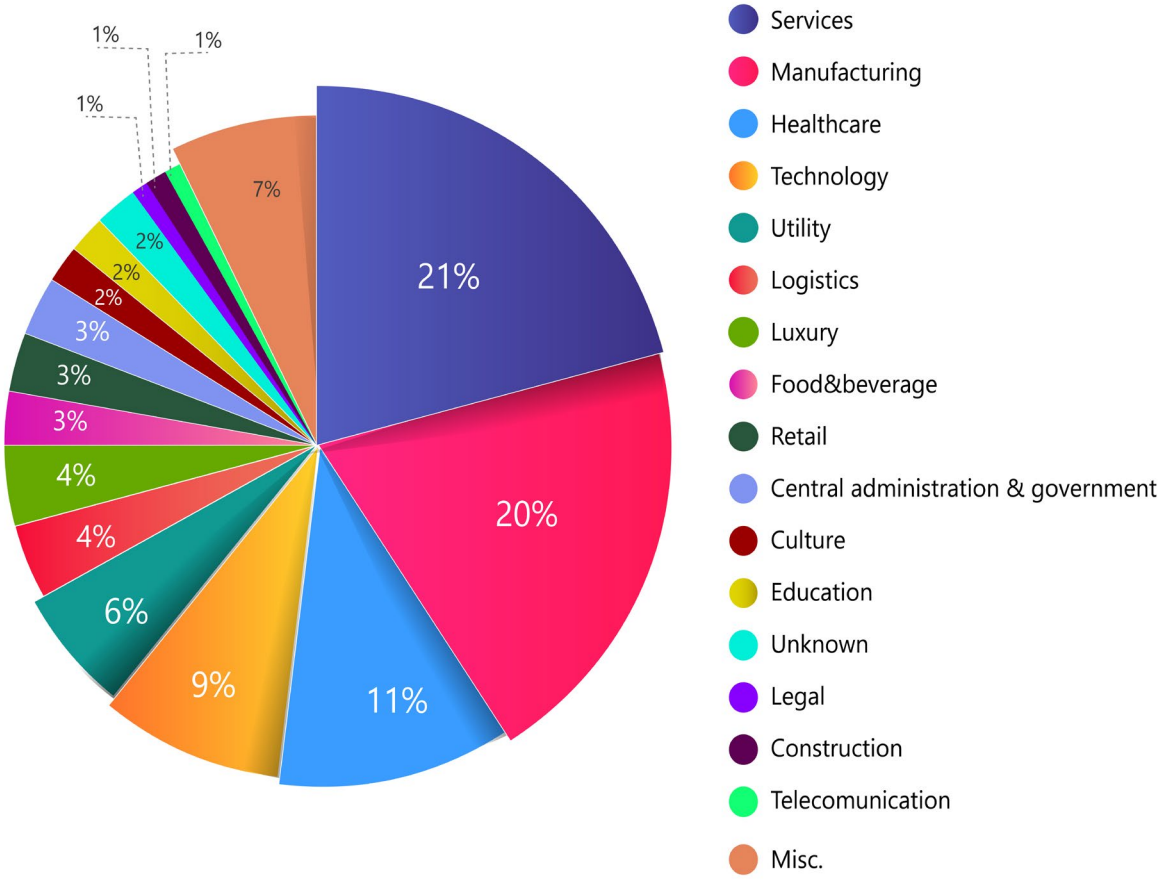
H2 Italia – Ransomware



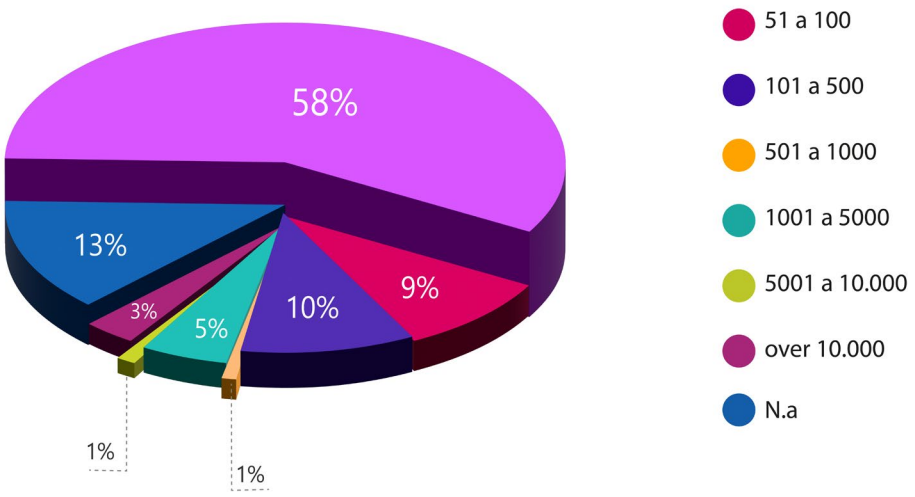
Attacchi per regioni - Italia
H2 - 2023



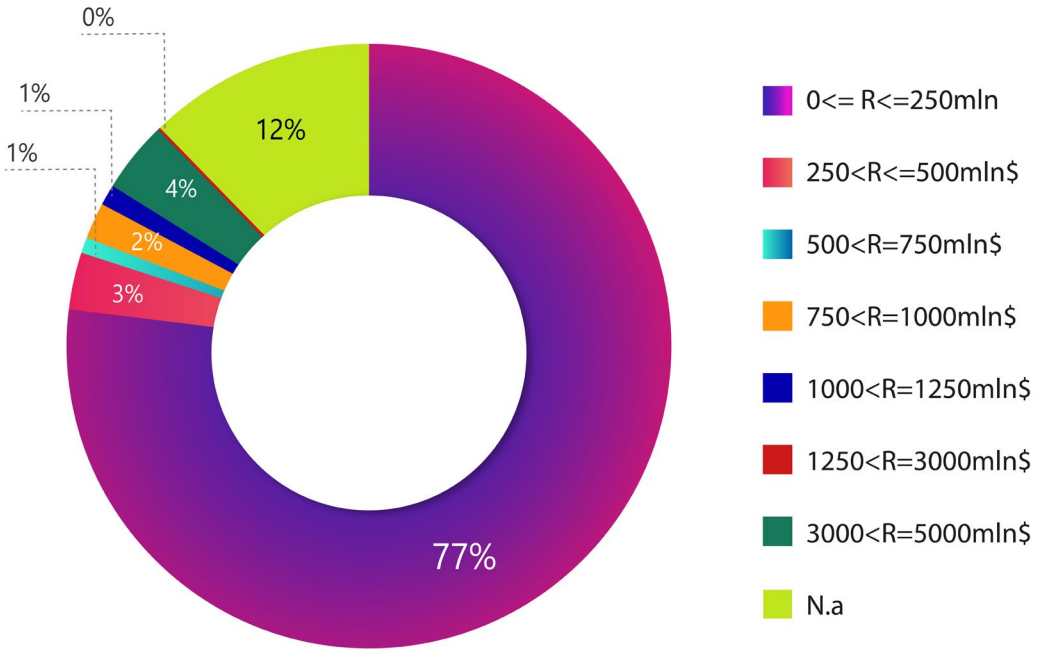
Attacchi per settore - Italia
H2 - 2023



Numero Dipendenti Aziende Colpite Italia - H2 2023



Spaccato Aziende Colpite In Base A Fatturato- Italia - H2 2023



Key Takeaway

L'analisi dei dati sugli attacchi ransomware in Italia nel secondo semestre (H2) dell'anno offre uno sguardo dettagliato sulla situazione, comprendendo le gang coinvolte, i settori colpiti, le dimensioni delle aziende coinvolte e il fatturato delle vittime. Ecco una disamina forbita:

Gang Coinvolte

Nel periodo considerato, l'Italia ha sperimentato un totale di **88 attacchi** ransomware. Le gang coinvolte mostrano una varietà di attori, con **Lockbit3** in testa, registrando 18 attacchi. **Alphv** e **NoEscape** seguono con 8 e 9 attacchi rispettivamente. La diversità delle gang riflette una minaccia crescente e articolata da parte di attori malevoli con tattiche sempre più sofisticate.

