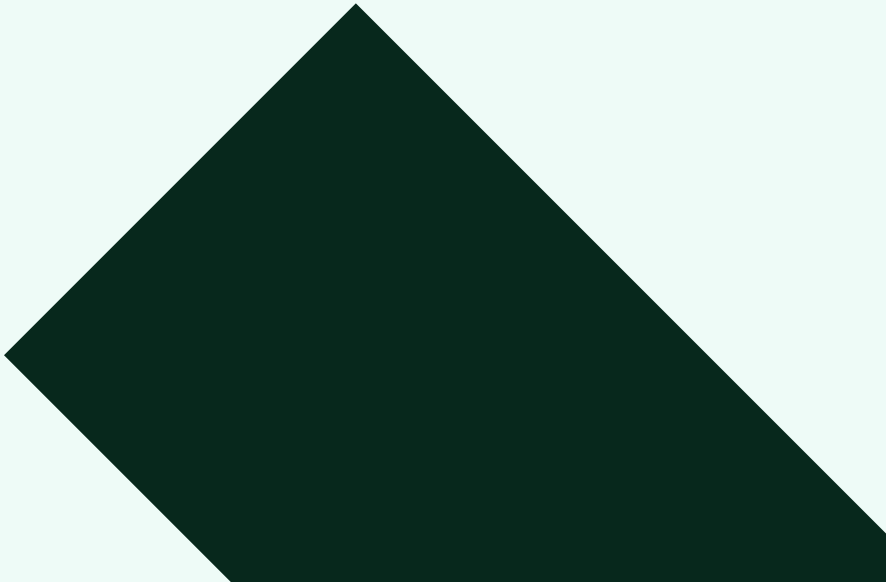
WITH secure

Cyber Threat Landscape

European Mid Market 2025



Indice

Prefazione

“Il passaggio da un anno solare all’altro rappresenta un traguardo relativamente arbitrario quando si considera lo sviluppo delle minacce informatiche che:
a) sono in fase di sviluppo attivo ed evoluzione da diversi anni, e
b) reagiscono agli eventi e alle attività intraprese da noi, in quanto industria, team di difesa (blue teams) e agenzie governative.

Pertanto, lo scopo di questo rapporto non è quello di offrire una serie di previsioni su come una minaccia potrebbe concretizzarsi nel 2025, ma piuttosto di articolare la natura della minaccia, prevedere quali saranno i principali campi di battaglia nel cyberspazio e mettere in luce dove si manifesteranno, nel breve termine (un periodo di 12 mesi), i continui progressi ed evoluzioni della minaccia.

Questa valutazione, contestualizzata nel mercato europeo di fascia media, è stata elaborata sulla base di ciò che osserviamo nel team di Threat Intelligence di WithSecure e fornirà ai soggetti interessati informazioni utili a supportare le operazioni di contrasto alle minacce, contribuendo così alla missione di WithSecure di costruire e mantenere fiducia digitale, sicurezza e parità.”

Tim West,
Dittore, Threat Intelligence & Outreach

Executive Summary

Il 2024 ha presentato uno scenario geopolitico, tecnologico ed economico turbolento, con un impatto significativo sull'ecosistema cyber e sul panorama delle minacce. Questo rapporto si propone di delineare le previsioni relative al crimine informatico cyber-dependent e alle minacce di tipo Computer Network Attack/Exploitation (CNA/E) che interesseranno il mercato medio europeo nel 2025.

Il grafico seguente illustra lo stato delle minacce per l'industria del mid-market in Europa. La minaccia principale proverrà da attori mossi da motivazioni economiche, come i gruppi ransomware. Tuttavia, anche attori specializzati in Business Email Compromise (BEC), hacktivisti, broker di accesso iniziale (IAB) e, in misura minore, attori APT russi, manifesteranno un'intenzione significativa nei confronti del mercato medio europeo.

Si tratta di una valutazione generale, che analizza le minacce sistemiche rivolte al mid-market europeo nel suo complesso, e non si applica in modo diretto a singole organizzazioni. Gli attori sponsorizzati da stati (APT) ricevono una quantità sproporzionata di attenzione mediatica nel campo della cybersicurezza, ma ciò non riflette la reale minaccia per la maggior parte delle organizzazioni operanti nel mid-market europeo.

La minaccia viene calcolata come funzione di Capacità × Intenzione, dove l'intenzione è definita come lo sforzo che un attore è disposto a impiegare per colpire un'organizzazione arbitraria del mid-market europeo.

L'impatto organizzativo varierà a seconda degli obiettivi dell'attore (ad esempio, gli attacchi distruttivi generano un impatto maggiore rispetto agli attacchi DDoS). Pertanto, la posizione nel grafico non deve essere interpretata come una rappresentazione diretta del rischio che ogni tipo di attore comporta per il mid-market europeo.

Campi di battaglia chiave

La tabella seguente rappresenta il cambiamento di scenario nei campi di battaglia della cybersicurezza dal 2024 al 2025. Gli elementi evidenziati in grassetto indicano le aree che continueranno a essere cruciali nel 2025, indipendentemente dalla direzione del cambiamento.

Battlegrounds	Trend
Windows	↓
Cloud	↑
MacOS	↗
Linux	→
Mobile	→
In code	↑
In browser	↗
Security tooling	→
At user (social engineering)	↗
In macro / In document	↓
Identity	↗

Temi chiave 2025

I seguenti aspetti saranno probabilmente i temi centrali per i difensori delle reti durante tutto il 2025.

Adozione del Cloud

Man mano che il Cloud diventa una parte integrante dell'infrastruttura delle reti organizzative, assistiamo a un'evoluzione degli attori delle minacce: da semplici conoscitori del cloud a veri e propri esperti. L'utilizzo di strumenti e funzionalità legittime per scopi illeciti sarà un tema centrale con cui i difensori dovranno confrontarsi nel 2025 – in continuità con quanto già osservato nel 2024.

Abbiamo iniziato a notare l'impiego di servizi cloud noti come nodi negli attacchi, non solo limitatamente all'infrastruttura di comando e controllo (C2). Con la crescente "de-perimetrazione" delle organizzazioni, l'industria degli infostealer ha ricevuto un forte impulso, e il furto di credenziali e materiali di autenticazione continuerà a essere una tendenza chiave.

L'adozione di architetture moderne, soprattutto in un contesto in cui la funzionalità è fluida come nel cloud, rischia di minare anni di formazione comportamentale rivolta agli utenti meno esperti in materia di cybersicurezza. Gli attori delle minacce sfrutteranno sempre più ambienti cloud che cercano di nascondere la loro complessità a utenti ormai abituati ad autenticarsi ripetutamente (e in modo arbitrario) a servizi diversi.

Nuove Tecniche di Social Engineering

Per molti attori, in particolare quelli con profili di targeting flessibili, è più semplice e veloce eludere i sistemi di prevenzione delle intrusioni tramite social engineering piuttosto che attraverso mezzi tecnologici. Il divario tra gli elementi malevoli (ad esempio malware) e la tecnica di contatto iniziale viene colmato proprio dalle tecniche di social engineering.

WithSecure ha osservato un aumento di attacchi innovativi e a più fasi basati su social engineering, estremamente efficaci nella diffusione di malware — e questa crescita probabilmente continuerà nel 2025. È probabile che assisteremo a un ulteriore cambiamento di paradigma: dal "pushing" (spingere un elemento malevolo, come un eseguibile o un link, verso la vittima) al preposizionamento strategico, che induce la vittima — tramite manipolazione sociale — a "tirare" attivamente l'elemento malevolo dall'attaccante.

Inoltre, ci si può aspettare un uso crescente di servizi di messaggistica alternativi come vettori principali per la distribuzione di malspam in arrivo.

Minacce emergenti alla supply chain del software

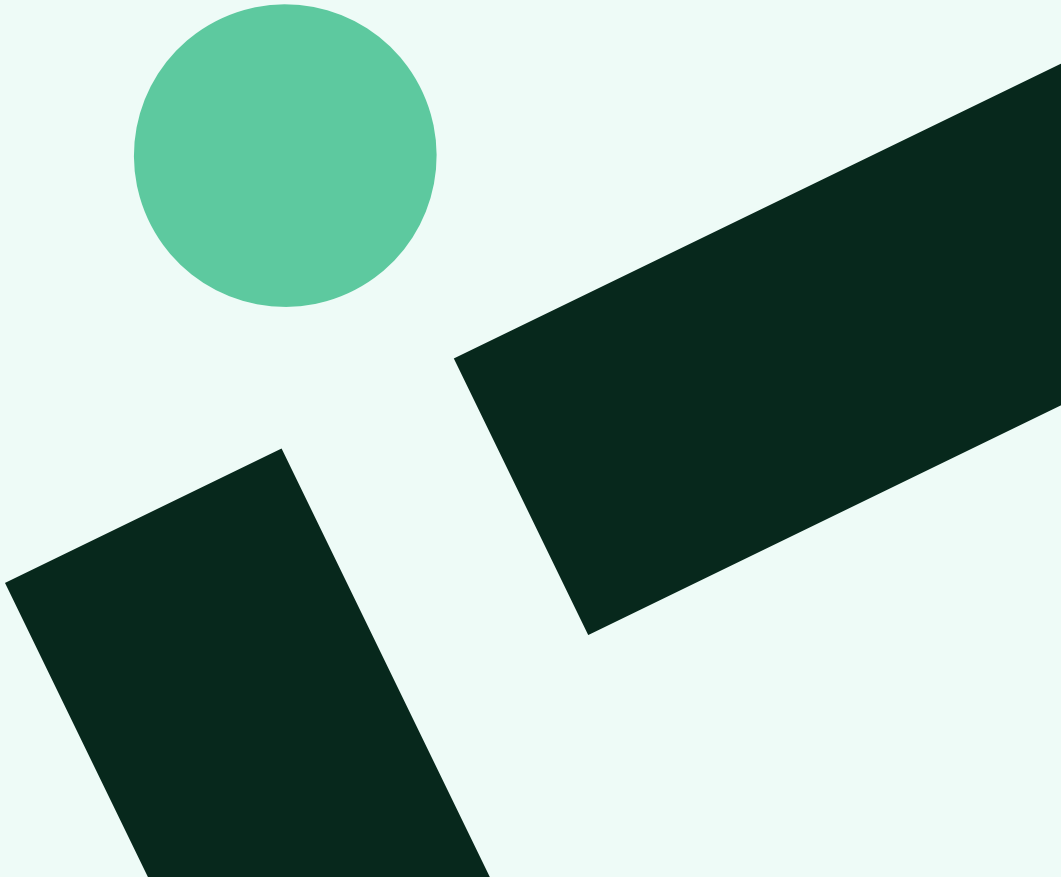
Un numero sempre maggiore di pacchetti software compromessi viene scoperto all'interno di librerie open-source. Questo rappresenta un metodo innovativo per eseguire codice malevolo, in grado di aggirare la whitelisting delle applicazioni e molte scansioni anti-malware.

Tali tecniche vengono utilizzate con crescente frequenza per diffondere infostealer all'interno dei team di sviluppo. Lo stesso vale per i plugin malevoli dei browser: i browser, infatti, memorizzano spesso materiali di autenticazione e stanno assumendo sempre più il ruolo di veri e propri ambienti di lavoro nei contesti SaaS.

Attacchi all'identità più avanzati

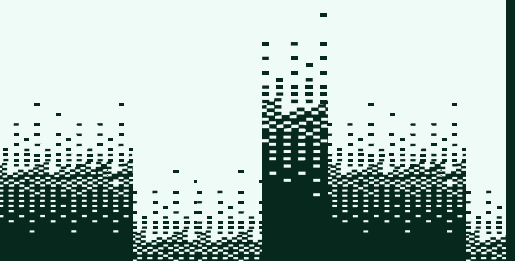
Con l'aumento continuo dell'adozione dei servizi Cloud, gli attacchi malware-less e focalizzati sull'identità daranno nuova linfa alle campagne di social engineering, utilizzando tecniche sempre più innovative e sofisticate. Le tecniche Attacker in The Middle (AiTM) aumenteranno quasi certamente in proporzione all'adozione dei servizi Cloud e dell'autenticazione a più fattori (MFA).

Il malware infostealer rimarrà estremamente attivo e versatile, in grado di rubare materiali di autenticazione da una vasta gamma di fonti.



Sfruttamento dei servizi edge / infrastruttura

Lo sfruttamento dei servizi edge e dell'infrastruttura sarà un tema comune nel 2025. I fornitori sembrano trovarsi in difficoltà sia con il processo di rimedio delle vulnerabilità che con il ritmo operativo intensivo. Le vulnerabilità sono spesso sia gravi che rudimentali, il che significa che una vasta gamma di attori ha la capacità di sfruttarle con effetti devastanti. Questi problemi sono spesso aggravati dall'incapacità di implementare strumenti di sicurezza proprietari su un'infrastruttura intrinsecamente vulnerabile.



Artificial Intelligence (AI) penetration

Sebbene esistano ancora alcune limitazioni fondamentali nelle capacità dell'AI generalmente disponibile, essa rimane uno strumento estremamente utile per attori malintenzionati.

È probabile che l'Intelligenza Artificiale consenta un aumento del numero di attori in grado di raggiungere uno "standard minimo sostenibile" per causare danni nel cyberspazio. Un incremento sia del numero di attori capaci sia dell'efficienza dei gruppi di intrusione già esistenti aumenterà quasi certamente il livello di minaccia affrontato da una tipica organizzazione europea di medie dimensioni.

Nel suo stato attuale, l'Intelligenza Artificiale probabilmente non rivoluzionerà la sofisticazione dei gruppi di intrusione più avanzati, ma offrirà un notevole incremento dell'efficienza (ovvero, aumenterà il numero di vulnerabilità che un esperto cacciatore di bug è in grado di individuare), oltre a fornire un grande impulso alla produttività delle tecniche di ingegneria sociale.

Attualmente, l'AI probabilmente offre opportunità uguali o maggiori anche per i difensori delle reti, che avranno un migliore accesso alle capacità difensive avanzate dell'AI. Tuttavia, questo equilibrio potrebbe facilmente essere compromesso se venissero prese decisioni irresponsabili sull'uso dell'AI da parte dei leader della tecnologia informatica.

L'AI amplificherà sia i rischi di sicurezza noti che quelli sconosciuti.

Key Drivers

I seguenti sono i principali fattori identificati in questo rapporto che quasi certamente influenzeranno il panorama delle minacce e altereranno la valutazione contenuta nel rapporto, ma che sono troppo imprevedibili per essere valutati con sufficiente certezza:

Eventi Geopolitici

Dopo una forte ondata anti-incumbent nelle elezioni nazionali, il 2025 probabilmente vedrà un ambiente geopolitico sempre più frammentato. La seguente lista di possibili eventi geopolitici che modelleranno l'ecosistema cyber potrebbe includere, ma non limitarsi a:

Le conseguenze del regime in arrivo negli Stati Uniti, in particolare le politiche commerciali e gli impegni relativi agli aiuti esteri verso la NATO e l'Ucraina.