Settori Colpiti

I settori maggiormente colpiti dagli attacchi ransomware sono **i servizi (21%)** e **la manifattura (20%)**. La crescente dipendenza digitale in settori critici come **la sanità (11%)** e **la tecnologia (9%)** dimostra la pervasività della minaccia. Altri settori interessati includono servizi pubblici, logistica, lusso e alimentari, rivelando una diversificazione delle vittime.

Dimensioni Aziendali

La maggior parte delle aziende coinvolte ha un numero di dipendenti compreso tra **1 e 50 (58%)**. Questo suggerisce che gli attacchi ransomware non colpiscono solo grandi imprese, ma anche PMI. Il coinvolgimento di aziende di varie dimensioni sottolinea la necessità di misure di sicurezza universali.

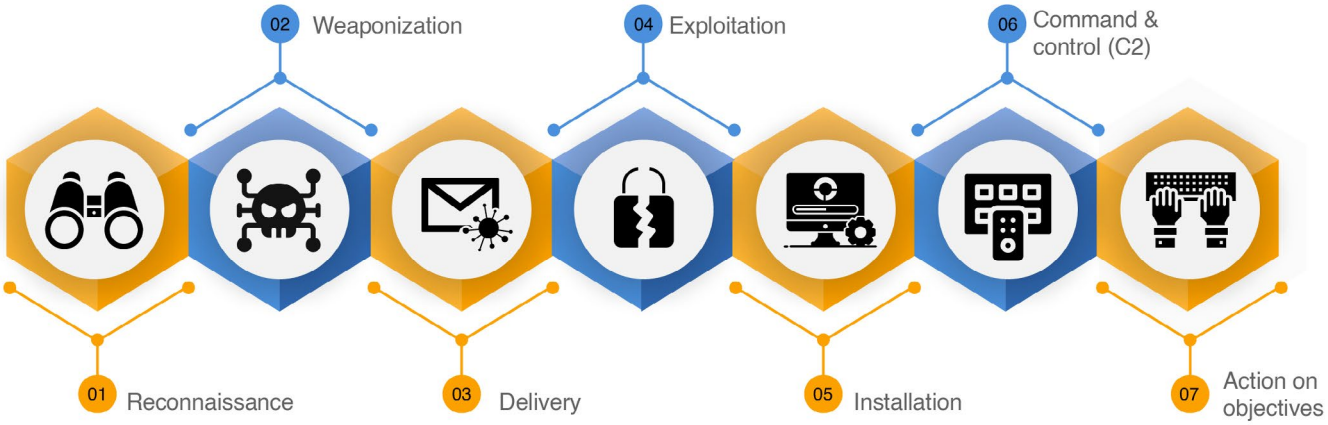
Fatturato Aziendale

L'analisi del fatturato delle aziende colpite mostra che la stragrande maggioranza **(77%)** ha un fatturato compreso tra 0 e 250 milioni di dollari. Questo dato sottolinea che anche aziende con un reddito relativamente modesto sono vulnerabili agli attacchi ransomware. La diversità delle vittime, dal punto di vista economico, mette in luce la necessità di soluzioni di sicurezza a tutte le dimensioni aziendali.

La cyber kill chain: un approccio strategico per difendersi dagli attacchi informatici

Dopo aver visto i numeri più significativi per gli attacchi ransomware, facciamo un passo indietro e diamo ad uno sguardo al come si giunge a subire un attacco.

Nel panorama sempre più complesso e frequente degli attacchi informatici, la Cyber Kill Chain si presenta come uno strumento fondamentale per identificare e contrastare le minacce provenienti dai criminal hacker. Questa metodologia di difesa, ispirata al concetto di Kill Chain utilizzato in campo militare, è stata adottata nel settore della cyber security al fine di individuare le fasi attraverso le quali un attacco si sviluppa e di preparare una strategia difensiva adeguata e si compone di sette fasi ben definite. Queste fasi rappresentano i passaggi che un potenziale criminal hacker dovrebbe compiere per portare a termine un attacco e consentono di comprendere il modus operandi degli aggressori, individuando i segnali di attacco e mettendo in atto le necessarie contromisure.

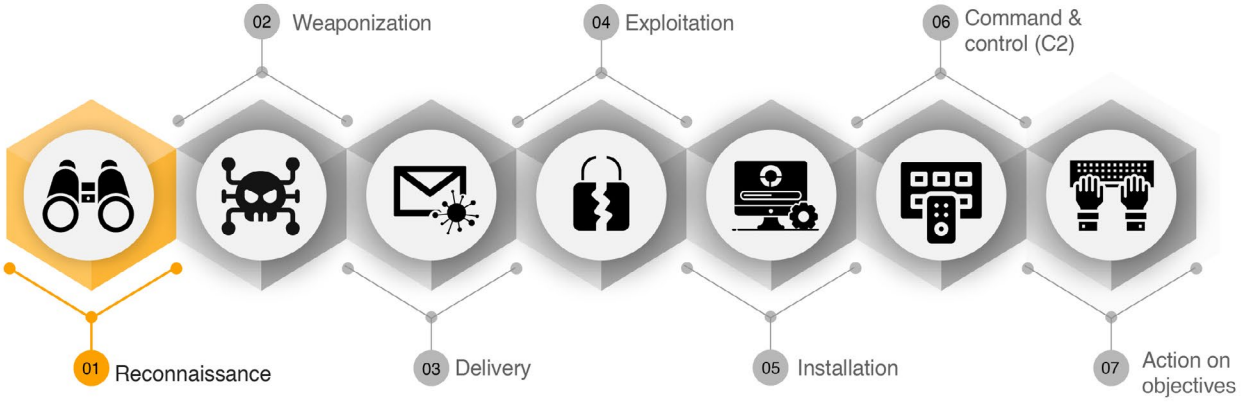


Le sette fasi della Cyber Kill Chain sono le seguenti:

1. **Reconnaissance:** in questa fase il criminal hacker individua il bersaglio e conduce una ricerca approfondita per identificare le vulnerabilità presenti nel sistema di sicurezza del target. Questa fase è di fondamentale importanza poiché determina il successo delle fasi successive.
2. **Weaponization:** nel secondo step l'attaccante utilizza le informazioni raccolte nella fase precedente per selezionare gli strumenti più adatti a creare un accesso remoto al sistema bersaglio.
3. **Delivery:** in questa fase, il malware creato viene consegnato al bersaglio attraverso diversi vettori, come ad esempio mail di phishing o link presenti su siti web compromessi.
4. **Exploitation:** una volta consegnato al bersaglio, il malware viene attivato e sfrutta le vulnerabilità del sistema per ottenere un accesso non autorizzato o eseguire altre azioni malevole.
5. **Installation:** durante la fase di installation, l'attaccante si assicura di installare ed eseguire il malware nel sistema bersaglio. Questo gli consente di aggirare i controlli di sicurezza e mantenere l'accesso al sistema. L'installazione del malware avviene grazie all'exploit selezionato durante la fase di weaponization e viene eseguita durante la fase di exploitation.
6. **Command & Control:** nel sesto step della catena, gli attaccanti stabiliscono una connessione tra il sistema vittima e la macchina remota da cui operano. Questa connessione permette loro di ottenere un controllo persistente e un accesso continuo all'ambiente della vittima.
7. **Actions on Objectives:** nell'ultimo anello della catena, gli attaccanti portano a termine l'attacco colpendo l'obiettivo prefissato, e questo può portare alla manipolazione dei dati, l'esfiltrazione di informazioni sensibili, la distruzione dei dati o l'accesso non autorizzato a risorse riservate.

La Cyber Kill Chain fornisce un quadro strategico per comprendere gli attacchi informatici e agire di conseguenza. Non esiste un approccio unico per affrontare un attacco, ma questo modello consente di mettersi nei panni dell'attaccante e di adottare un approccio simile per prevenire o mitigare l'intrusione. Nell'analisi di seguito vedremo le diverse fasi della Cyber Kill Chain nel dettaglio.

Reconnaissance



La fase di reconnaissance è la prima importante tappa all'interno della Cyber Kill Chain, durante la quale gli attaccanti raccolgono informazioni preziose per pianificare un attacco mirato. Durante questa fase, vengono adottate diverse strategie, tra cui, ad esempio, la raccolta di credenziali da mercati nel Darkweb, l'identificazione di nuove vulnerabilità (CVE) e l'utilizzo di campagne di social engineering.

Gli attaccanti possono acquisire credenziali sensibili da mercati nel Deep e Darkweb, dove vengono scambiate illegalmente informazioni rubate come username, password e dettagli di accesso a sistemi o account online. Queste credenziali possono provenire da violazioni dei dati precedenti o da tecniche di phishing e possono essere utilizzate per ottenere un accesso non autorizzato a sistemi o per impersonare un utente legittimo.

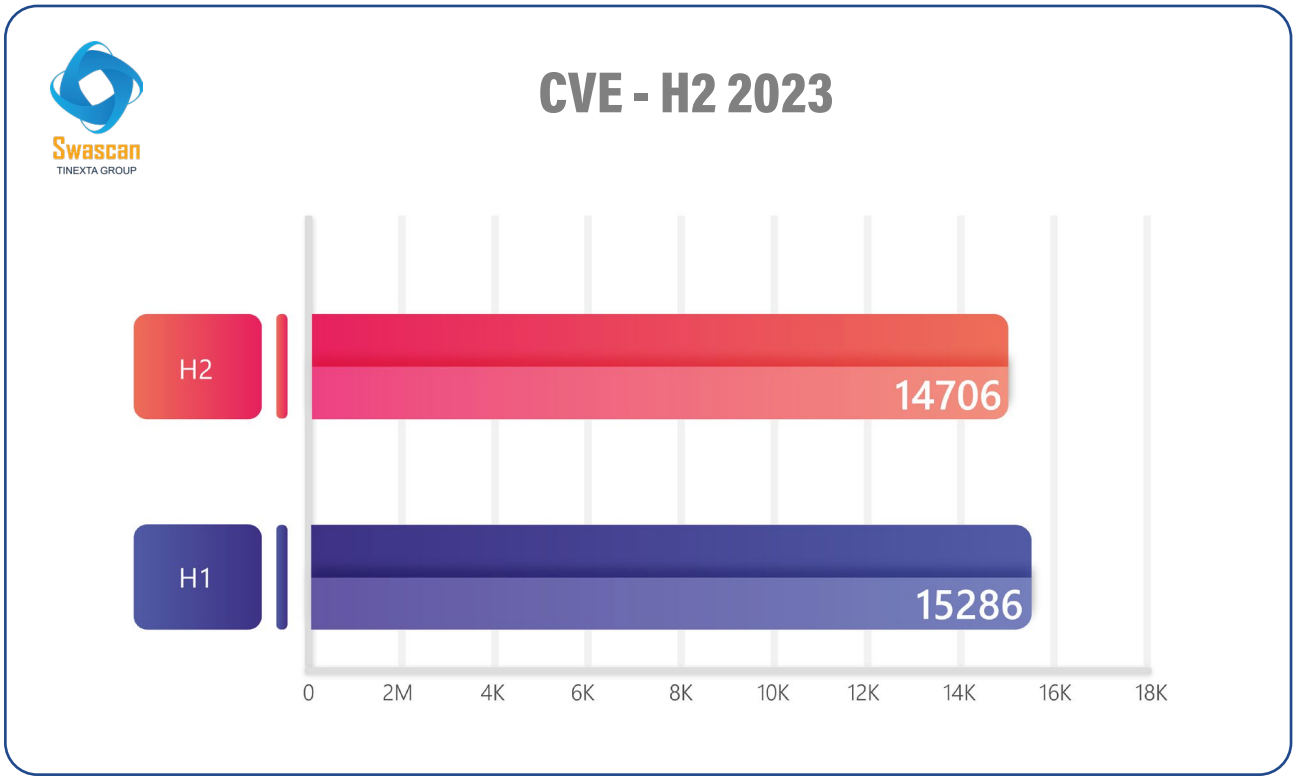
Le campagne di social engineering costituiscono un'altra tattica comune nella fase di Reconnaissance. Gli attaccanti cercano di raccogliere informazioni preziose sugli utenti o sulle organizzazioni attraverso l'inganno e la manipolazione psicologica. Questo può coinvolgere l'invio di e-mail o messaggi di testo fraudolenti che richiedono informazioni sensibili o che inducono gli utenti a fare click su link malevoli. Per esempio, nel **Q2** sono state osservate difatti **155'683 campagne di phishing.** Attraverso queste tattiche, gli aggressori cercano di ottenere accesso a informazioni confidenziali o di ingannare gli utenti per facilitare fasi successive dell'attacco.

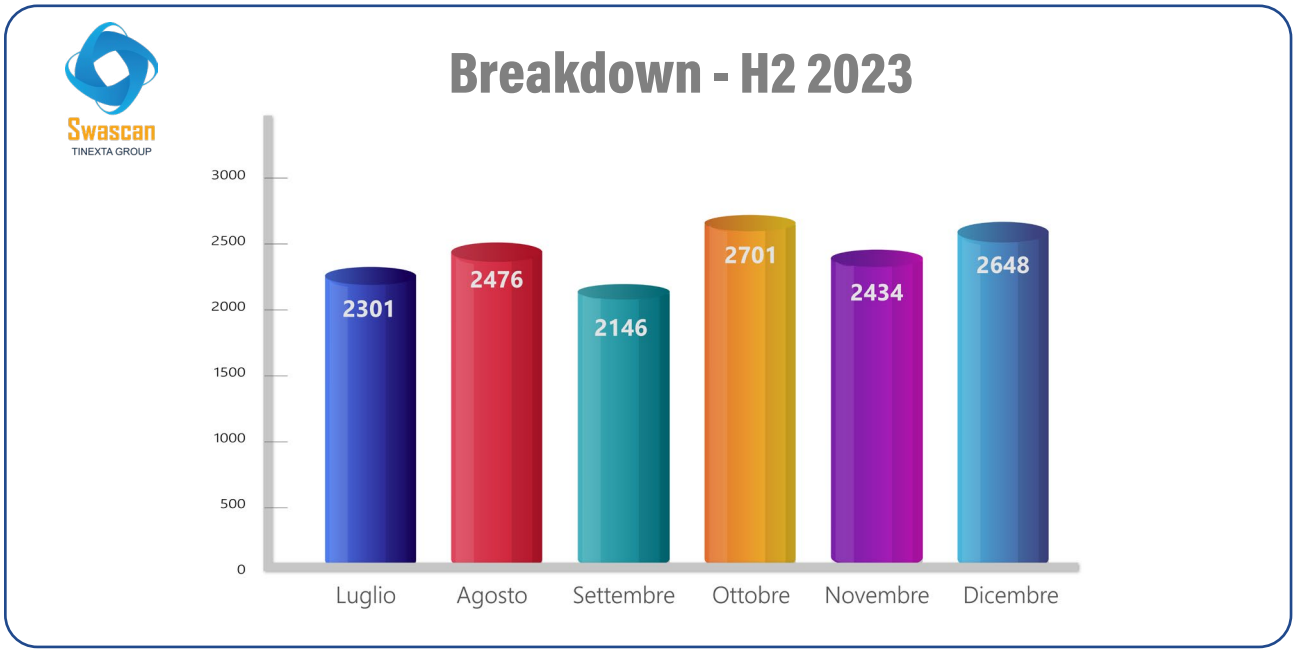
Tra le campagne analizzate è possibile notare alcuni esempi dove si tenta di ingannare la vittima fingendosi prodotti o servizi reali:

Common Vulnerabilities and Exposures

L'identificazione di nuove vulnerabilità, note come **CVE** (Common Vulnerabilities and Exposures), è un'altra componente critica della fase di Reconnaissance. Gli aggressori monitorano costantemente le nuove vulnerabilità che vengono scoperte nei software, nei sistemi operativi o nelle applicazioni. Questo permette loro di individuare i punti deboli nei sistemi bersaglio e di sfruttarli successivamente durante l'attacco.