Come si svilupperà il conflitto tra Israele e Hamas e gli eventi con l'Iran.

Come procederà la rivendicazione della Cina su Taiwan.

Ragionamento dell'Intelligenza Artificiale

L'Intelligenza Artificiale è in rapida evoluzione e i modelli pubblici vengono frequentemente aggiornati con nuove funzionalità. Queste funzionalità sono spesso relativamente cosmetiche, migliorando l'efficienza e le prestazioni, ma rimanendo all'interno dello stesso tetto di capacità dei modelli precedenti. Un vero progresso nell'AI Agente potrebbe avere un impatto molto più ampio di quanto attualmente valutato in questo rapporto.

Regolamentazione dell'Intelligenza Artificiale

Sebbene esistano diversi modi per "sbloccare" i modelli linguistici di grandi dimensioni, i team di Trust and Security dei fornitori commerciali di AI saranno fondamentali nel tentativo di combattere l'abuso delle capacità generiche dell'AI. La regolamentazione sarà fondamentale per gestire positivamente i modi in cui l'AI influenzerà l'economia e la società nel 2025.

Introduzione

Scope

Questo rapporto sarà preparato, quando possibile, attraverso la lente del mercato medio europeo. Il cyberspazio non rispetta sempre i confini geografici e spesso dobbiamo fare riferimento a incidenti ed eventi che esulano da un profilo geografico per fare una valutazione adeguata.

Nel corso di questo rapporto, la minaccia viene calcolata come una funzione di Capacità x Intento che un'entità può esercitare verso le organizzazioni all'interno del mercato medio europeo. I lettori devono notare che, mentre le organizzazioni possono essere targetizzate (deliberatamente o incidentalmente) a causa della geografia in cui si trovano, raramente sono targetizzate per la loro dimensione o posizione all'interno del mercato. La valutazione dell'intento è più semplice quando si considerano attori minacciosi opportunistici e finanziariamente motivati, ma è difficile generalizzare una minaccia quando si trattano organizzazioni di nicchia o specializzate che rientrano nel mercato medio europeo. È importante che queste organizzazioni siano in grado di calcolare il proprio modello di minaccia in base al loro profilo unico.

Questo rapporto si concentrerà sul "crimine dipendente dal cyberspazio" e non sul "crimine abilitato dal cyberspazio". Il crimine abilitato dal cyberspazio definisce dove gli obiettivi criminali più tradizionali vengono raggiunti utilizzando tecniche che possono essere utilizzate anche in operazioni offensive nel cyberspazio. Ad esempio, stabilire un dominio simile per ingannare un individuo e rubare informazioni sulla carta di credito. Tale attività è fuori dall'ambito di questo rapporto. Questo rapporto si concentrerà sul crimine informatico inteso come "Computer Network Exploitation" (CNE) o "Computer Network Attacks" (CNA), che mirano a compromettere la riservatezza, l'integrità o la disponibilità delle informazioni e dei sistemi informatici. Frodi, truffe e sfruttamento sessuale minorile (CSE), pur essendo illegali e spesso verificandosi nel cyberspazio, sono fuori dall'ambito di questo rapporto.

Le operazioni informative e la disinformazione sono forme di social engineering di massa. Questi temi non saranno trattati in questo rapporto, poiché le minacce in questo ambito non rappresentano un rischio per la sicurezza informatica delle organizzazioni.

Questo rapporto sarà strutturato in tre sezioni principali:

Campi di battaglia chiave – La tecnologia e le TTP (Tattiche, Tecniche e Procedure) degli attaccanti sono in continua evoluzione, in base all'adozione di diverse architetture e all'utilizzo di vettori di attacco di tendenza e di successo. Questa sezione del rapporto fornirà una previsione dello stato delle minacce agli ambienti e dei vettori di attacco più in voga che verranno impiegati nel 2025.

Nel suo stato attuale, l'Intelligenza Artificiale probabilmente non rivoluzionerà la sofisticazione dei gruppi di intrusione più avanzati, ma offrirà un notevole incremento dell'efficienza (ovvero, aumenterà il numero di vulnerabilità che un esperto cacciatore di bug è in grado di individuare), oltre a fornire un grande impulso alla produttività delle tecniche di ingegneria sociale.

Driver chiave - Il panorama delle minacce è in evoluzione ed è guidato e influenzato da una miriade di fattori esterni, come le tecnologie emergenti o gli eventi geopolitici. Questi fattori sono spesso quasi impossibili da prevedere, e pertanto è inappropriato cercare di prescrivere tutti i possibili scenari di minaccia derivanti da essi. Questo rapporto, invece, evidenzierà e descriverà questi driver chiave che influenzeranno il panorama delle minacce nel 2025.

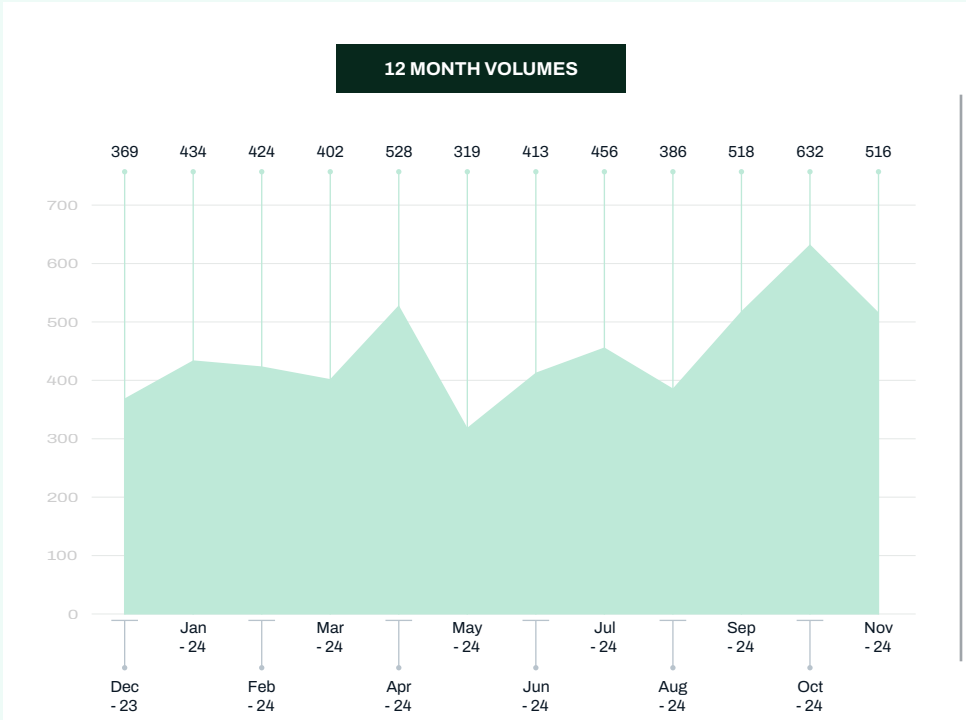
Lo scopo di questo rapporto è prevedere le minacce fino al 2025, e mentre queste verranno menzionate, il rapporto non rielaborerà i vettori che possono essere considerati come "status-quo". Al contrario, i dettagli saranno riservati a dove la minaccia cambierà e si evolverà nel 2025.

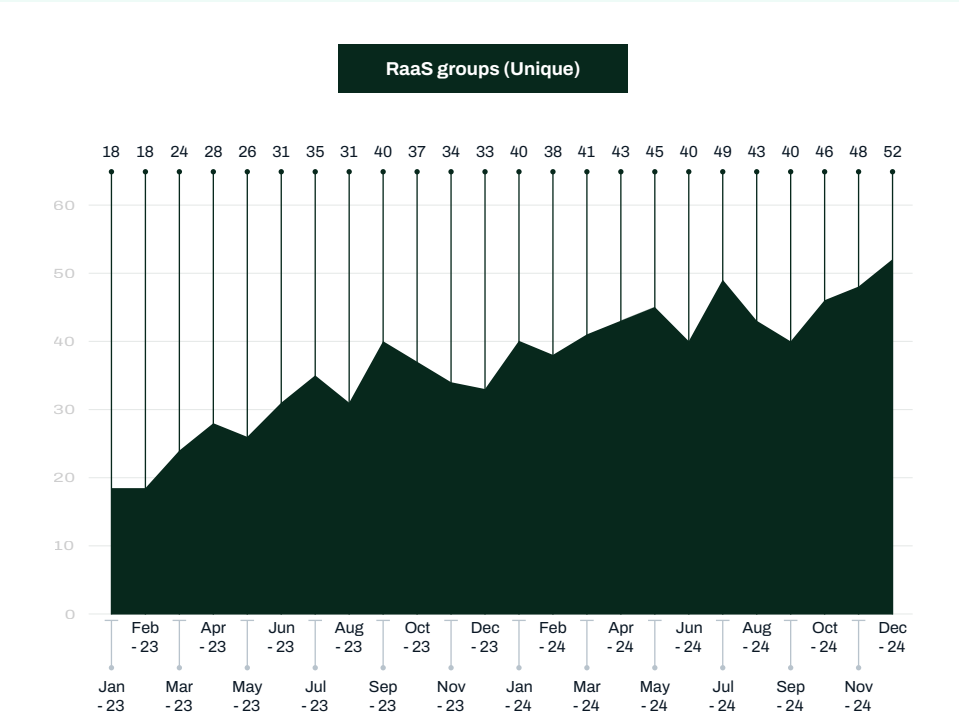
Minacce tematiche 2025

Crimine finanziario

Ransomware

Durante il 2024, il panorama del ransomware è stato sconvolto da una serie di eventi chiave. Questi eventi hanno ridotto il tasso di attacchi ransomware durante il terzo trimestre (Q3) del 2024, tuttavia l'ecosistema del ransomware ha mostrato segni di recupero nel quarto trimestre (Q4). I volumi di attacchi di ottobre, novembre e dicembre hanno presentato numeri molto più alti rispetto a quanto visto precedentemente durante il 2024, e il numero di marchi di ransomware unici e attivi è aumentato verso la fine del 2024.

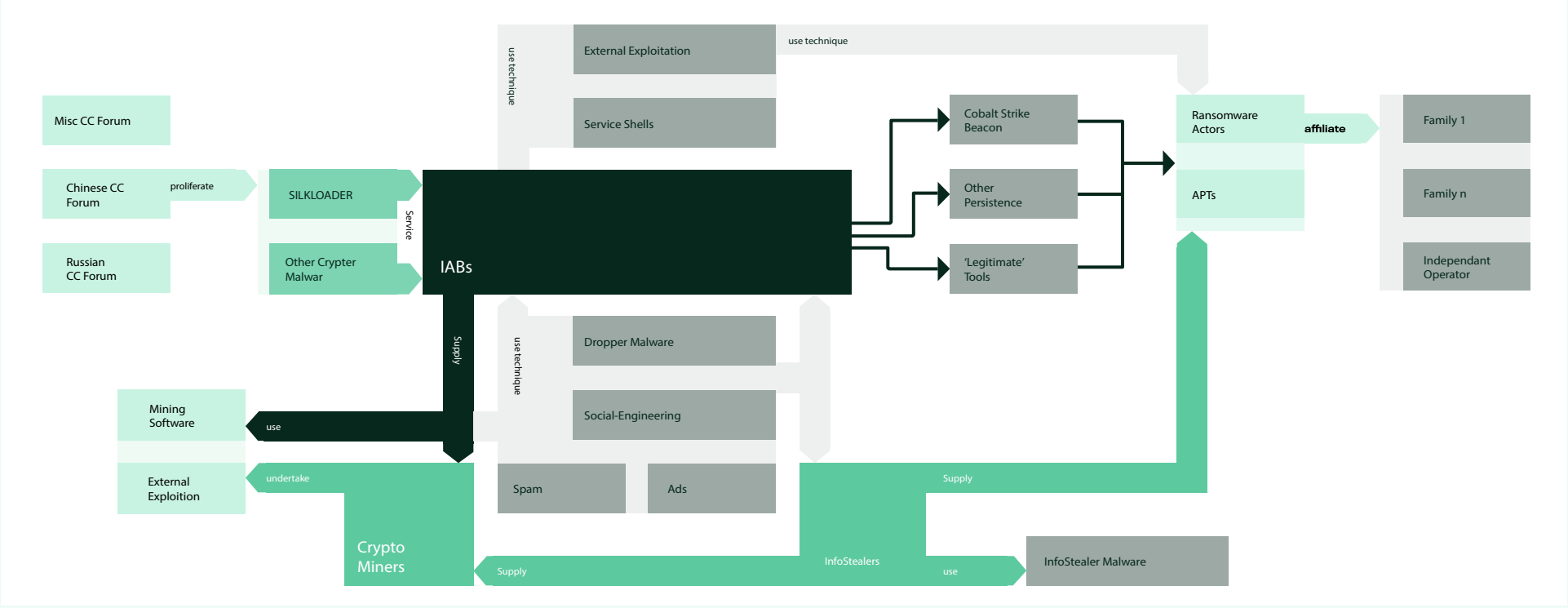




Architettura di un collettivo RaaS.

La comprensione di WithSecure sull'architettura di un Ransomware as a Service (RaaS) non cambierà significativamente nel 2025. L'architettura del crimine informatico sarà principalmente definita da un'industria del tipo "as-a-service". Gli sforzi delle forze dell'ordine nel 2024, e in previsione nel 2025, potrebbero spingere alcuni attori ad operare in modo da oscurare l'impatto completo delle loro azioni; per esempio, gli affiliati potrebbero scegliere di utilizzare diverse famiglie di ransomware. Mentre ci sono alcuni attori del ransomware che operano una catena di attacco completa (senza usare i servizi) sotto un marchio di ransomware coerente, questo probabilmente rimarrà meno comune rispetto agli affiliati del ransomware che utilizzano pesantemente il modello 'as-a-service' definito in questa sezione.

È altamente probabile che il numero di gruppi di ransomware attivi continui a salire nel 2025. Questo è probabilmente il risultato di due fattori principali: la disponibilità di codice di "costruttori" di ransomware trapelato o open-source, e il desiderio di offuscare l'importanza di qualsiasi affiliato. È probabile che molti degli affiliati di ransomware più produttivi continueranno o espanderanno il loro lavoro su più marchi di ransomware differenti. Il seguente diagramma dettaglia l'architettura "as-a-service" degli attacchi di crimine informatico. Sebbene sia stato sviluppato verso la fine del 2023, sarà quasi certamente ancora rilevante nel 2025.