Nell'H1 relativo al 2023 erano state pubblicate **15286 nuove CVE** contro le 14706 pubblicate nell'H2:





Come mitigare il rischio:

1. Monitoraggio costante:

Mantenere un monitoraggio regolare delle fonti di informazioni sulle vulnerabilità, come NIST National Vulnerability Database (NVD), per essere tempestivi nell'identificare nuove CVE rilevanti per i propri sistemi.

2. Valutazione dell'impatto:

Classificare le vulnerabilità in base all'impatto che potrebbero avere sui sistemi e sui dati. Questo aiuta a prioritizzare le azioni e a concentrarsi sulle vulnerabilità più critiche.

3. Applicazione rapida di patch:

Aggiornare e Patchare i sistemi tempestivamente, seguendo le indicazioni delle CVE. L'implementazione tempestiva riduce la finestra di esposizione alle minacce.

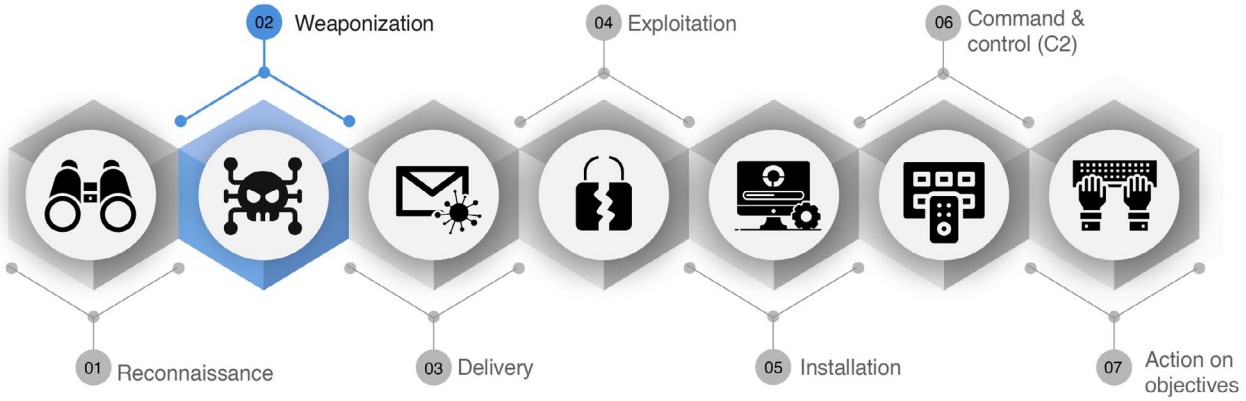
4. Gestione delle configurazioni:

Assicurarsi che i sistemi siano configurati correttamente e che le misure di sicurezza siano adeguate. Una corretta configurazione può mitigare molte vulnerabilità.

5. Monitoraggio delle reti:

Utilizzare strumenti di monitoraggio delle reti per rilevare attività sospette o tentativi di sfruttare vulnerabilità noti. La tempestiva identificazione può prevenire potenziali danni.

Weaponization



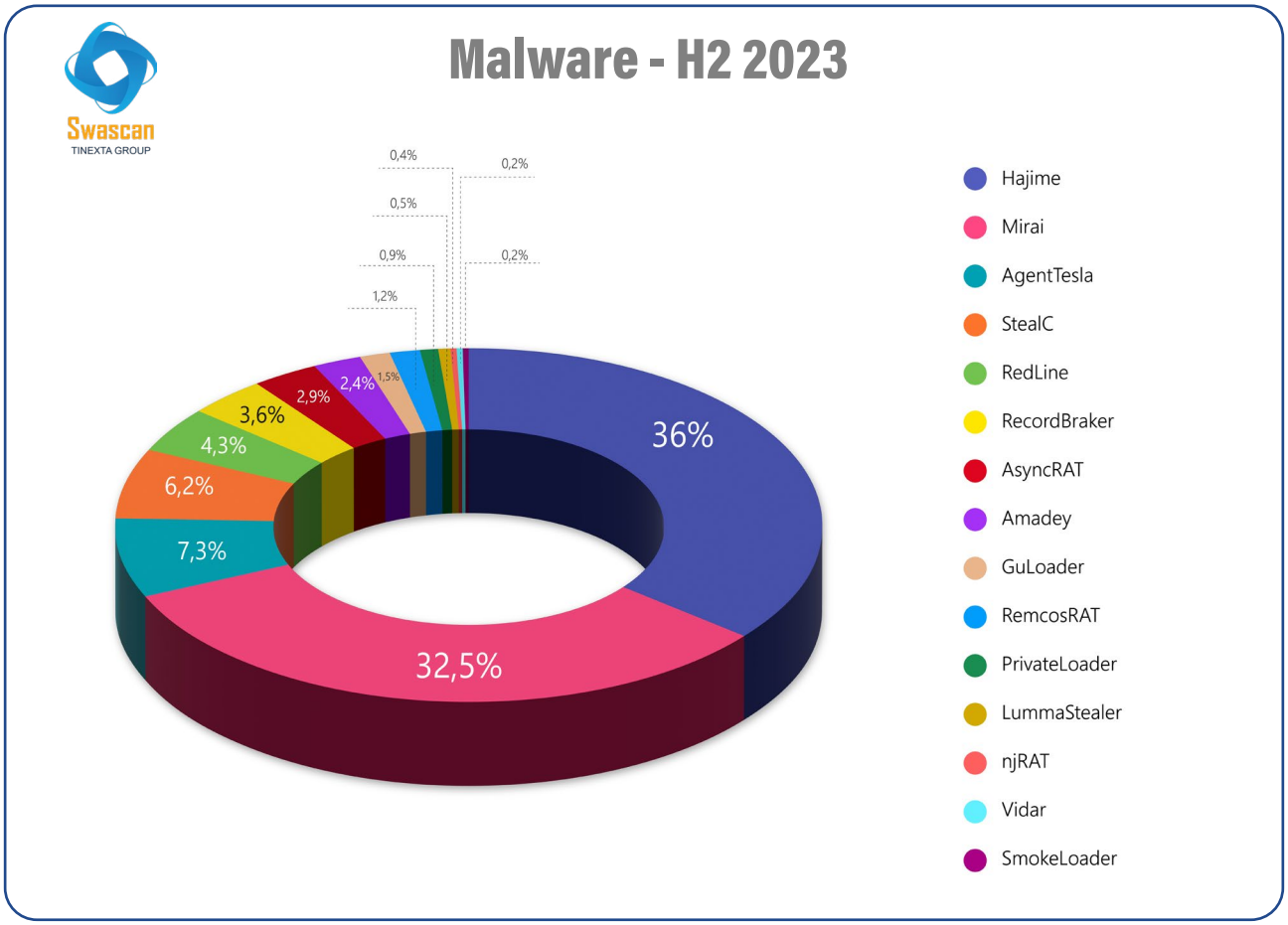
La fase di weaponization è un'importante tappa all'interno della Cyber Kill Chain, in cui gli aggressori trasformano un payload malevolo in un'arma pronta per essere utilizzata contro il sistema target. Durante questa fase, vengono spesso veicolati diversi tipi di malware, tra cui botnet, infostealer e RAT.