Broker di Accesso Iniziale.

I Broker di Accesso Iniziale (IAB) sono al centro del modello as-a-service. Sono molto difficili da attribuire e rappresentano un fattore chiave nell'aumento significativo della produttività del ransomware.

Molti dei broker di accesso iniziale più capaci hanno industrializzato l'accesso iniziale attraverso vulnerabilità e repository di identità rubate. Gli IAB investiranno risorse per compromettere le aziende del mercato medio europeo, indipendentemente dal loro profilo (settore, dimensione, ecc.), poiché questi fattori non influenzano il loro modello di business.

WithSecure ha osservato gli IAB operare sia con attacchi APT sponsorizzati dallo stato che con operatori di ransomware.

Nazionalità

Europa dell'Est e Russia sono frequentemente citate come la fonte della maggior parte degli attacchi ransomware. Questa attribuzione è spesso dovuta alle barriere di esecuzione presenti nei binari del ransomware, che impediscono la detonazione se vengono eseguiti su computer con caratteri cirillici, e alla presenza abbondante di forum di cybercriminalità in lingua russa. Questo è ancora comune, anche se probabilmente meno frequente come impostazione predefinita. Le operazioni ransomware vengono lanciate da tutto il mondo e molti affiliati operano in Europa e Nord America.

Nel 2024, ci sono stati esempi di affiliati arrestati negli Stati Uniti e in Europa, e ci sono anche gruppi ransomware che operano principalmente da paesi che non hanno un trattato di estradizione con gli Stati Uniti e l'Europa. Ad esempio, RA World (visto per la prima volta nell'estate del 2023) è un gruppo ransomware che crediamo si sovrapponga con DEV-0401 / EMPORER DRAGONFLY, un set di intrusione domiciliato in Cina. WithSecure ha anche osservato il ransomware 'Phalcon', altamente probabile che sia operato da attori iraniani. La Corea del Nord (DPRK) è una chiara eccezione quando si considera l'evento di CNE/CNA (Computer Network Exploitation / Attack) sponsorizzato dallo stato, poiché i loro set di intrusione operano anche con un mandato di generazione di reddito. Ci sono esempi di famiglie ransomware direttamente sviluppate dalla DPRK; tuttavia, questi non sono stati osservati da molto tempo. È molto più probabile che gli attori che operano dalla DPRK stiano utilizzando modelli consolidati di ransomware-as-a-service per portare avanti i loro attacchi.

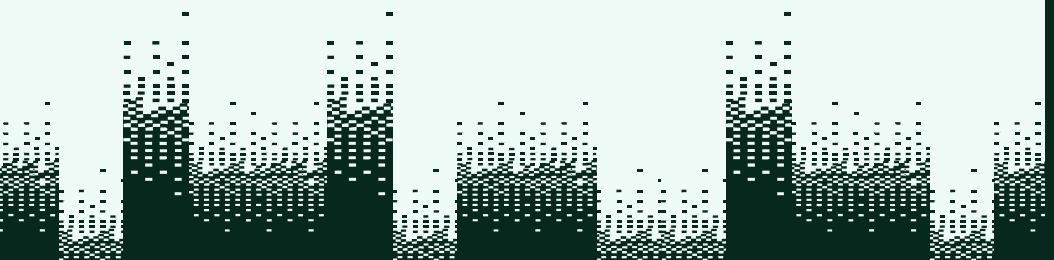
WithSecure Threat Intelligence ha osservato una sovrapposizione tra le infrastrutture utilizzate in intrusioni orchestrate dalla DPRK e quelle di affiliati ransomware più 'tradizionali'.

C'è quasi certezza che un numero significativo di cacciatori di piccole prede indipendenti non segnalati stia capitalizzando sul codice sorgente ransomware trapelato e su indirizzi e-mail usa e getta per lanciare attacchi senza fare affidamento su infrastrutture di estorsione consolidate.

Impatto delle forze dell'ordine

L'impatto delle forze dell'ordine nel corso del 2024 è stato efficace, almeno temporaneamente, nel ridurre l'efficacia dell'ecosistema ransomware più ampio. È probabile che le agenzie di contrasto cerchino di replicare questo successo anche nel 2025. Pertanto, è possibile che le azioni di contrasto al ransomware proseguano con successo e che le forze dell'ordine continuino a colpire gli affiliati alle reti ransomware. È altamente probabile che tali operazioni abbiano un impatto positivo sul panorama del ransomware; tuttavia, per ottenere un cambiamento duraturo e significativo, è necessario un impegno concertato e multilaterale a livello governativo.

L'Operazione Cronos è stata con ogni probabilità l'azione di contrasto al ransomware più riuscita ed efficace nella storia delle forze dell'ordine, e al momento della stesura del rapporto vi sono segnali che l'industria del ransomware stia cercando di riprendersi dall'impatto subito. Poiché il settore privato, da solo, non possiede il mandato per contrastare in modo fondamentale gli attori del ransomware (potendo in pratica solo reagire agli eventi, senza poter colpire direttamente gli affiliati), è quindi possibile che la situazione peggiori prima che si riesca ad adottare un'azione duratura contro gli attori ransomware che prendono di mira le piccole e medie imprese europee.



Vittimologia

La seguente data è limitata ai gruppi di estorsione multi-punto che stanno operando un sito di fuga di dati che è analizzabile. In questa sezione esamineremo i siti di fuga delle vittime. Questo dataset è probabilmente la migliore e la fonte più consistente che abbiamo per comprendere il panorama, ma i dati raccolti qui non sono infallibili.

Ci sono diverse variabili che influenzano e distorcono questo dataset:

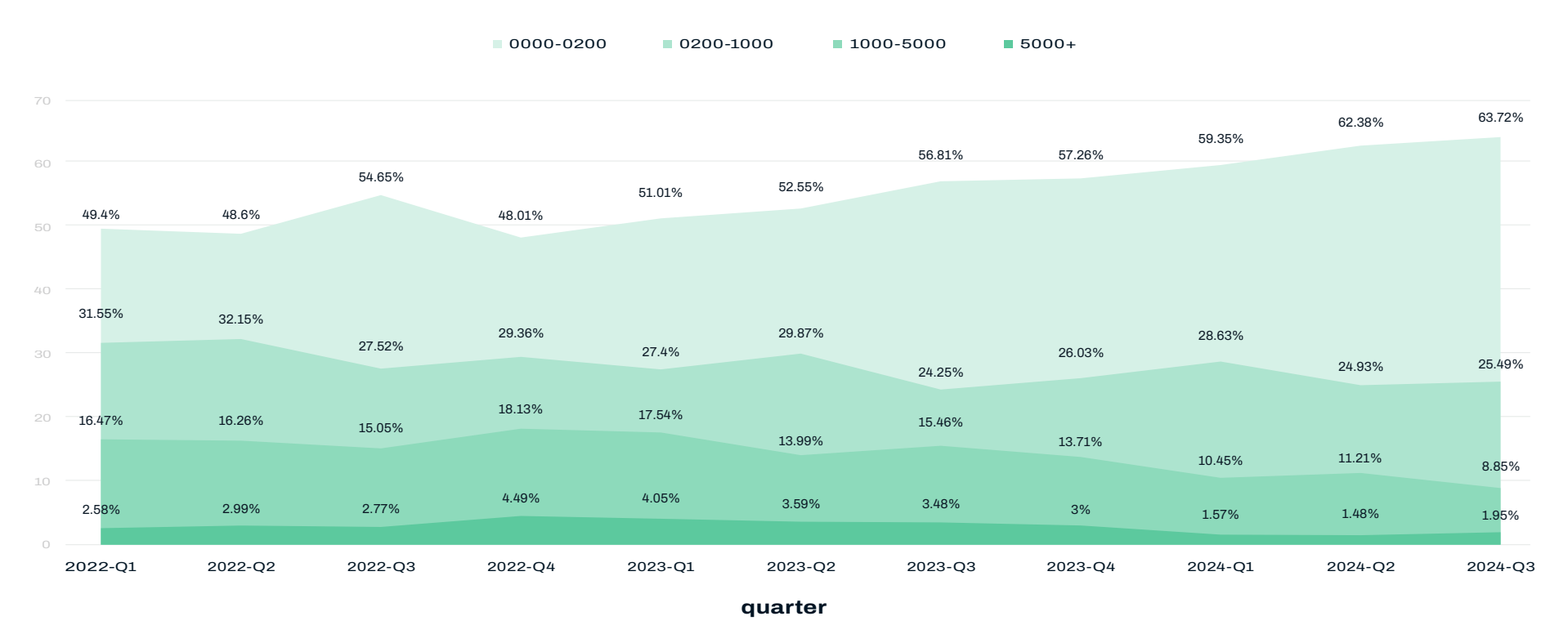
- È guidato dagli attaccanti, e alcuni attaccanti potrebbero essere incentivati a pubblicare dati errati.
- È fluido, e le vittime vengono aggiunte e rimosse frequentemente.
- Il successo dell'estorsione è un altro fattore chiave: se il numero di vittime che pagano aumenta significativamente, i numeri complessivi dei ransomware potrebbero sembrare diminuire.

Detto ciò, possiamo trarre alcune informazioni da questi dati facendo assunzioni sensate – e riconoscendo che i dati non sono perfetti, essi forniscono comunque una buona indicazione del panorama del ransomware.

Le assunzioni a cui l'industria solitamente si attiene sono:

- È fluido, c'è un tasso di pagamento delle vittime relativamente costante di mese in mese,e vengono aggiunte e rimosse frequentemente.
- I post degli attori (malintenzionati) contengono un elemento di verità.

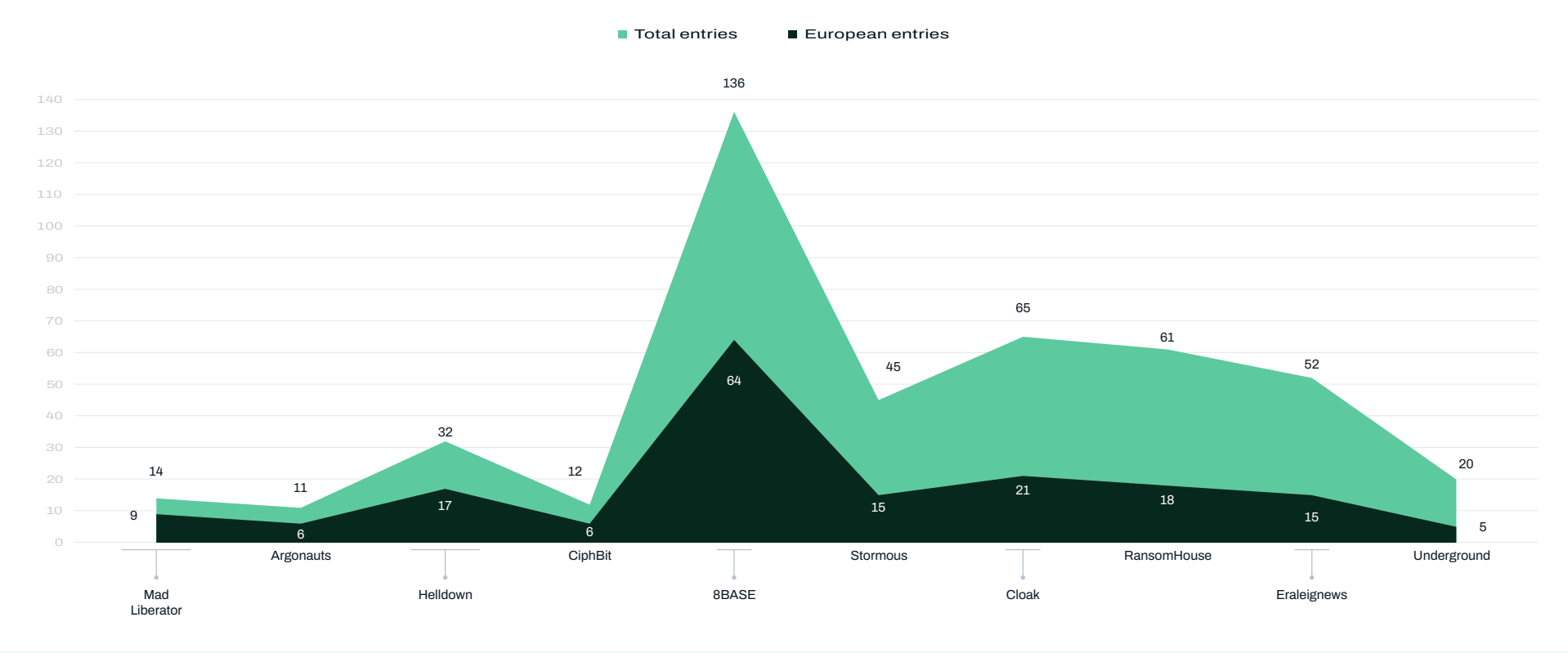
Dal 2022, la proporzione di vittime tra le piccole imprese (0-200 dipendenti) è aumentata ogni anno, passando dal 50% nel 2022, a circa il 62% nel 2024. Mentre la proporzione delle imprese di dimensioni medie (200-1000 dipendenti) è rimasta relativamente costante, le organizzazioni grandi (1.000-5.000 dipendenti) e molto grandi (oltre 5.000 dipendenti) hanno rappresentato una percentuale sempre minore di vittime.



È possibile che la continua riduzione delle vittime grandi e molto grandi nei siti di violazioni da ransomware sia in parte dovuta a una maggiore capacità di soddisfare le richieste degli estorsori. È quasi certo che ciò derivi dalla migliorata capacità di mitigare i rischi informatici, grazie alla possibilità di impiegare team dedicati, prodotti e servizi con assicurazione cyber e processi di recupero dettagliati. Le piccole e medie imprese sono quindi molto più vulnerabili all'impatto del ransomware, un impatto che rappresenta anche un rischio più esistenziale per il mercato medio.

Minacce ransomware in Europa

Il ransomware colpisce gli Stati Uniti in misura molto maggiore rispetto all'Europa. Non si tratta probabilmente di una scelta intenzionale da parte degli attori ransomware (anche se potrebbero esserci alcune eccezioni), ma è più verosimilmente rappresentativo del volume complessivo di infrastrutture connesse che possono essere prese di mira. La media delle vittime europee rispetto a quelle globali si attesta intorno al 21%. La tabella seguente mostra le varianti di ransomware con almeno 10 vittime che prendono di mira in modo sproporzionato le organizzazioni europee.



Questo dimostra che ci sono probabilmente alcune marche di ransomware i cui affiliati operano con una preferenza verso l'Europa. Queste marche non sono le più prolifiche nell'ecosistema del ransomware.