Le botnet sono reti di computer compromessi e controllati da remoto dagli attaccanti. Questi bot possono essere utilizzati per condurre attacchi distribuiti di denial of service (DDoS), inviare spam o propagare ulteriormente il malware. L'attaccante sfrutta la botnet per inviare comandi ai bot compromessi e per ricevere informazioni raccolte da essi.

Gli infostealer sono tipi di malware progettati per rubare informazioni sensibili dai sistemi infettati. Possono infatti raccogliere dati come credenziali di accesso, informazioni bancarie, dati di carte di credito o altre informazioni personali. Una volta raccolte, le informazioni vengono inviate al C2 dell'attaccante per un successivo sfruttamento o utilizzo a fini illeciti.

I RAT, ovvero i Trojan di accesso remoto, consentono agli aggressori di assumere il controllo completo del sistema compromesso da remoto. Gli attaccanti possono accedere al sistema, eseguire comandi, scaricare e installare ulteriori malware, esfiltrare dati o compiere altre azioni dannose. Questi strumenti offrono agli attaccanti un controllo furtivo e persistente sul sistema compromesso.

La fase di weaponization è cruciale per gli aggressori, poiché rappresenta il momento in cui il payload malevolo viene trasformato in uno strumento di attacco funzionante. Gli aggressori sfruttano queste forme di malware, come botnet, infostealer e RAT, per ottenere e mantenere l'accesso non autorizzato al sistema bersaglio e per condurre ulteriori fasi dell'attacco informatico.



Key Takeaway

Hajime e **Mirai** sono i malware più diffusi con **1127** e **1019** rilevamenti rispettivamente. Entrambi sono noti per attaccare dispositivi Internet of Things (IoT) e possono essere correlati a botnet finalizzate a svolgere attacchi distribuiti del tipo DDoS.

D'altro canto, AgentTesla e StealC sono più orientati al furto di informazioni. La loro presenza potrebbe indicare un interesse crescente nel furto di dati sensibili o informazioni personali.

Come se non bastasse, la presenza di diversi tipi di malware come RedLine, RecordBraker, AsyncRAT, Amadey, GuLoader, ecc., suggerisce un panorama variegato di minacce informatiche. Questa diversità può indicare che gli attaccanti stanno sfruttando diverse tattiche e vettori di attacco, mentre alcuni malware come GuLoader, PrivateLoader, e LummaStealer sono progettati per caricare e distribuire ulteriori carichi dannosi. La presenza di questi malware può indicare una tendenza a utilizzare tecniche di caricamento di payload specifici per compiere attacchi mirati.

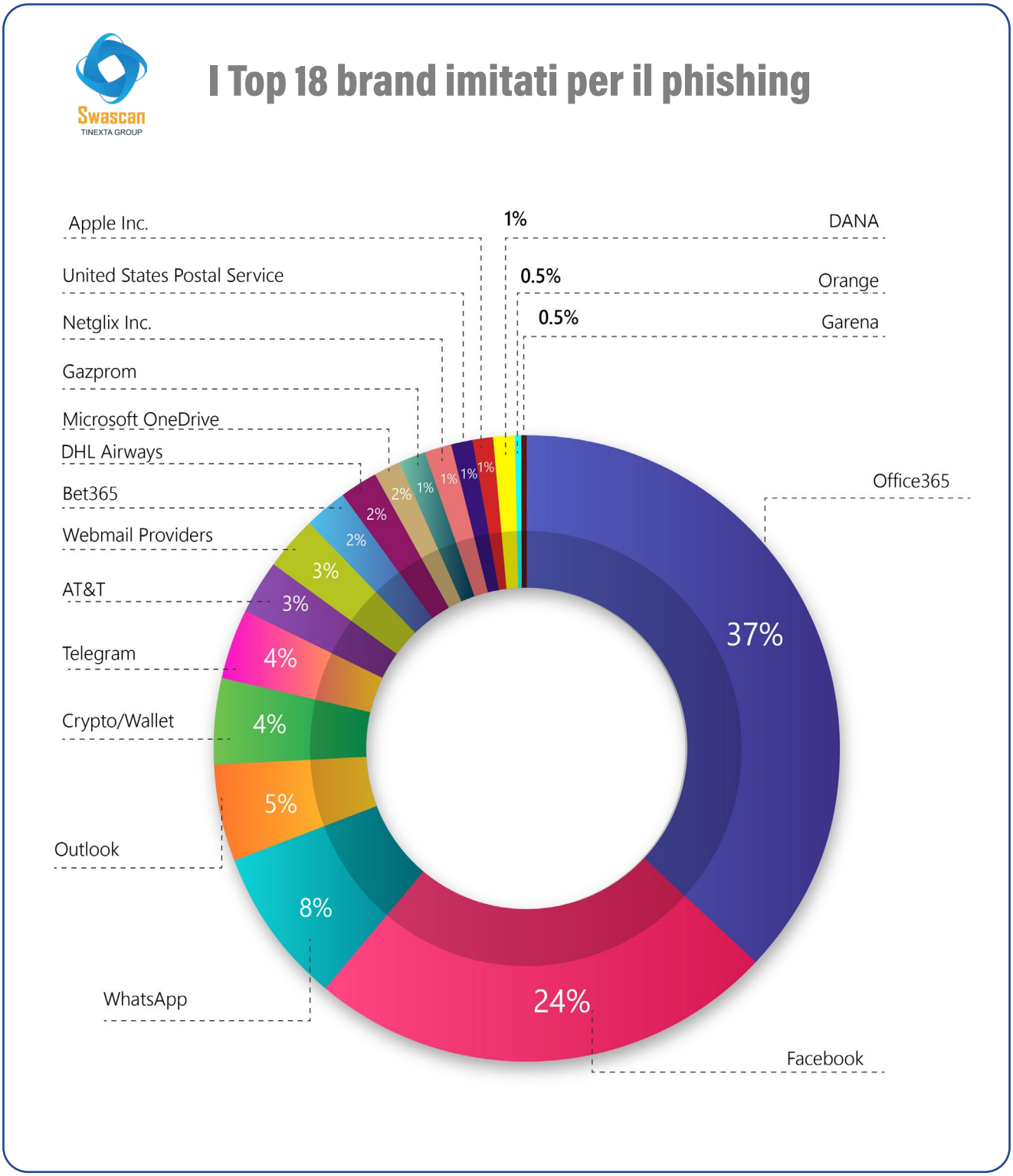
Delivery – Phishing

Una delle minacce più diffuse e dannose rilevate nell'H1 è il phishing, un attacco informatico che mira a ingannare gli utenti e a ottenere accesso non autorizzato alle loro informazioni.

Nel contesto della Cyber Kill Chain il phishing si colloca nella fase di "Delivery" o consegna.

La fase di delivery rappresenta il momento in cui l'attaccante consegna un payload o un meccanismo di attacco all'utente prescelto. Il phishing, in particolare, sfrutta tecniche sofisticate per inviare e-mail, messaggi di testo o comunicazioni ingannevoli che sembrano provenire da fonti attendibili o legittime. Gli aggressori cercano di ingannare gli utenti persuadendoli a fare clic su link malevoli, scaricare allegati infetti o rivelare informazioni riservate.

Il phishing è una minaccia in costante evoluzione, adattandosi alle nuove tecnologie e alle difese implementate dagli esperti di sicurezza. Durante il secondo semestre del 2023 (H2 2023), sono stati segnalati complessivamente 448,665 portali dedicati al di phishing, con alcune campagne particolarmente rilevanti che hanno coinvolto diverse aziende e settori.