Tariffe di pagamento nel 2025

"WithSecure non partecipa alle negoziazioni o ai pagamenti dei ransomware come parte del suo servizio di risposta agli incidenti, pertanto WithSecure Threat Intelligence deve fare affidamento su segnalazioni di terze parti per fare valutazioni sulle tariffe di pagamento nel 2025."

La minaccia ransomware per le organizzazioni è più compresa nel 2024 e, di conseguenza, le organizzazioni ben strutturate sono sempre più preparate a mitigare i rischi che il ransomware comporta. Con l'aumento dell'adozione delle assicurazioni informatiche e con l'accesso democratizzato agli strumenti di sicurezza protettiva e alle capacità di recupero, è probabile che le tariffe di pagamento diminuiscano nel 2025. Durante il 2024, è probabile che le tariffe di pagamento siano diminuite, anche se esiste una grande disparità nelle segnalazioni riguardo all'entità di questa diminuzione. È probabile che questa discesa continui nel 2025.

Ciò probabilmente non rifletterà una riduzione totale delle somme pagate agli attori di ransomware. I numeri dei pagamenti probabilmente aumenteranno in linea con la frequenza degli attacchi, e la frequenza degli attacchi quasi certamente non diminuirà senza un intervento significativo da parte di organizzazioni competenti e autoritative – questo è improbabile che accada nel 2025.

Tecniche, Tattiche e Procedure (TTPs)

È improbabile che le tattiche, le tecniche e le procedure (TTP) ad alto livello utilizzate dagli attori di ransomware cambieranno significativamente entro il 2025. La tabella seguente mostra le tecniche di accesso iniziale che vedremo gli affiliati ai ransomware implementare nel 2025. Tutte le TTP indicate e come probabilmente si manifesteranno nel 2025 sono esplorate ulteriormente in questo documento:

T1566.002	Phishing: Spearphishing Link
T1133	External Remote Services
T1190	Exploit Public-Facing Application
T1078	Valid Accounts
T1566.002	Spearphishing Link
T1566.001	Spearphishing Attachment
T1566.003	Spearphishing via Service

Consapevolezza dell'infrastruttura Cloud

I ransomware mirano alle architetture in proporzione all'adozione di tali architetture nel settore. I ransomware basati su Windows sono i più comuni, e anche se esistono varianti di ransomware per Mac/Linux, queste sono molto meno comuni. La consapevolezza del cloud e il targeting da parte degli attori di ransomware aumenteranno ampiamente in proporzione all'adozione delle architetture Cloud da parte delle organizzazioni. Questa sezione non fa riferimento all'infrastruttura cloud ospitata on-premise (cioè i servizi ESXi), poiché queste sono da tempo oggetto di attacchi da parte degli attori di ransomware.

Gli attori di ransomware consapevoli del cloud spesso mirano allo storage dei dati nel cloud come mezzo per accedere ai dati sensibili o per impedire il recupero dai dati "offline". I fornitori di servizi cloud hanno in parte mitigato questi rischi, ad esempio definendo periodi di tempo tra le richieste di eliminazione e la rimozione dei dati; tuttavia, in molti casi, l'efficacia di questi controlli dipende dalla configurazione del servizio e potrebbe non essere abilitata per impostazione predefinita. Con l'aumento dell'adozione del cloud che continuerà nel 2025, gli attori di ransomware non avranno altra scelta che continuare lo sviluppo delle TTP (Tattiche, Tecniche e Procedure) specifiche per il cloud. Ci sono sviluppi attivi nelle tecniche di attacco al cloud da parte di ricercatori di sicurezza offensiva, e è probabile che molte di queste tecniche vengano adottate da attori maligni. Detto ciò, gli attacchi nativi al cloud osservati nel mondo reale quasi sempre si basano sull'esploitazione di funzionalità legittime, identità insicure e ambienti mal configurati. Gli attacchi più approfonditi e accademici documentati dai ricercatori di sicurezza sono spesso risolti dai CSP (Cloud Service Providers) prima della loro pubblicazione, ma servono a dimostrare che esiste quasi sicuramente un ampio numero di possibili percorsi di attacco che non sono ancora noti. È probabile che questi vengano presi di mira da attori di minaccia più capaci, sebbene ciò probabilmente coinvolga un sottoinsieme più ridotto di attori di ransomware.

L'igiene informatica nell'architettura cloud è diversa rispetto a quella delle architetture tradizionali on-premise. La gestione delle patch e delle vulnerabilità è esternalizzata per definizione, quindi la gestione della configurazione e della postura è fondamentale. È quasi certo che nel 2025 gli attori di ransomware mireranno alle errate configurazioni, piuttosto che all'esploitazione delle vulnerabilità. Questo probabilmente avrà un impatto sproporzionato sulle organizzazioni di piccole e medie dimensioni, poiché la complessità del cloud è spesso offuscata per l'utente e le PMI di solito non dispongono di team dedicati all'infrastruttura in grado di garantire una gestione robusta della postura.

Nel corso del 2025 è probabile che vedremo ulteriori sviluppi degli strumenti progettati per migliorare l'efficienza degli attori nell'eseguire attività specifiche in determinati ambienti. Questi strumenti saranno quasi certamente focalizzati principalmente sulla distruzione, crittografia e/o esfiltrazione dei dati. Gli attori di ransomware cercheranno quasi certamente di utilizzare servizi legittimi per supportare le varie fasi dei loro attacchi. La funzionalità nativa del cloud progettata per sincronizzare i dati tra tenant [ad esempio, Azure Storage Explorer] è stata osservata negli sforzi di esfiltrazione del ransomware. L'uso illecito di tale funzionalità è quasi sicuramente più difficile da rilevare per gli strumenti di sicurezza, a causa della non disponibilità dei log rilevanti o dell'alto tasso di falsi positivi associato alle rilevazioni euristiche.

Servizi ibridi:

Gli attori di ransomware continueranno a mirare alle applicazioni cloud vulnerabili nel 2025. L'identità sarà probabilmente il principale vettore di attacco per tali servizi, alimentando l'alto volume di campagne di malware infostealing che continueranno nel 2025. I repository di dati di alto valore saranno attivamente mirati, come i servizi di archiviazione nel cloud e i servizi di trasferimento file gestiti. Abbiamo osservato campagne di sfruttamento di massa che mirano specificamente a questi servizi nel corso del 2024 [Snowflake, Cleo], e questi continueranno a essere visti come obiettivi attraenti per gli attori di ransomware nel 2025.

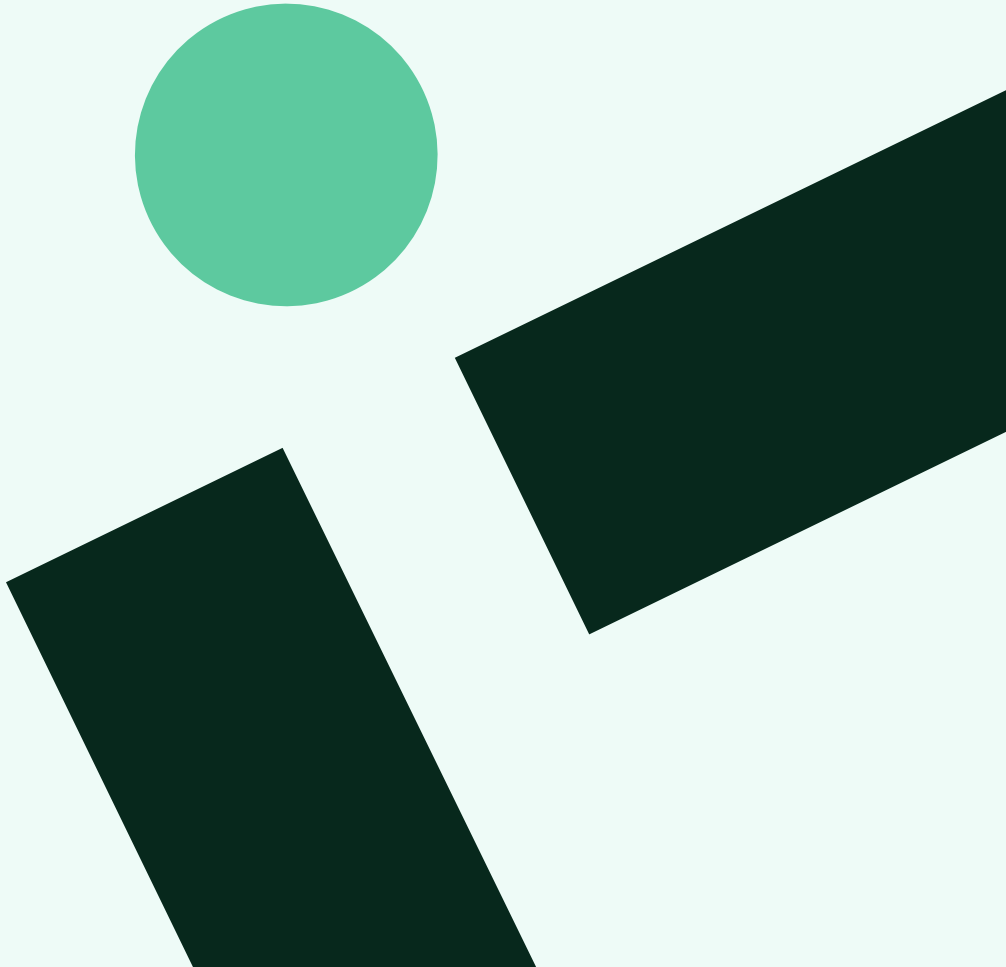
Attacchi "smash and grab"

Molti attori del ransomware stanno perseguendo attacchi più efficienti in termini di costi e tempo. Ciò probabilmente deriva dal fatto che gli attori non prevedono una contrazione nel loro bacino di bersagli, ma riconoscono che le organizzazioni potrebbero essere in grado di riprendersi senza soddisfare le richieste degli attaccanti (ovvero, l'offerta di vittime è elevata, ma il successo dell'estorsione è difficile da prevedere). Invece di investire tempo e sforzi significativi per colpire un'intera rete, una porzione più piccola può essere attaccata a una velocità maggiore.

Questa è una tattica efficace poiché il furto di dati, piuttosto che la loro cifratura, è ora probabilmente una leva di estorsione più attraente per gli attori del ransomware. Attori affiliati ad Akira sono stati osservati alla fine del 2024 mentre lanciavano attacchi ad alta frequenza e velocità contro infrastrutture virtuali on-premises (ESXi). Questo consente inoltre agli attori ransomware di massimizzare il numero di potenziali vittime a partire da un singolo exploit, che potrebbe essere rapidamente corretto dopo il suo primo utilizzo.

Servizi legittimi

Gli attori legati al ransomware utilizzano sempre più frequentemente servizi legittimi lungo l'intero percorso dei loro attacchi. Questo aspetto è trattato in dettaglio nella sezione "Strumenti Legittimi" e non verrà ripetuto qui.



Resource Jacking

Il resource jacking è un vettore di minaccia in gran parte non riportato. Questo è quasi certamente dovuto al fatto che l'impatto degli attacchi di resource jacking è spesso relativamente basso. Il resource jacking viene quasi sempre utilizzato per il mining di criptovalute. Ai fini di questo rapporto, verranno esplorate due diverse modalità di cryptomining: 1)l'utilizzo di risorse cloud rubate, e 2) l'impiego del calcolo distribuito tramite hardware compromesso.

Questa distinzione è importante perché le bollette derivanti dall'uso di risorse cloud possono avere un impatto serio su una piccola organizzazione, mentre molto spesso i cryptominer installati on-premise vengono scoperti solo a seguito di indagini relative a un'altra intrusione.

Cloud resource jacking

La forma più impattante di attacco di resource jacking si verifica quando vengono avviate istanze cloud, tipicamente attraverso la compromissione di un account amministratore cloud o tramite lo sfruttamento di configurazioni di sicurezza cloud inadeguate. Gli attori malevoli creano quindi nuove istanze cloud o potenziano servizi esistenti per distribuire cryptominer.

Questo può tradursi in bollette di calcolo molto elevate da parte del fornitore di servizi cloud (Cloud Service Provider, CSP). È probabile che i CSP siano oggi più consapevoli dei vettori descritti in questa sezione e abbiano implementato maggiori misure di mitigazione. Tuttavia, i CSP sembrano ancora assumersi poche responsabilità per le risorse di calcolo rubate e, di conseguenza, bollette molto elevate possono avere un impatto significativo sulle organizzazioni europee di medie dimensioni.

Hardware Exploitation

Sebbene attori sponsorizzati dallo Stato, gruppi ransomware e hacktivisti vengano spesso segnalati per l'uso di vulnerabilità in dispositivi connessi a Internet, è possibile che in realtà gli attori più prolifici nello sfruttare tali vulnerabilità siano i cryptominer. I team di risposta agli incidenti di WithSecure rilevano spesso malware per cryptomining durante gli interventi.

Esistono numerosi crawler malevoli attivi su Internet in ogni momento, ed è altamente probabile che una buona parte di questi cerchi di distribuire software per il mining di criptovalute. È praticamente certo che i cryptominer cerchino di causare il minimo impatto possibile sulla vittima, al fine di mantenere l'accesso al sistema per il maggior tempo possibile.

Sebbene la minaccia rappresentata da questi operatori (determinata dalla formula capacità × intenzione) sia elevata, il rischio è molto basso a causa del ridotto impatto concreto che causano. È improbabile che questa minaccia subisca variazioni significative nel passaggio dal 2024 al 2025.

APT / Spionaggio

Russia

Le minacce informatiche sponsorizzate dallo Stato russo sono altamente capaci e attive nel cyberspazio. Nel corso del 2025, l'attenzione principale della Russia rimarrà focalizzata sul conflitto in Ucraina, con il lancio di operazioni di spionaggio e attacchi distruttivi volti a indebolire la resistenza ucraina.

Parallelamente, il 2024 è stato definito "l'anno delle elezioni", spesso sfavorevole ai governi in carica. Durante il 2025, la Russia cercherà anche di utilizzare il cyberspazio per raccogliere informazioni e condurre operazioni di intelligence in seguito ai cambiamenti di regime in diversi Paesi. È quasi certo che Mosca tenterà di sfruttare l'insediamento di governi più favorevoli o "simpatetici" nei suoi confronti, alimentando sentimenti nazionalisti con l'obiettivo di:
a) promuovere la propria posizione e le proprie ambizioni sulla scena internazionale;
b) minare la cooperazione tra i Paesi dell'Unione Europea e della NATO.

È possibile che la Russia miri a consolidare i propri guadagni territoriali in Ucraina attraverso una risoluzione del conflitto, sebbene l'attività nel cyberspazio a supporto di tale obiettivo probabilmente non cambierà in modo sostanziale la minaccia sistemica già esistente per le imprese europee di medie dimensioni, che rimane da moderata ad alta.