Le principali campagne di phishing durante l'H2 2023 hanno utilizzato i seguenti brand come esca:

1. **Office365:** Con un totale di **79,809 istanze**, Office365 è stato ampiamente utilizzato come esca per convincere gli utenti a inserire le proprie credenziali di accesso in siti web contraffatti, con l'obiettivo di rubare informazioni personali e compromettere la sicurezza.

2. **Facebook:** con **51,698 istanze,** Facebook è stato sfruttato per indurre gli utenti a fornire le proprie credenziali attraverso siti web falsificati, sfruttando la popolarità del social network per attirare le vittime.

3. **Whatsapp:** gli attaccanti hanno sfruttato la popolarità di Whatsapp, con **17,556 istanze,** per ingannare gli utenti attraverso messaggi falsi e siti web contraffatti, mirando a ottenere informazioni sensibili.

4.**Outlook:** con **10,809 istanze**, Outlook è stato spesso utilizzato come esca per inviare e-mail contraffatte, mirando a indurre gli utenti a cliccare su link malevoli o fornire informazioni riservate.

5. **Crypto/Wallet:** con **9,417 istanze**, le campagne di phishing relative a Crypto/Wallet hanno cercato di sfruttare l'interesse crescente nelle criptovalute, cercando di ottenere accesso a portafogli digitali e informazioni finanziarie.

6. **Telegram:** anche Telegram è stato coinvolto in **7,701 istanze**, utilizzato per ingannare le vittime attraverso messaggi fraudolenti, con l'obiettivo di ottenere informazioni personali.

Questi dati evidenziano come i brand menzionati siano stati sfruttati come esche in varie campagne di phishing, dimostrando la versatilità degli attaccanti nel mirare le piattaforme e i servizi popolari per ingannare le vittime. È fondamentale che gli utenti siano consapevoli di tali minacce e adottino misure di sicurezza adeguate a proteggere le proprie informazioni personali e aziendali.

Analizzando i brand coinvolti nelle campagne di phishing durante l'H2 2023, emergono diverse considerazioni. Gli attaccanti hanno mirato piattaforme ampiamente utilizzate come **Office365**, **Facebook, Whatsapp** e **Outlook**, sfruttando la familiarità degli utenti con questi servizi per ingannarli. Questo evidenzia una strategia volta a massimizzare il numero di vittime sfruttando la popolarità delle piattaforme online.

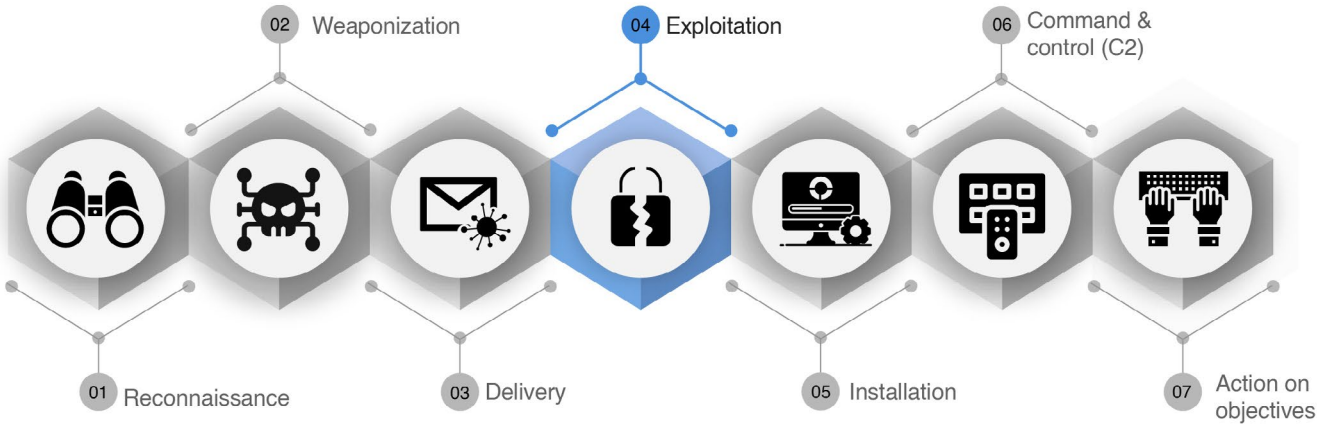
La presenza di **Crypto/Wallet** tra i brand bersagliati indica un interesse crescente da parte degli attaccanti nelle criptovalute. Questo può essere collegato all'obiettivo di ottenere accesso a portafogli digitali o informazioni finanziarie legate alle criptovalute, riflettendo l'evoluzione delle tendenze nel mondo della sicurezza informatica. **Telegram** è stato coinvolto in attacchi di phishing, suggerendo che gli attaccanti stanno esplorando l'uso di piattaforme di messaggistica per diffondere messaggi fraudolenti. Questa tattica potrebbe rivelarsi efficace data la diffusione di queste applicazioni per la comunicazione.

Inoltre, L'inclusione di **DHL** preda sul classico sentimento di attesa per tutti coloro che utilizzano servizi di spedizione/consegna pacchi. Questo approccio mira a ingannare le vittime, convincendole a fornire informazioni personali.

Oltre ai servizi online e alle piattaforme di comunicazione, settori specifici come le scommesse online (**Bet365**) e l'energia (**Gazprom**) sono stati coinvolti.

Ciò indica una diversificazione degli obiettivi degli attaccanti, che cercano di sfruttare la popolarità e la fiducia legate a brand specifici in settori vari. La mutevole natura delle minacce di phishing durante l'H2 2023 riflette un adattamento continuo degli attaccanti alle abitudini degli utenti e alle tendenze del momento. La consapevolezza degli utenti e l'implementazione di pratiche di sicurezza avanzate sono fondamentali per mitigare questi rischi in un contesto di minacce in costante evoluzione.

Exploitation



La "exploitation" è la fase che segue la consegna (delivery) e la messa in opera (weaponization). Nella Cyber Kill Chain, durante la fase di exploitation, gli attaccanti sfruttano le vulnerabilità scoperte nelle fasi precedenti per infiltrarsi ulteriormente nella rete di un obiettivo e raggiungere i loro obiettivi. In questo processo, i criminali informatici spesso si spostano lateralmente attraverso una rete per raggiungere i loro bersagli.