Esiste una remota possibilità che la Russia tenti di allentare le tensioni con l'amministrazione Trump in arrivo, offrendo cooperazione in operazioni di contrasto al ransomware. Tuttavia, secondo l'analisi di WithSecure, questa eventualità è al momento improbabile e dipenderà dalla percezione statunitense della minaccia ransomware e dall'effettiva volontà della Russia di migliorare i rapporti con gli Stati Uniti.

Nel corso del 2024 si è molto discusso del rischio, secondo alcune valutazioni, che la Russia stia effettuando attività di pre-positioning all'interno delle infrastrutture critiche nazionali occidentali, con l'intento di sfruttare tale accesso in caso di conflitto diretto. Si tratta di un'analisi complessa, tuttavia, qualora fosse corretta, è improbabile che la Russia intenda utilizzare tale accesso per lanciare attacchi distruttivi contro infrastrutture critiche europee già nel 2025.

Durante il 2024 si sono verificati eventi significativi in cui attori quasi certamente sponsorizzati dallo Stato russo hanno preso di mira cavi sottomarini per Internet. Pur avendo implicazioni nel cyberspazio, tali attacchi esulano dall'ambito di questo rapporto.

Come evidenziato anche nella sezione dedicata all'hacktivismo, esiste un precedente di utilizzo da parte della Russia di tecniche di false-flag per raggiungere i propri obiettivi. Minacce simulate, come falsi attacchi ransomware o finti attacchi hacktivisti, potrebbero concretizzarsi per le aziende europee di medie dimensioni nel corso del 2025. Tuttavia, è probabile che tali minacce si manifestino nell'ambito di un conflitto (quasi certamente legato all'Ucraina) o in risposta a eventi geopolitici rilevanti.

Guardando al 2025, la Russia resta una minaccia significativa per il mid-market europeo e cercherà attivamente di compromettere organizzazioni che possano contribuire ai suoi obiettivi di intelligence e spionaggio. Il rischio per queste imprese derivante dalle APT russe è probabilmente inferiore rispetto a quello rappresentato dal ransomware, principalmente a causa del minore impatto distruttivo lasciato dalla maggior parte delle operazioni di spionaggio.

Cina

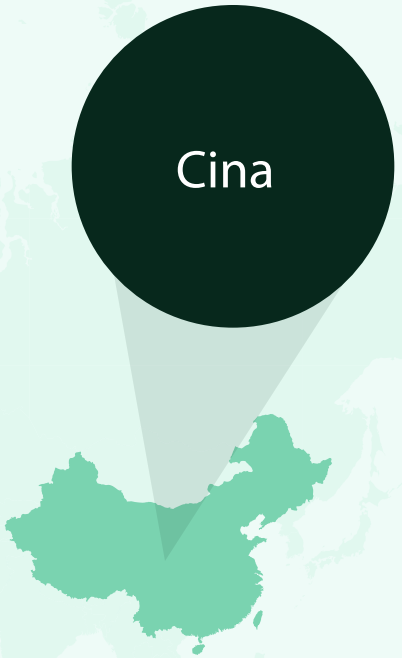
La Cina probabilmente dispone dell'apparato di intelligence con le maggiori risorse umane al mondo, e ciò si estende quasi certamente anche al cyberspazio. Questo conferisce alla Repubblica Popolare Cinese (RPC) la capacità di condurre operazioni estremamente ampie e articolate, sia in termini di portata che di scala. Unita a un'infrastruttura altamente sofisticata e ben finanziata, la Cina viene spesso indicata come la principale minaccia informatica per i governi occidentali.

Le operazioni di raccolta informazioni e le attività di pre-positioning non producono spesso effetti immediati e tangibili sulle organizzazioni vittime. Per questo motivo, fintanto che le relazioni internazionali con la Cina restano relativamente stabili, il rischio cibernetico associato alla RPC per il mid-market europeo è inferiore rispetto a quello che grava su reti governative o infrastrutture critiche dei Paesi percepiti da Pechino come avversari.

Gli attori legati alla RPC sono noti per colpire infrastrutture critiche nazionali, tra cui – ma non solo – comunicazioni, energia, settore militare, governo, gestione idrica e dei rifiuti. La CISA (Cybersecurity and Infrastructure Security Agency) ha osservato che l'attività "più attiva e persistente" attualmente in corso non corrisponde ai modelli tradizionali di spionaggio, ma è più probabilmente una preparazione per future azioni distruttive o di disturbo.

La Cina considera quasi certamente gli Stati Uniti il proprio principale rivale internazionale, ma è altrettanto certo che tali attività non siano limitate agli USA. Anche agenzie e organizzazioni europee sono state – e continueranno a essere – bersagliate.

Quantificare il rischio per il mid-market (in base al fatturato e/o al numero di dipendenti) risulta difficile, poiché il targeting da parte della Cina dipende maggiormente dalla funzione svolta dalla vittima e da quanto essa sia allineata con gli obiettivi strategici di Pechino.



I gruppi di intrusione statali sono noti per impiegare tattiche estremamente furtive nei loro attacchi, rendendone la rilevazione particolarmente difficile. In particolare, gli APT (Advanced Persistent Threats) cinesi sono notoriamente persistenti, ed è spesso molto complesso espellerli completamente da una rete anche dopo averli individuati.

Nel corso del 2025, la RPC continuerà quasi certamente a utilizzare exploit zero-day, n-day e vulnerabilità note contro infrastrutture connesse a Internet, industrializzando ulteriormente la raccolta e l'utilizzo di tali exploit.

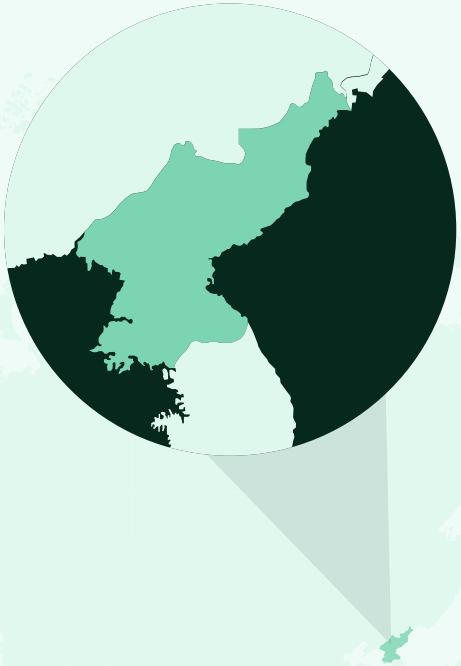
La compromissione di apparecchiature di routing contribuirà allo sviluppo di reti di offuscamento cinesi, che servono a mascherare il traffico degli attaccanti da e verso le reti delle vittime. Gli attori cinesi sono spesso osservati mentre prendono di mira dispositivi di rete, come firewall, su scala industriale, esfiltrando configurazioni e informazioni sugli utenti. Questo avviene quasi certamente con l'obiettivo di decifrare informazioni sensibili che potranno poi essere utilizzate in operazioni successive.

Le ambizioni della Cina nel cyberspazio non si limiteranno al pre-positioning, allo spionaggio e alla raccolta di informazioni. È quasi certo che Pechino continuerà a rubare proprietà intellettuale (IP) in settori chiave, per competere con gli sforzi di ricerca e sviluppo dell'industria occidentale. Sebbene l'impatto di queste attività non sia immediato, spesso portano all'erosione del vantaggio competitivo di un'azienda o di un prodotto sul mercato.

Come la Russia, anche gli attori sponsorizzati dallo Stato cinese cercheranno di condurre operazioni informative con l'obiettivo di influenzare le intenzioni di voto e l'opinione pubblica in Paesi strategicamente importanti. Questo sarà fatto a sostegno delle ambizioni strategiche cinesi, in particolare nell'area della cosiddetta nine-dash line, ma anche per rafforzare la posizione della Cina sul piano internazionale.

Gli eventi geopolitici influenzeranno fortemente le operazioni di informazione e spionaggio della Cina, e questo aspetto viene approfondito ulteriormente nella sezione geopolitica del rapporto.

Corea del Nord (DPRK)



La Repubblica Democratica Popolare di Corea (DPRK) impiega tipicamente le proprie capacità nel cyberspazio a supporto delle necessità economiche e degli obiettivi geopolitici del regime. Il focus geopolitico della Corea del Nord rimane concentrato nella propria regione, e considera la Repubblica di Corea (ROK / Corea del Sud) come il principale avversario. Per questo motivo, una parte significativa delle capacità offensive in ambito cibernetico sarà verosimilmente impiegata in operazioni di spionaggio contro la Corea del Sud. È inoltre probabile che la DPRK cercherà di condurre operazioni di disinformazione con l'obiettivo di minare la stabilità del governo sudcoreano o fomentare disordini interni.

Nel corso del 2025, la portata delle operazioni di spionaggio nordcoreane potrebbe estendersi oltre i confini sudcoreani, potenzialmente in risposta a esigenze tattiche legate ad ambiti come quello militare o sanitario. In quanto paese fortemente sanzionato e isolato dalla comunità internazionale, la Corea del Nord si affida pesantemente alle proprie capacità cibernetiche per ottenere risorse e tecnologia. La recente presenza di truppe nordcoreane in Ucraina è quasi certamente da interpretare come un'operazione condotta in veste mercenaria, probabilmente con l'intento di ottenere finanziamenti, equipaggiamenti o know-how da parte della Russia.

La principale minaccia della DPRK nei confronti del mid-market europeo si concretizza attraverso le sue vaste operazioni finalizzate alla generazione di entrate illecite. Le organizzazioni che operano nel settore delle criptovalute, o che detengono asset crittografici, continueranno con ogni probabilità a essere obiettivi diretti o indiretti degli attori nordcoreani. La Corea del Nord è nota per l'adozione di tecniche e procedure particolarmente innovative, soprattutto quando mira a colpire entità legate al mondo delle criptovalute. È altamente probabile che continui a sviluppare malware specifici per il sistema macOS, costituendo una delle minacce più rilevanti per quell'ecosistema. Allo stesso tempo, gli attacchi alla supply chain del software rappresentano per la DPRK un metodo produttivo per distribuire infostealer progettati per colpire chi opera nell'ambito cripto. Entrambe queste tattiche consentono alla Corea del Nord di estendere in modo efficace il proprio raggio d'azione, colpendo organizzazioni e individui appartenenti a un settore ben definito ma sempre più strategico come quello del Web3 e delle criptovalute.

È altamente probabile che gli attori della DPRK partecipino attivamente ai circuiti della criminalità informatica, inclusi quelli legati al ransomware. Al pari di altri gruppi criminali, anche i nordcoreani faranno ricorso a tecniche di social engineering per ottenere accesso alle reti aziendali, e con ogni probabilità utilizzeranno strumenti di intelligenza artificiale generativa, in particolare deepfake, per aumentare l'efficacia di tali attacchi. Tuttavia, a differenza della maggior parte dei gruppi criminali, la Corea del Nord dispone delle capacità, delle risorse, dell'infrastruttura e della pazienza necessarie per portare avanti operazioni complesse e di lungo periodo contro obiettivi difficili, ossia aziende ben difese e dotate di team di sicurezza informatica avanzati. Un esempio rilevante di questo approccio è rappresentato dall'infiltrazione di propri operatori IT all'interno di decine di organizzazioni appartenenti alla classifica 'Fortune 100'.

È improbabile che la capacità cibernetica della DPRK stia diminuendo con l'ingresso nel 2025; al contrario, il regime è pienamente consapevole del valore strategico che le operazioni nel cyberspazio apportano. La Corea del Nord dispone ormai di percorsi formativi ben strutturati e consolidati per alimentare i ranghi delle proprie unità cyber, ed è riuscita a rendersi relativamente impermeabile all'efficacia delle sanzioni occidentali. Inoltre, l'aumento del valore delle criptovalute potrebbe rappresentare un ulteriore incentivo e fattore di rafforzamento per le attività cibernetiche del regime, contribuendo a mantenerne alta la motivazione e l'intensità operativa.

Iran

Nel 2025, l'Iran concentrerà principalmente le sue attività cibernetiche su Israele e Hamas, con un focus particolare sul Medio Oriente. Israele sarà visto come una minaccia prioritaria e le tensioni tra i due paesi, già aumentate nel 2024, continueranno a riflettersi in azioni cibernetiche da entrambe le parti. Le operazioni iraniane mireranno a governi, telecomunicazioni, vantaggi militari e giornalisti dissidenti. Inoltre, l'Iran ha mostrato un coinvolgimento nelle operazioni di ransomware. Nel contesto europeo, la minaccia iraniana per il mid-market è considerata di livello moderato-basso nel 2025.

State Ransomware

Il ransomware è diventato così diffuso che il suo utilizzo non può più essere limitato solo al guadagno finanziario. L'industria della cybersicurezza ha numerosi esempi di attacchi distruttivi sponsorizzati da stati che si travestono da ransomware. Attualmente, questo modello di minaccia non è realistico per la maggior parte delle organizzazioni che operano lontano dalla sfera di conflitto nell'Europa orientale, ma potrebbe cambiare in risposta all'aumento delle tensioni geopolitiche. Alcune organizzazioni private, non con sede in Ucraina, sono state colpite dalla campagna di "ransomware" di stato russo, chiamata Prestige. Microsoft ha documentato attacchi a organizzazioni in Polonia, e WithSecure ha rilevato impianti collegati a Prestige nelle reti estoni. Sebbene WithSecure Threat Intelligence abbia osservato eventi di ransomware operati dallo stato che mirano a piccole organizzazioni europee, è probabile che questa rappresenti una minaccia significativa solo per le organizzazioni che operano nelle aree di conflitto. Tuttavia, tale minaccia potrebbe estendersi a un numero maggiore di organizzazioni nel mid-market europeo nel caso di un'escalation tra Iran e Israele o tra Cina e Taiwan, in cui le organizzazioni dovrebbero riconsiderare questo modello di minaccia.

La Corea del Nord (DPRK) è un'eccezione quando si considerano gli eventi di CNE/CNA (Computer Network Exploitation / Attack) sponsorizzati dallo stato, poiché i loro gruppi di intrusione operano anche con un mandato di generazione di entrate. Sebbene ci siano esempi di famiglie di ransomware sviluppate direttamente dalla DPRK, questi non sono stati osservati da molto tempo. È molto più probabile che gli attori della DPRK utilizzino modelli consolidati di ransomware-as-a-service per condurre i loro attacchi. WithSecure ha rilevato sovrapposizioni nelle infrastrutture utilizzate nelle intrusioni orchestrate dalla DPRK e in quelle condotte da affiliati al ransomware. Questo modello viene anche impiegato da alcuni attori sponsorizzati dallo stato iraniano, che probabilmente "lavorano part-time" con operazioni di ransomware.

Cloud

È quasi certo che ogni nazione avversaria elencata sopra avrà la capacità di mirare ai servizi cloud di una vittima. Come per altri tipi di attori, è molto probabile che gli APT sponsorizzati dallo stato considerino questo vettore attraente a causa della relativa mancanza di comprensione da parte degli utenti, delle impostazioni predefinite insicure, della mancanza di registrazioni e di poche soluzioni EDR, nonché dell'abbondanza di identità compromesse a loro disposizione.

Non ci sono eventi significativi documentati che suggeriscano una minaccia sistematica alle risorse nel cloud tramite il compromesso dell'infrastruttura di base dell' "host". Tuttavia, è probabile che gli stati nazionali avanzati abbiano la capacità di raggiungere questo obiettivo. La Cina ha dimostrato la propria volontà e capacità di mirare ai servizi di backbone (ISP / Telecomunicazioni) e è improbabile che vedano i CSP come sostanzialmente diversi da questo profilo di targeting consolidato. È improbabile che anche un piccolo numero di organizzazioni criminali possa condurre operazioni simili su sistemi sicuri [mirando remotamente all'infrastruttura "guest" spostandosi lateralmente dall'infrastruttura "host"] senza un aiuto significativo.

Hacktivismo

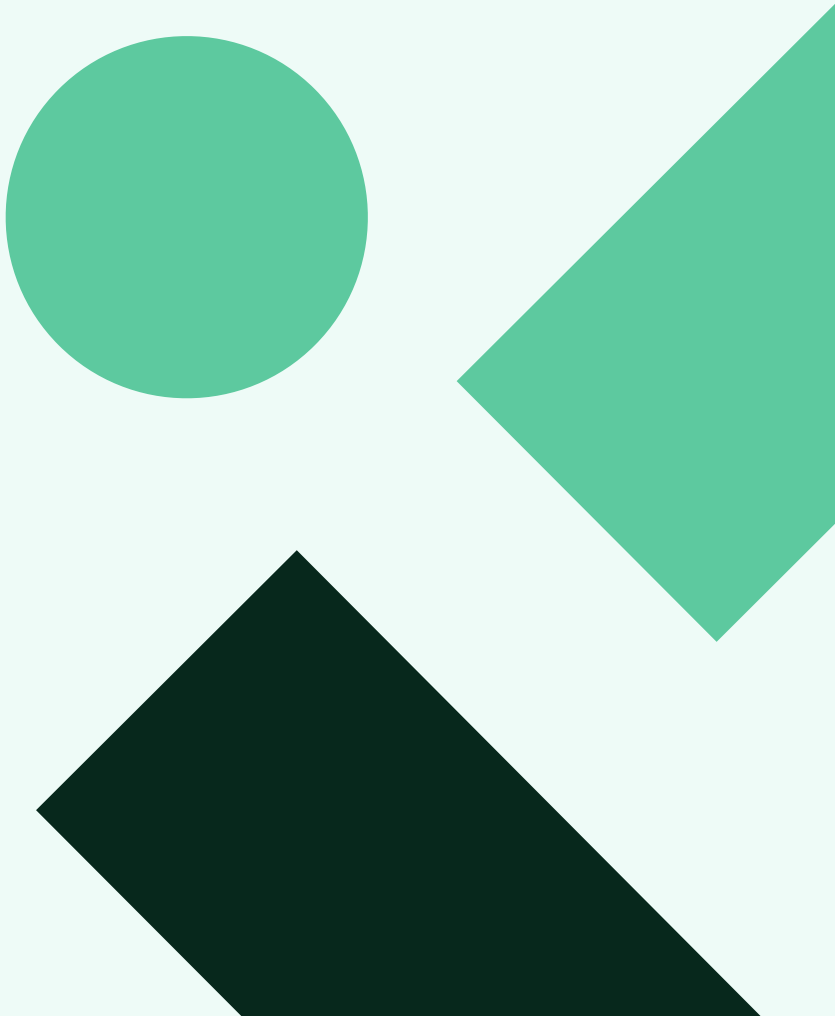
I collettivi hacktivisti pro-russi rimangono una minaccia per le organizzazioni in tutta Europa. Non è chiaro come eventuali negoziati di pace influenzeranno le loro operazioni nel 2025, ma nel caso in cui l'Unione Europea aumenti il suo supporto militare all'Ucraina (forse per colmare un vuoto lasciato dagli Stati Uniti), è probabile che le organizzazioni europee affrontino una maggiore minaccia da parte degli hacktivisti. Questa minaccia si manifesterebbe principalmente sotto forma di attacchi DDoS e eventi sporadici di distruzione di dati (wiper).

I collettivi hacktivisti, per loro natura, rispondono principalmente a eventi geopolitici, pur mantenendo una cadenza regolare di attacchi. Gli attacchi DDoS sono lanciati quotidianamente dagli hacktivisti. È comune che gli hacktivisti pro-russi cambino i paesi target quotidianamente (sebbene l'Ucraina venga sempre presa di mira). Gli obiettivi sono spesso piccole imprese, nodi di trasporto o funzioni governative regionali. È probabile che venga effettuata una leggera attività di ricognizione per verificare se una particolare tecnologia sia in uso dalla vittima potenziale o se sia in atto una protezione DDoS, prima che vengano scelti i target per gli attacchi. Questo porta spesso a colpire organizzazioni di dimensioni medie e governi locali.

Come notato, ci sono anche eventi hacktivist più distinti che si allineano con eventi geopolitici significativi. Questo spesso porta a un attacco DDoS più concertato (e ampiamente impattante). L'attività hacktivist legata alle elezioni romene della fine del 2024 è apparsa particolarmente coreografata, proprio come gli attacchi ai bersagli governativi francesi durante le loro elezioni parlamentari a metà del 2024. Un nuovo governo negli Stati Uniti cambierà la politica estera riguardo alla Russia (influenzando la politica europea) e questo influenzerà la minaccia hacktivista, in un modo o nell'altro.

Nel corso del 2024, con il progredire degli eventi riguardanti Israele, Palestina e Iran, sono emersi nuovi collettivi hacktivist. Gli hacktivist focalizzati sul Medio Oriente sono localizzati e principalmente indirizzano attacchi offensivi dall'Iran verso Israele (o aziende israeliane) e viceversa. Se l'attività cinetica tra Iran e Israele si intensificherà, è quasi certo che l'attività informatica seguirà lo stesso percorso. L'attività militare israeliana in Palestina a seguito dell'attacco terroristico di Hamas del 7 ottobre 2023 ha attirato molta attenzione internazionale, con molteplici accuse di violazioni dei diritti umani contro Israele. Questi eventi si sono in qualche modo riversati nello spirito politico europeo, tanto da interrompere eventi sportivi. È probabile che gli eventi hacktivist si espanderanno anche oltre questa sfera geografica. Le organizzazioni europee che prenderanno una posizione netta su uno dei lati del conflitto o che si associano con l'esercito o il governo israeliano, affronteranno una minaccia hacktivista crescente. Come nel caso dei gruppi hacktivist filo-russi, ciò avverrà probabilmente sotto forma di attacchi DDoS e attacchi wiper.

I gruppi hacktivist cercheranno anche di compromettere e disturbare i sistemi SCADA/ICS. Gli hacktivist generalmente utilizzano tecniche e tattiche di attacco poco sofisticate e saranno dipendenti dal mirare a sistemi poco sicuri e accessibili da internet.



Capacità DDoS

Gli attori DDoS e gli hacktivisti utilizzano una combinazione di servizi di "stresser" facilmente accessibili e botnet proprietarie. Queste botnet sono principalmente composte da reti di dispositivi vulnerabili appartenenti a piccole imprese o a dispositivi IoT (Internet of Things), sebbene a volte siano inclusi anche endpoint aziendali come parte di grandi botnet DDoS. Questi dispositivi sono particolarmente attraenti per i "bot herders" (gestori di botnet) a causa di configurazioni predefinite deboli e della generale mancanza di monitoraggio della sicurezza e aggiornamenti. I servizi cloud sono anche presi di mira e utilizzati negli attacchi DDoS, tra cui, ma non solo: Jupyter, Hadoop, HugeGraph.

Si prevede che il numero di dispositivi IoT aumenterà a 30-40 miliardi nel 2025. Il Cyber Resilience Act dell'UE è entrato in vigore verso la fine del 2024, imponendo standard di sicurezza informatica più elevati per i dispositivi IoT. Questo limiterà la proliferazione di dispositivi vulnerabili, tuttavia è improbabile che i bot herders siano dissuasi, poiché non mancheranno dispositivi vulnerabili fuori dall'Unione Europea. Sfruttare dispositivi IoT / SOHO continuerà anche nel 2025, in particolare poiché molte delle vulnerabilità sfruttate dai bot herders sono vecchie; ad esempio, una vulnerabilità sfruttata a metà del 2024 nei router D-Link è stata rilasciata per la prima volta nel 2014.

Altri rischi

Hack and Leak

Gli operatori di "hack and leak" sono definiti da attori che eseguono operazioni di furto o fuga di dati. Spesso, non hanno un obiettivo apparente e si limitano a divulgare i dati. Molti attori cercano di vendere i dati ad altri soggetti, che probabilmente tenteranno poi di sfruttare queste informazioni per estorcere denaro alla vittima o lanciare ulteriori attacchi. Gli attori che eseguono queste operazioni mostrano una minore sofisticazione rispetto ad altri attori. Quasi esclusivamente mirano a sfruttare vulnerabilità in modo speculativo. Ciò significa che, sebbene possano causare un impatto tangibile sulle loro vittime, possono essere considerati una minaccia bassa per il mercato medio europeo.

DDoS Anarchici

I DDoS non motivati da ideologie, che non si allineano agli obiettivi di altri attori (ad esempio, come parte di una richiesta di estorsione tramite ransomware), possono essere considerati "Anarchici". Questo termine definisce gli attori che potrebbero avere vendette personali contro un'organizzazione o un servizio, desiderano ottenere notorietà o forse sono semplicemente "annoiati". Questi attori rappresentano una minaccia bassa per il mercato medio europeo, tuttavia causano impatti sporadici, spesso sotto forma di interruzioni minori.

Fattori Chiave 2025

Cambiamenti nelle Forze Geopolitiche

Le forze geopolitiche plasmano in modo significativo il panorama delle minacce cibernetiche. Le principali potenze mantengono e impiegano capacità offensive nel cyberspazio. Le azioni geopolitiche e statali (sia dentro che fuori dal cyberspazio) stabiliscono il tono per altre minacce che potrebbero non operare sotto il controllo diretto di uno stato.

I gruppi APT (Advanced Persistent Threat) tipicamente agiscono direttamente per promuovere gli obiettivi strategici di uno stato-nazione. Queste minacce, nonostante un'impronta mediatica asimmetricamente grande, non sono generalmente il rischio maggiore per la maggior parte delle organizzazioni di medie dimensioni. Detto ciò, l'analisi geopolitica non deve essere trascurata, poiché, come già sottolineato, queste forze influenzano l'ambiente macro-cibernetico più di quanto spesso venga riconosciuto. Ad esempio, mentre le difficoltà economiche catalizzano direttamente l'aumento dell'attività criminale informatica, le conseguenze continue dall'invasione illegale dell'Ucraina da parte della Russia e la conseguente crisi energetica ed economica avranno quasi sicuramente spinto gli attori verso una partecipazione attiva nell'ecosistema del crimine informatico.

Questo ha un impatto economico significativo – se il crimine informatico fosse un'economia, per PIL, sarebbe la terza più grande al mondo. Il 2024 è stato un anno rilevante a causa del numero di elezioni tenute in vari paesi del mondo. Cinque dei sette paesi del G7 hanno tenuto elezioni nazionali, mentre gli altri due (Canada e Italia) hanno avuto elezioni regionali. Diciassette paesi africani hanno tenuto elezioni generali, presidenziali o parlamentari, così come altre potenze internazionali, come l'Unione Europea e l'India. Mentre anche la Russia e la Corea del Nord hanno tenuto elezioni, è quasi certo che queste siano state solo dimostrative.

Le elezioni presidenziali negli Stati Uniti

Al momento della redazione di questo rapporto, Donald Trump è stato eletto come prossimo presidente degli Stati Uniti. Mancano ancora alcune settimane prima che assuma il potere, e c'è ancora incertezze riguardo l'orientamento della Camera dei Rappresentanti, che potrebbe favorire o limitare le ambizioni del governo Trump. È probabile che Trump segua un'agenda "America First" e adotti una posizione più isolazionista. Ciò potrebbe influire economicamente sull'Europa, poiché potrebbero essere introdotti o aumentati barriere commerciali e tariffe sulle importazioni dal principale partner commerciale dell'UE. Le barriere commerciali potrebbero essere viste come ostili dalla Cina, portando alcuni commentatori a speculare su una possibile guerra commerciale. Non sappiamo ancora quale sarà la posizione degli Stati Uniti riguardo le importazioni dalla Cina, ma è altamente probabile che ciò stimolerà l'attività statale cinese nel cyberspazio.

Negli ultimi anni, la cooperazione tra le forze dell'ordine europee e statunitensi è stata un motore fondamentale per numerose azioni di successo contro le reti criminali informatiche e i singoli attori. È improbabile che una nuova amministrazione Trump cambi significativamente questa cooperazione, soprattutto considerando che gli Stati Uniti rimangono il paese più colpito da attacchi ransomware e altri attori criminali.

Russia/Ucraina

Dopo l'invasione dell'Ucraina da parte della Russia nel 2022, l'aumento dei prezzi del petrolio ha aggravato le pressioni economiche causate dai pacchetti di stimolo in risposta alla pandemia di Covid-19, scatenando una crisi del costo della vita in molti paesi. Donald Trump ha affermato che sarà in grado di portare a una rapida fine della guerra in Ucraina, probabilmente minacciando di ritirare gli aiuti se l'Ucraina non accetterà alcune delle sue perdite territoriali. WithSecure non ha allocato risorse analitiche per valutare completamente la probabilità o l'impatto di ciò, ma è improbabile che, a breve termine, ciò comporti una riduzione dell'attività informatica intorno all'Ucraina. Rimane altamente probabile che, in caso di questo scenario, gli attacchi entreranno in una nuova fase nel 2025. L'attività informatica offensiva russa in Ucraina è cambiata nel corso del 2022 (con un focus sullo smantellamento delle infrastrutture), nel 2023 (concentrandosi sulla messa in sicurezza delle posizioni e cercando feedback sulle azioni cinetiche) e nel 2024 (con operazioni di spionaggio, targeting militare e delle infrastrutture critiche nazionali). È quasi certo che, dal 2022, queste operazioni si siano estese nei paesi europei circostanti. In caso di negoziati di cessate il fuoco, è improbabile che la minaccia da parte della Russia e degli attori allineati con lo Stato cambi per i paesi europei che sono periferici rispetto all'Ucraina e che la supportano.