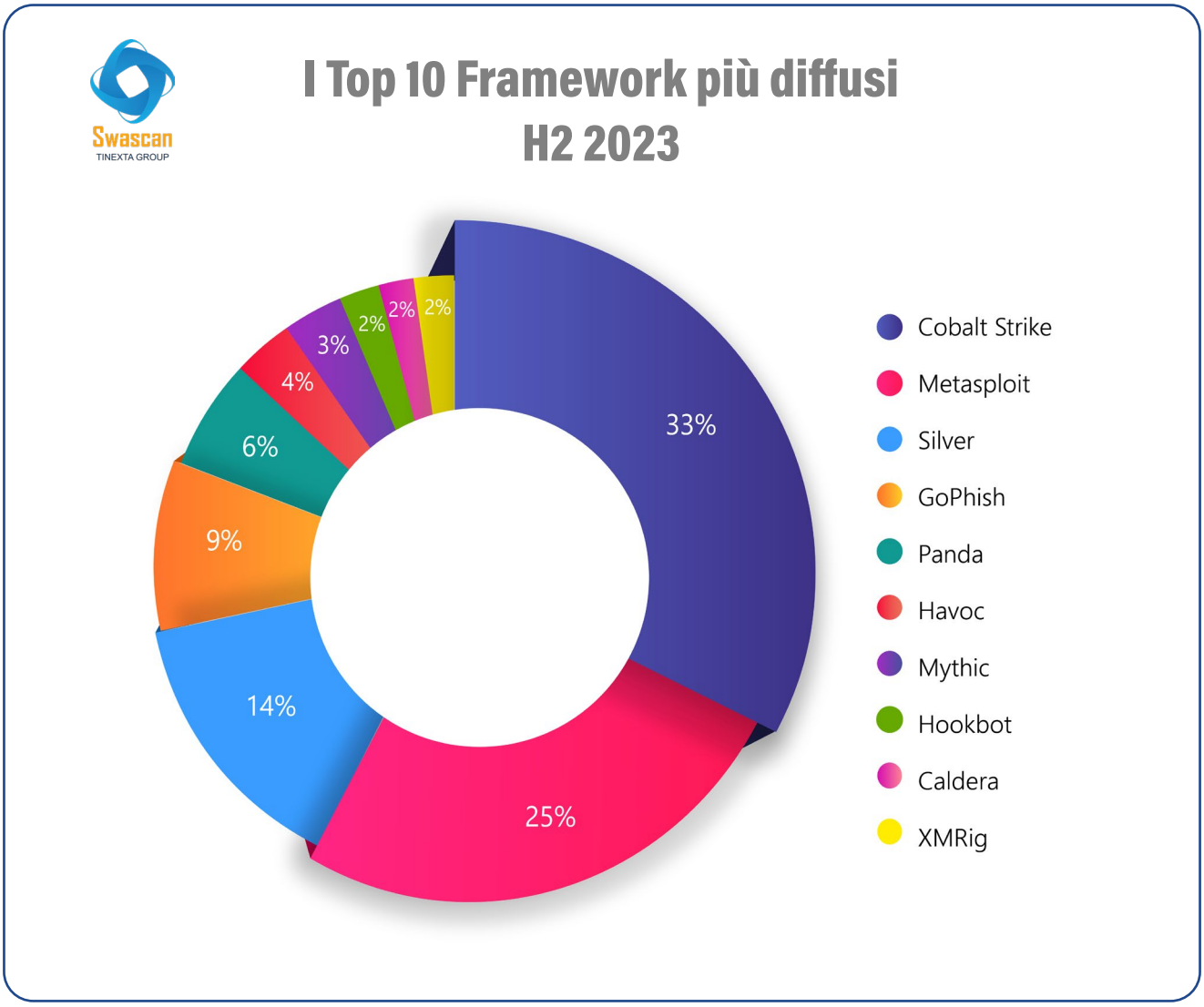
L'exploitation può talvolta condurre gli attaccanti ai loro obiettivi se coloro responsabili della rete non hanno implementato misure sufficienti. In sostanza, questa fase è il passo successivo dopo che gli attaccanti hanno consegnato e messo in opera i loro malware o codici dannosi. In questa fase, cercano di sfruttare le vulnerabilità del sistema per ottenere un controllo più profondo e persistente sulla rete o sul dispositivo target.

Command&Control

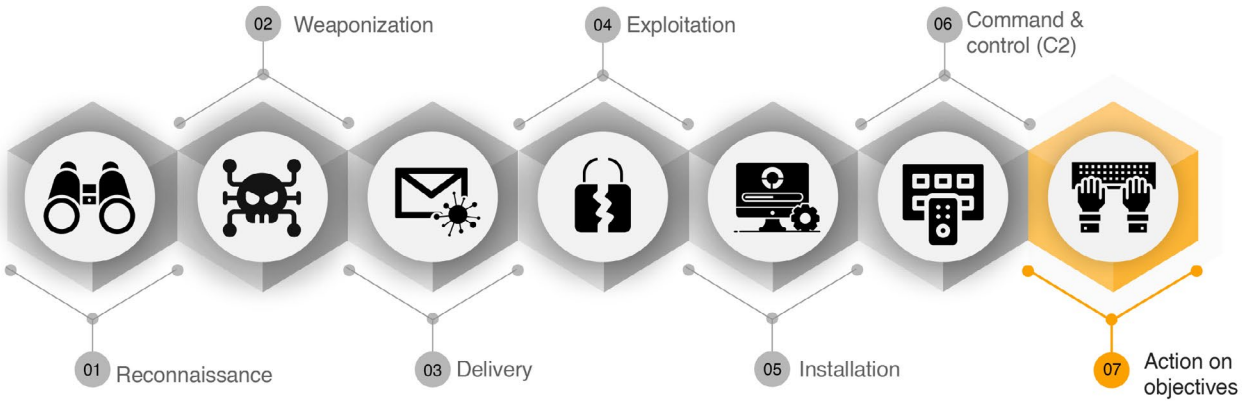
Nel secondo trimestre del 2023, i malware continuano a rappresentare una minaccia per la sicurezza informatica di aziende e individui in tutto il mondo. Nel contesto della Cyber Kill Chain, l'installazione di Malware per la comunicazione con un server remoto si colloca nella fase di "Command&Control".

La fase di Command & Control ("C2") è cruciale per gli attaccanti, poiché consente loro di mantenere il controllo sulle macchine compromesse e di continuare a eseguire operazioni malevole senza essere rilevati. È essenziale che le organizzazioni implementino soluzioni di rilevamento delle minacce avanzate per identificare e bloccare la comunicazione tra i sistemi compromessi e gli attaccanti.

Durante la fase di C2, gli aggressori utilizzano una varietà di tecniche e strumenti per mantenere il controllo sul sistema compromesso e interagire con esso. Questo coinvolge l'uso di malware sofisticati e framework di Command & Control.



Actions On Objectives



Come riportato in partenza. Nell'H2 2023 si è registrato un significativo aumento delle vittime colpite da attacchi ransomware, con un totale di oltre 2600 incidenti segnalati in tutto il globo. Si tratta dell'ultima fase della Cyber Kill Chain, conosciuta come "Actions on Objectives", che rappresenta il momento culminante di un attacco. Una volta infiltratosi con successo nel sistema bersaglio, l'attaccante è in grado di agire per raggiungere il suo obiettivo iniziale. Le azioni intraprese in questa fase possono assumere molteplici forme, che vanno dall'estrapolazione di dati sensibili fino alla completa distruzione degli stessi.

Le vittime del ransomware nel secondo trimestre provengono da un'ampia gamma di paesi e isole, raggiungendo un totale di 94 paesi coinvolti. Questo dimostra come il ransomware sia un problema globale che non conosce confini geografici: le organizzazioni e gli individui di tutto il mondo sono stati bersaglio di attacchi, mettendo a rischio la sicurezza dei dati e la continuità operativa.

Il commento del CEO, Pierguido Iezzi

Oggi ci troviamo di fronte a una realtà digitale che si evolve a una velocità impressionante, con il secondo semestre del 2023 che ha portato un aumento significativo degli attacchi informatici in tutto il mondo. I numeri parlano chiaro: **2.616 incidenti** di ransomware hanno coinvolto **94 paesi**, con un incremento del 11.4% rispetto al primo semestre. L'Italia, purtroppo, non è rimasta immune, registrando un **aumento del 44.1%** degli incidenti di ransomware. Questi attacchi, orchestrati da gang ransomware, hanno colpito 88 aziende nel nostro paese, creando significative interruzioni in diversi settori.

Insomma, il panorama del cyber crime ha continuato il suo percorso di continua evoluzione nel 2023, dimostrando un approccio più efficiente e aggressivo. I Criminal hacker continuano a innovare e adattarsi ai cambiamenti normativi e alle azioni delle forze dell'ordine. Nonostante casi come il sequestro di Hive e la disruption di BlackCat, il ransomware ha visto comunque una crescita significativa.

Il fenomeno, come dimostrano i dati del report, sta evolvendo verso una dimensione sempre più "commodity". Questo cambiamento può essere attribuito alla crescente democratizzazione del cyber crimine, resa possibile dall'accesso semplificato a nuovi codici e competenze verticali. Tale democratizzazione si traduce anche in una maggiore accessibilità, permettendo a una varietà di attori, anche meno esperti, di sfruttare queste risorse cyber criminali.