Supporto europeo / NATO

L'aumento della spesa per la difesa in Europa è stato significativo dopo l'invasione dell'Ucraina da parte della Russia nel 2022. I paesi che non raggiungono l'impegno del 2% di spesa per la difesa sono stati costantemente criticati dal presidente eletto Trump, che probabilmente ritiene che gli Stati Uniti stiano sopportando un "carico" sproporzionato in termini di difesa dell'Europa. Non è chiaro in che misura gli Stati Uniti manterranno o ridurranno il loro supporto militare alla difesa europea, anche se è improbabile che gli Stati Uniti rinuncino completamente agli obblighi di difesa collettiva della NATO nel 2025. Tuttavia, è possibile che una NATO percepita come indebolita possa spingere la Russia ad agire con maggiore aggressività nella regione, il che, a sua volta, potrebbe portare a un aumento dell'attività informatica (cyber attività).

Cina/Taiwan

Molti commentatori politici hanno osservato che l'accomodamento delle ambizioni territoriali della Russia potrebbe creare un precedente che la Cina potrebbe cercare di sfruttare nelle sue ambizioni di espandere il proprio territorio all'interno della "linea delle nove dash" – un'area che comprende Taiwan. Le dichiarazioni di Trump relative all'imposizione di tariffe elevate minacciano una guerra commerciale con la Cina e, di conseguenza, c'è una possibilità reale che le relazioni tra Stati Uniti e Cina peggiorino in qualche misura. Detto ciò, non è possibile fare una valutazione con sufficiente fiducia su come si svilupperanno gli eventi relativi a Taiwan nel 2025.

Cryptovalute

Da quando Donald Trump è stato eletto come prossimo presidente degli Stati Uniti, il prezzo del Bitcoin ha raggiunto un massimo storico, con un valore aggiuntivo del 41% (al momento della scrittura) rispetto al mese precedente. Le criptovalute sono preferite dai criminali informatici a causa della loro natura decentralizzata e della mancanza di regolamentazione. Mentre il Bitcoin è considerato una delle criptovalute più "legittime", altre monete più focalizzate sulla privacy, come Monero, non hanno registrato lo stesso aumento del prezzo. È probabile che l'aumento del prezzo galvanizzi attori motivati finanziariamente, che cercheranno di frodare, truffare o rubare Bitcoin dalle vittime. I criminali che potrebbero detenere Bitcoin (forse come pagamento da tentativi di estorsione riusciti) ora avranno accesso a risorse aumentate. Risorse che, in molti casi, sono già considerevoli. È possibile che l'aumento del prezzo del Bitcoin galvanizzi in qualche modo il mercato sotterraneo dei criminali informatici e gli attori minacciosi motivati finanziariamente. Come per ogni attacco al "settore bancario" dei consumatori, le principali aree di battaglia continueranno a concentrarsi sull'identità e sui materiali di autenticazione della vittima. Questa valutazione si basa sull'assunzione che il valore del Bitcoin, un asset notoriamente volatile, rimarrà stabile o crescerà.

Tecnologie emergenti

Intelligenza Artificiale

L'intelligenza artificiale sta avanzando rapidamente e sta diventando sempre più accessibile al grande pubblico. Nuovi modelli migliorati vengono rilasciati con crescente frequenza, migliorando continuamente sia l'accuratezza che la qualità dei risultati. Da una prospettiva concettuale, ci sono attualmente alcune limitazioni fondamentali che impediscono il raggiungimento dell'Intelligenza Artificiale Generale (AGI), il che riduce in parte l'impatto attuale dell'intelligenza artificiale. Il vero ragionamento AI non è ancora possibile, il che significa che un essere umano (in questo caso, un attaccante) deve rimanere "coinvolto nel processo". Nonostante ciò, è quasi certo che ci sarà un aumento significativo delle capacità che assisterà sia gli attori positivi che quelli maligni.

Molti modelli linguistici di grandi dimensioni (Large Language Models) e servizi di AI generativa (genAI) commercialmente disponibili contengono misure di sicurezza che impediscono la creazione di contenuti dannosi o illegali. Detto ciò, esistono molti modelli open-source disponibili, che offrono agli attori l'opportunità di implementare AI generativa dannosa e non regolamentata. Poiché l'implementazione di un modello privato non è così semplice, capace o economica come l'utilizzo di soluzioni genAI commerciali, gli attori delle minacce stanno cercando di aggirare le misure di sicurezza messe in atto dai servizi genAI. È relativamente semplice farlo, e i ricercatori di sicurezza e i criminali informatici stanno liberamente condividendo guide pratiche per "jailbreak" delle capacità di AI generativa. Questo dimostra un tasso crescente, ma ancora nascente, di adozione di servizi AI facilmente accessibili da parte dei criminali.

Abbassare il livello

Nella sua forma attuale, e probabilmente anche nelle future iterazioni dei modelli, l'AI generativa rappresenta uno strumento estremamente utile per gli attori delle minacce, ma è improbabile che rivoluzioni drasticamente gli attacchi informatici nel 2025. Piuttosto, probabilmente integrerà e migliorerà gli attori che saranno in grado di ottenere fondamentalmente ciò che ottengono attualmente, in modo più economico ed efficiente. Tuttavia, l'impatto che avrà sul panorama della criminalità informatica non deve essere sottovalutato, poiché le lacune tra gli attori più capaci e quelli meno capaci si ridurranno. Il ritmo dei progressi nelle capacità dell'AI abbassa la capacità di prevedere il lungo termine con alta confidenza.

L'avvento dell'AI non ha cambiato il fatto che il ransomware rimanga una minaccia primaria per il mercato medio europeo. Nel breve periodo, un aumento del numero di attori criminali capaci di operare in modo relativamente efficace in questo settore potrebbe risultare più dannoso nel complesso rispetto allo sviluppo di nuove e altamente avanzate tecniche di attacco guidate dall'AI. Questi sviluppi potrebbero arrivare, ma saranno quasi certamente pionieristici da parte di set di intrusioni altamente capaci, probabilmente operanti su un profilo di vittima molto più specifico rispetto al mercato medio europeo.

L'intelligenza artificiale porterà vantaggi sia agli attaccanti che ai difensori; pertanto, il suo impatto sul panorama informatico sarà un'economia, offrendo un insieme diseguale di benefici e svantaggi per la missione di difesa della rete. Le imprese legittime avranno un accesso migliore a un'AI più capace e, di conseguenza, nel 2025, l'AI probabilmente produrrà un bilancio positivo per i difensori della rete e le funzioni legittime di sicurezza informatica, purché sia democratizzata e disponibile anche per coloro che non dispongono di grandi budget IT.

Implicazioni Geopolitiche

L'Unione Europea osserva che "l'adozione della tecnologia AI probabilmente determinerà il percorso dello sviluppo economico futuro dell'UE". Questa visione è quasi certamente condivisa anche da altre economie, rendendo l'accesso alla tecnologia e ai materiali che la sostengono una battaglia geopolitica fondamentale. La regolamentazione dell'AI sarà un tema centrale di discussione nel 2025, poiché le autorità saranno sotto pressione per non "sovra-regolamentare" il suo uso e la sua distribuzione al fine di sbloccare maggiori potenzialità economiche. Ovviamente, una regolamentazione più flessibile può lasciare la tecnologia più esposta agli abusi.

Attacchi contro l'AI

WithSecure Consulting è all'avanguardia nella ricerca sugli attacchi contro l'AI/LLM e sugli attacchi che utilizzano AI/LLM. Poiché si tratta ancora di una capacità relativamente emergente, questa ricerca è rilevante per le previsioni sulle minacce nel 2025 .

Ai Genetica

L'AI agentica è un metodo che consente all'intelligenza artificiale di agire in modo indipendente per raggiungere i suoi obiettivi prefissati. L'adozione dei flussi di lavoro agentici da parte delle organizzazioni aumenterà quasi certamente nel 2025, il che aumenterà a sua volta il rischio di attacchi tramite iniezione di prompt, un problema ancora irrisolto anche nei modelli più recenti di OpenAI. Se jailbroken, questi flussi di lavoro possono naturalmente essere abusati da attori con intenzioni malevoli. È molto probabile che ci sarà un alto livello di intenzionalità da parte degli attori, tuttavia ci saranno dei limiti su come potrà essere implementato "in azione". Al momento della stesura di questo rapporto, Anthropic ha rilasciato una capacità beta chiamata "uso del computer" che cerca di emulare un essere umano che usa un computer. Ciò ha portato a speculazioni sull'uso dell'AI agentica nelle funzionalità di comando e controllo. In realtà, questa capacità è inefficace nella sua forma attuale e probabilmente presenterebbe anche una maggiore possibilità di rilevamento rispetto ad altri metodi di comando e controllo. Come con altri concetti di AI, se l'AI agentica riuscirà a uscire dallo stato attuale di "prototipo/ricerca", i flussi di lavoro offriranno alcuni vantaggi agli attori maligni, così come agli utenti legittimi, ma è improbabile che ci sarà un aumento significativo della minaccia come risultato. L'AI è in rapido sviluppo e, con l'aumento delle capacità, è possibile che questa valutazione cambi.

Tecnologia Deepfake

La tecnologia deepfake è già utilizzata da truffatori e truffatori informatici, e come notato, questo è al di fuori dello scopo di questo rapporto in quanto non si tratta di tecniche di sfruttamento o attacco di rete informatica. Detto ciò, è stato osservato che, con la prevalenza delle tecniche di ingegneria sociale, la tecnologia deepfake potrebbe essere vista come un modo valido per ottimizzare e migliorare gli elementi di ingegneria sociale di un'intrusione in una rete informatica.

Quantum Computing

Il calcolo quantistico è stato a lungo descritto come una tecnologia trasformativa che minaccerà gravemente alcuni degli standard di crittografia fondamentali per la sicurezza dei sistemi informativi e i processi di autenticazione. Teoricamente, i computer quantistici potrebbero anche indebolire la crittografia simmetrica (anche se l'aumento della lunghezza delle chiavi potrebbe offrire una mitigazione sufficiente nel breve termine). Non c'è dubbio che il calcolo quantistico avrà un impatto serio sul panorama della sicurezza quando diventerà generalmente disponibile, anche se è improbabile che rappresenti una minaccia significativa e diretta nel 2025. Le organizzazioni sono, e sono state, istruite a prepararsi per un mondo post-quantistico, dove saranno necessarie tecniche di crittografia resistenti al calcolo quantistico. Molti fornitori di servizi cloud (CSP) stanno già aggiungendo metodi di crittografia resistenti al calcolo quantistico alle loro offerte. C'è anche speculazione sul fatto che alcune organizzazioni governative stiano adottando una strategia di "raccogliere ora, elaborare dopo", sebbene non abbiamo prove di ciò presso WithSecure. Il calcolo quantistico sta avanzando, e Google ha dimostrato nuove capacità con il loro processore Willow, e mentre è quasi certo che ciò non rappresenterà una minaccia per il mercato medio europeo nel 2025, molte organizzazioni dovrebbero iniziare a prepararsi per il futuro.

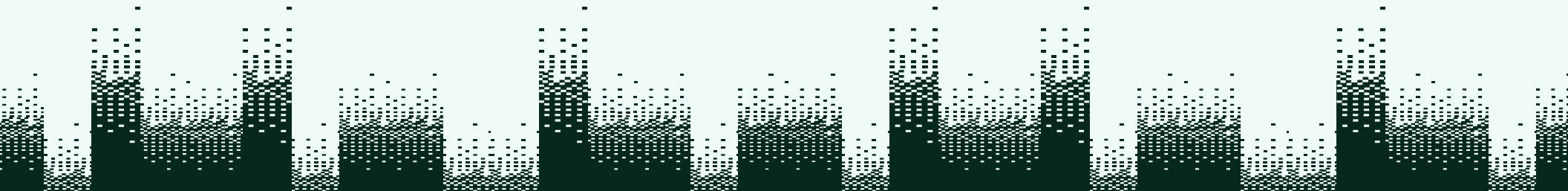
Battlegrounds 2025

Identity and Cloud

Più il cloud diventa una parte intrinseca delle reti organizzative, più vediamo l'evoluzione da attori minacciosi "cloud-aware" (consapevoli del cloud) a "cloud-astute" (esperti del cloud). L'uso di strumenti e funzionalità legittimi per completare compiti illegittimi sarà un tema chiave con cui i difensori delle reti dovranno confrontarsi nel 2025, continuando dal 2024. Abbiamo iniziato a osservare l'uso di servizi cloud noti come nodi negli attacchi, non limitandosi solo all'infrastruttura C2. Poiché le organizzazioni sono diventate sempre più "de-perimeterizzate", ciò ha catalizzato l'industria degli infostealer e il furto di identità/materiale di autenticazione continuerà a essere una tendenza chiave, sebbene ciò non significhi che lo sfruttamento massivo dei servizi edge cesserà nel 2025.

I Major Cloud Service Providers (CSPs) sono abbastanza risorse per impiegare la propria capacità di risposta agli incidenti a tempo pieno. Questo rende estremamente difficile condurre valutazioni sulla minaccia per i fornitori di infrastrutture Cloud, in particolare se si cerca di chiarire se l'assenza di prove riguardanti compromissioni dei sistemi infrastrutturali sottostanti del cloud possa essere interpretata come prova di assenza. Un problema chiave con la tecnologia del cloud è che gli utenti dei servizi spesso non hanno visibilità sulla residenza dei dati specifici, le vulnerabilità o gli incidenti che coinvolgono l'infrastruttura sottostante e i sistemi che supportano i servizi 'aaS'.

Poiché il cloud computing rappresenta un cambiamento così significativo nell'architettura dei sistemi informativi delle imprese globali, alcune sezioni specifiche di questo rapporto non verranno duplicate in questa parte. I lettori dovrebbero fare riferimento a queste sezioni per una comprensione più dettagliata della superficie di minaccia del cloud, contestualizzata dal tipo di minaccia.



Mobile

I dispositivi mobili sono ormai la scelta preferita come dispositivi informatici personali per gli individui. Per questo motivo, il targeting dei dispositivi mobili è stato a lungo un metodo efficace per attaccare il settore bancario personale. Ci sono anche numerosi esempi di attacchi sofisticati e altamente mirati contro individui di valore strategico.