Questi numeri riflettono quindi una minaccia sempre più sofisticata e diversificata. **CobaltStrike** e **Metasploit** dominano il panorama dei malware di command and control, mentre il phishing continua a essere un problema pervasivo, con **oltre 448.000 attacchi globali.**

In questa era digitale, la sicurezza informatica è diventata una priorità ineludibile, le aziende devono rafforzare le loro misure di sicurezza, devono rimanere vigili. L'Italia ha già rafforzato la sua resilienza cibernetica attraverso l'istituzione dell'Agenzia per la Cybersicurezza Nazionale (ACN) e del Nucleo per la CyberSicurezza (NCS), dimostrando un impegno tangibile nel fronteggiare le minacce emergenti.

Ma il loro sforzo non può prescindere dalla collaborazione tra settore privato, istituzioni accademiche e governo; essenziale per affrontare questa sfida. Un concetto ripreso e sottolinato, in Italia, dallo stesso Ministro della Difesa Guido Crosetto; che ha già sottolinato l'importanza della collaborazione tra enti pubblici e privati e la necessità di un approccio sistematico per affrontare le minacce.

Dobbiamo considerare la sicurezza informatica non solo come una questione tecnologica, ma come una necessità imperativa per proteggere il nostro patrimonio, l'economia e, soprattutto, i cittadini. Solo attraverso una strategia di difesa predittiva, preventiva e proattiva possiamo affrontare le continue minacce emergenti e preservare la nostra sicurezza digitale. In particolare oggi, un'epoca in cui la minaccia cibernetica è diventata ancor più evidente in relazione agli attuali accadimenti internazionali.

Come difendersi dal ransomware:
Il cyber security framework

L'approccio migliore per aumentare la resilienza del perimetro passa per i tre pilastri della Cyber Security moderna. Per questo motivo vanno consolidati e rispettati i tre canoni di:

- **Sicurezza Predittiva**
- **Sicurezza Preventiva**
- **Sicurezza Proattiva**

Sicurezza Predittiva

1. Identifica le minacce Cyber fuori dal perimetro aziendale operando a livello di web, Darkweb e Deepweb.
2. Ricerca eventuali minacce emergenti.
3. Effettua attività di Early Warning.
4. Fornisce le evidenze alla sicurezza preventiva.
5. Indica le aree di attenzione alla sicurezza proattiva.

Sicurezza Proattiva

1. Identifica le minacce cyber che operano nel perimetro aziendale.
2. Contrasta e blocca gli attacchi informatici
3. Gestisce i Cyber Incidents.
4. Fornisce le evidenze alla sicurezza preventiva. Indica le aree di investigazione alla sicurezza predittiva.

Sicurezza Preventiva

1. Verifica e misura il rischio Cyber.
2. Definisce i piani di Remediation.Indica il rischio esposto al Layer di sicurezza proattiva.
3. Fornisce le aree di investigazione alla sicurezza predittiva.

Action Plan

In linea con le best practice descritte nel Cyber Security Framwork è consigliato implementare un action plan di Cyber Secuirty basato sui seguenti Step:

Sicurezza Predittiva:

Domain Threat Intelligence: La Domain Threat Intelligence ricerca le informazioni pubbliche e semipubbliche relative alle vulnerabilità del dominio, sottodomini ed email compromesse. Il servizio non effettua alcun test sul target. Opera unicamente sulle informazioni disponibili sul web, Darkweb e deepweb. Raccoglie, analizza e clusterizza le informazioni disponibili a livello OSINT (Open Source Intelligence) e Closint (Close Source Intelligence) presenti su database, forum, chat, newsgroup.
Nello specifico, in base al dominio target di analisi, identifica:

- Potenziali vulnerabilità
- Dettagli delle vulnerabilità in termini di CVE, impatti e severity
- Impatti GDPR (CIA)
- Numero dei sottodomini
- Numero potenziali e-mail compromesse (vengono solo conteggiate e non raccolte o trattate)
- Numero delle source delle e-mail compromesse
- Typosquatting

Cyber Threat Intelligence: È il servizio evoluto di Threat Intelligence di Swascan. Effettua una attività di ricerca, analisi e raccolta delle informazioni presenti a livello web, Darkweb e Deepweb relativamente al dominio/target di analisi.
Nello specifico:

- Data Leaks: credenziali/source/data
- Identifica Forum/Chat ...
- Botnet relative a dispositive di clienti, fornitori e dipendenti
- Botnet con credenziali e relative url di login page
- Typosquatting/Phishing
- Surface
- Top Manager Analysis

Sicurezza Preventiva:

Vulnerability Assessment: Esegue la scansione di siti e applicazioni web per identificare e analizzare i modo proattivo le vulnerabilità di sicurezza.

Penetration Test: Le attività di Penetration Test sono svolte da Penetration Tester certificati e in linea con gli standard internazionali OWASP, PTES e OSSTMM.

Phishing/Smishing attack Simulation: Permette alle aziende di prevenire i danni dovuti ad attacchi di phishing/smishing attraverso delle vere e proprie simulazioni di attacco. È infatti possibile, attraverso un'interfaccia web inviare vere e proprie campagne di phishing/ smishing simulate che generano delle insostituibili occasioni di apprendimento per i dipendenti. Quest'ultimi, infatti, grazie a tali attacchi simulati riusciranno, in futuro, ad individuare una vera e-mail di phishing o un messaggio di smishing e ad evitarla. Un'insostituibile attività di formazione e awareness dei tuoi dipendenti tramite vere e proprie simulazioni di attacco phishing/smishing .

Awareness (Cyber Academy): Corsi di formazione dedicati di Cybersecurity in aula o tramite Webinar. Attività di Awareness per il personale tecnico, per i dipendenti e per i Top Manager.

Sicurezza Proattiva:

SOC: La progettazione, la messa in esercizio e il mantenimento di un Security Operation Center può essere costoso e complesso. Il servizio **SOC as a Service** Swascan è la soluzione più efficace, efficiente, coerente e sostenibile per i contesti aziendali. Il Soc as a service con il suo servizio di Monitoring & Early Warning permette di **identificare**, **rilevare, analizzare** e segnalare gli attacchi cyber prima che possano trasformarsi in una minaccia concreta per l'azienda.

Un team dedicato nell'attività di **Monitoring & Early Warning** reattivo delle minacce informatiche sulle reti locali, ambienti cloud, applicazioni ed endpoint aziendali. Il nostro team di Security Analyst monitora i dati e le risorse ovunque risiedano all'interno dell'azienda. Indipendentemente dal fatto che le risorse siano archiviate nel cloud, in locale o in entrambi. L'attività di monitoring e segnalazione permette di agire solo quando viene identificata una minaccia reale.

Incident Response Team: Il Cyber Incident Response Team by Swascan è un servizio di Pronto Intervento Cyber h24 con obiettivo e scopo di supportare le aziende nell'attività di risposta e gestione degli incidenti di sicurezza informatica e attacchi Ransomware.

In linea con lo standard internazionale NIST SP 800-61rev2 Computer Security Incident Handling Guide, a seguito di un incidente informatico l' IRT di Swascan ha l'obiettivo di:

- Contenimento dei possibili danni
- Determinare i possibili danni e impatti
- Garantire una risposta efficace ed efficiente
- Supportare il ripristino della Business Continuity
- Fornire indicazioni e suggerimenti per prevenire il verificarsi di incidenti futuri

Analysis by:

Riccardo Michetti
Riccardo D'Ambrosio
Martina Fonzo

Technical Contributors:

Soc Team Swascan

Editing & Graphics:

Federico Giberti
Melissa Keysomi

Contact Info

Milano
+39 0278620700
www.swascan.com
info@swascan.com
Via Fabio Filzi, 2b, 20063, Cernusco sul Naviglio, MI