I dispositivi Apple iOS spingono automaticamente gli aggiornamenti di sicurezza sui dispositivi degli utenti e le applicazioni devono essere scaricate dall'App Store ufficiale, solo dopo aver ottenuto l'approvazione a seguito di un rigoroso controllo da parte di Apple. Pertanto, per attaccare dispositivi iOS, gli attacchi richiedono spesso competenze molto specifiche per scoprire e sfruttare vulnerabilità zero-day.

Le aziende di intelligence private sono state note per acquistare tali vulnerabilità "0-click" [senza interazione dell'utente] per 1 milione di dollari USA. Poiché questi exploit sono così preziosi, e spesso vengono mitigati subito dopo la loro scoperta da parte dei ricercatori, non vengono di solito utilizzati in modo ampio. Per questa ragione, è improbabile che le minacce specifiche ai dispositivi Apple iOS rappresentino una minaccia significativa per le imprese di media grandezza in Europa nel loro complesso, tuttavia ci potrebbero essere eccezioni specifiche per individui o singole organizzazioni.

C'è una maggiore minaccia per i dispositivi Android, poiché l'ambiente è molto meno restrittivo per gli sviluppatori di applicazioni. I malware mobili segnalati nel dominio pubblico prendono di mira principalmente informazioni sensibili, con l'intento di accedere a conti bancari e criptovalute. Ciò rappresenta una minaccia per individui e piccoli imprenditori. Il malware bancario mobile su Android è molto più comune in Sud America che in Europa e è molto probabile che ciò sia dovuto a pratiche culturali e ai differenti controlli imposti dal settore bancario. Prendere di mira i dispositivi mobili non è un vettore particolarmente praticabile per gli attori del ransomware, ma le risorse organizzative sono spesso accessibili tramite tali dispositivi. Pertanto, il malware mobile rappresenterà una minaccia da moderata a bassa per il mercato medio europeo, dove sono in atto controlli e politiche adeguate.

È stato a lungo previsto che, con l'aumento dell'adozione dei dispositivi mobili, aumentassero anche le minacce mobili. Tuttavia, ciò non si è verificato come previsto, in parte grazie alle restrizioni di sicurezza efficaci messe in atto negli ambienti mobili, ma anche perché il mirare agli endpoint rimane ancora un modo più praticabile per ottenere un punto d'accesso quando si cerca di compromettere una rete. È altamente improbabile che la minaccia mobile per il mercato medio europeo nel 2025 sarà sostanzialmente diversa rispetto al 2024.

MacOS

Gli infostealer rappresentano la principale minaccia per gli utenti MacOS, e diversi fornitori di Infostealer Malware as a Service (MaaS) per MacOS stanno proliferando questi infostealer. Esiste molto poco ransomware che prende di mira specificamente MacOS, e non ci sono indicazioni che le varianti conosciute di ransomware per MacOS siano minacce credibili per il mercato medio europeo. Probabilmente ciò è dovuto al fatto che MacOS ha una quota di mercato inferiore nel settore aziendale, dove il ransomware genera i maggiori profitti. Inoltre, non esistono server MacOS, che sono solitamente il bersaglio principale del ransomware per ottenere il massimo effetto.

Poiché l'architettura del processore Apple silicon è condivisa tra dispositivi desktop e mobili Apple, è possibile che una singola applicazione dannosa possa essere efficace su più piattaforme hardware. Tuttavia, al momento, ci sono pochissimi casi conosciuti di malware su dispositivi iOS/mobili, e questo è improbabile che cambi entro il 2025.

La quota di mercato di MacOS non cambierà drasticamente nei prossimi 0-5 anni. La tendenza principale attuale su cui i fornitori di hardware e software stanno puntando sono i modelli di linguaggio di grandi dimensioni (LLM), e sembra che Apple abbia dichiarato di stare indagando sull'esecuzione di LLM sui dispositivi tramite hardware personalizzato. Questo potrebbe essere una soluzione attraente per alcuni utenti, ma l'hardware personalizzato è costoso, quindi è improbabile che il prezzo dei dispositivi Apple scenda rispetto alla concorrenza. Di conseguenza, non c'è motivo di aspettarsi un cambiamento improvviso nella domanda o nella quota di mercato.

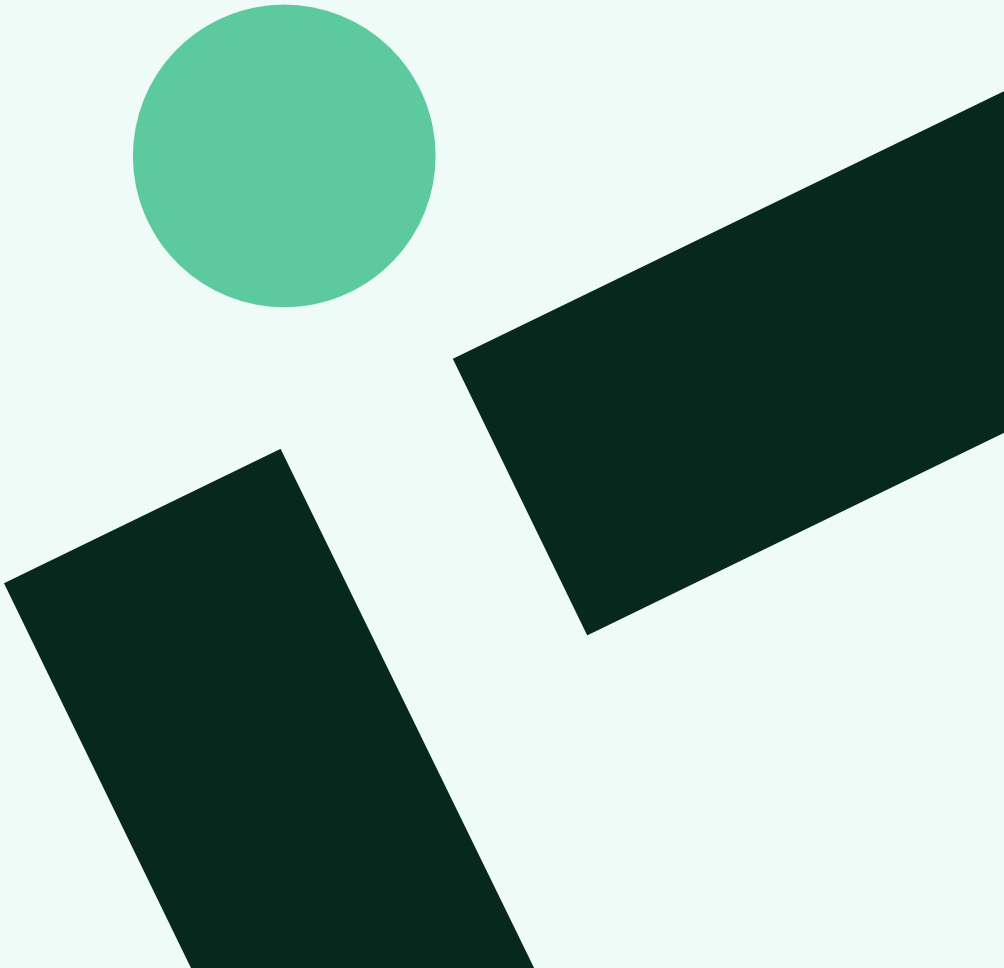
Con l'attuale turbolenza geopolitica e la possibilità di una guerra commerciale tra gli Stati Uniti e la Cina, il prezzo di tutto l'hardware informatico potrebbe aumentare in modo imprevedibile, così come i prezzi dei servizi cloud che comunque si basano su hardware, come qualsiasi altro software. Tuttavia, non c'è motivo di credere che Apple sia più esposta a questa minaccia di qualsiasi altro produttore. L'adozione di servizi ibridi e cloud è destinata a continuare, permettendo agli utenti e alle organizzazioni di scegliere il dispositivo locale in base alla preferenza personale piuttosto che alla compatibilità software. Questo potrebbe portare più utenti a scegliere dispositivi MacOS, poiché saranno compatibili con le applicazioni aziendali basate su cloud. Tuttavia, potrebbe anche ridurre la necessità di investire in hardware per endpoint, spingendo il mercato dei dispositivi aziendali ulteriormente verso dispositivi a basso costo/client sottili, allontanandosi dall'hardware premium come i Mac.

Man mano che l'adozione del cloud continua a crescere, gli attacchi contro i servizi cloud e le identità cresceranno anch'essi in popolarità. Pertanto, la minaccia fuori dal dispositivo è destinata a crescere per gli utenti di tutti i sistemi operativi, incluso MacOS. Il passaggio verso l'autenticazione multifattore (MFA) e le soluzioni di identità cloud significa che negli ambienti aziendali gli infostealer autonomi diventeranno meno efficaci, ma questo porterà probabilmente a un aumento degli attacchi di ingegneria sociale, poiché gli attaccanti che hanno rubato le credenziali cercheranno di superare le protezioni MFA.

Linux

Simile a MacOS, non ci sono segnali importanti che suggeriscano che la quota di mercato di Unix cambierà drasticamente entro il 2025. Un sistema operativo basato su Unix, Linux viene tipicamente utilizzato meno come endpoint/stazione di lavoro rispetto a Windows/MacOS e, pertanto, è principalmente mirato nella sua capacità di server o come ospite per i servizi software "on-premise".

Gli attori criminali sono capaci di lavorare su Linux, e molti attori ransomware hanno accesso a eseguibili di ransomware specifici per Linux. Linux è un sistema operativo popolare per i servizi di cloud computing in quanto è economico da distribuire e flessibile nel suo utilizzo. Questo vale sia per i servizi cloud "host" che per quelli "guest". Man mano che i servizi cloud diventano sempre più onnipresenti, potrebbe esserci un aumento dell'intento di attaccare i servizi "host" con l'obiettivo di compromettere informazioni o l'ambiente del "tenant" o "guest", ma è improbabile che questo diventi comune nel 2025. Probabilmente è una capacità attualmente riservata solo agli attori statali più avanzati.



Key Vectors

Phishing

Il phishing è il metodo più comune di ingegneria sociale. Definito nel contesto di questo rapporto come un messaggio elettronico che può essere trasferito attraverso diversi mezzi (anche se tipicamente tramite email) per raccogliere materiale di autenticazione o informazioni sensibili da una vittima.
L'ingegneria sociale rimarrà una minaccia significativa per tutte le organizzazioni nel 2025. Pochi controlli tecnici possono essere applicati per difendersi dagli attacchi di ingegneria sociale. Questo è possibile attraverso la rilevazione di anomalie e la rilevazione di frasi chiave, e diventerà meno difficile man mano che le implementazioni dei modelli linguistici di grandi dimensioni (LLM) matureranno. Tuttavia, il più capace arbitro di se un messaggio sia business as usual o un attacco di ingegneria sociale sarà spesso l'utente.

Entro il 2027, il numero di utenti di email aumenterà del 9%, arrivando a 4,9 miliardi, con un aumento simile nel numero di email ricevute ogni giorno, che arriveranno a 410 miliardi. Questo rappresenta un aumento annuale del 3%, in linea con l'aumento del 3% annuo dal 2018. Di conseguenza, nel 2025, l'email sarà il principale vettore di phishing. Detto ciò, altri formati di messaggistica stanno aumentando in popolarità tra gli attori delle minacce, e il mercato medio europeo dovrebbe essere consapevole della minaccia del phishing attraverso piattaforme di messaggistica come Microsoft Teams.

Il numero di SMS inviati ogni anno nel Regno Unito è diminuito dell'80%, passando da 151 miliardi a 36 miliardi tra il 2012 e il 2022. Tuttavia, sebbene il numero di SMS inviati possa essere diminuito, è molto probabile che il numero di dispositivi capaci di inviare SMS sia aumentato e che non diminuisca nel medio periodo. Pertanto, gli SMS rimarranno un mezzo di phishing valido, fino a quando non verranno più utilizzati dalle vittime come vettore MFA (autenticazione multifattore) o canale di comunicazione. È possibile che la comunicazione mobile basata su IP emerga come successore degli attacchi SMS, tuttavia ciò richiederà quasi sicuramente un modo migliore per legare l'identità del mondo reale a quella telefonica (attualmente rappresentata dai numeri di telefono).

Secondo Ofcom, l'uso dei "servizi di comunicazione online", che in questo contesto significa la messaggistica istantanea esclusa l'email, è aumentato del 1.300% passando da 100 miliardi di messaggi all'anno a 1,3 trilioni di messaggi all'anno tra il 2012 e il 2022, con un tasso di crescita sostenuto di circa il 10% all'anno dal 2018. Se il tasso di crescita continua nel medio periodo, potrebbe esserci un aumento superiore al 50% nell'uso della messaggistica di terze parti nei prossimi 5 anni. Pertanto, è probabile che il phishing tramite piattaforme di messaggistica di terze parti aumenti.

Non c'è motivo di credere che l'abuso di URL o allegati come payload dannosi diminuisca nel breve periodo. I tipi di payload dannosi che vengono consegnati riflettono tipicamente gli ambienti vittima più comuni (sistemi operativi, hardware, software) e la quota di mercato/-demografica dell'ambiente utente non cambia rapidamente. È probabile che ci siano picchi brevi quando vengono scoperti nuovi exploit relativi a determinati ambienti e vengono fortemente mirati, ma questi non avranno effetti a lungo termine sui payload.

Phishing con AI

Il NCSC del Regno Unito valuta che l'impatto dell'IA nei prossimi due anni (2024-2026) sarà tangibile, ma non rivoluzionario. Con questa valutazione concorda anche il team di Threat Intelligence di WithSecure.

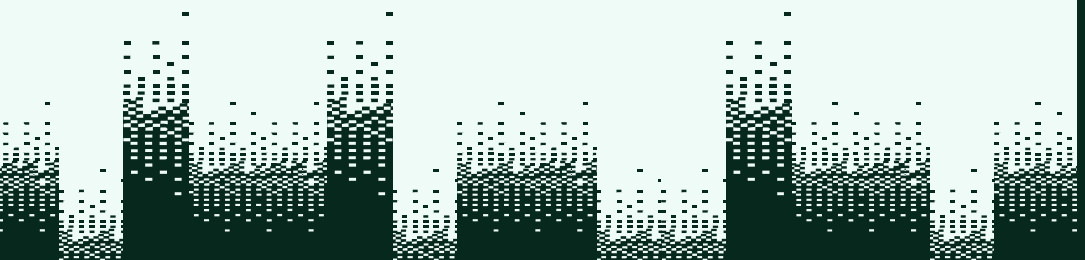
	Highly capable state threat actors	Capable state actors, commercial companies selling to states, organised cyber crime groups	Less-skilled hackers-for-hire, opportunistic cyber criminals, hacktivists
Intent	High	High	Opportunistic
Capability	Highly skilled in AI and cyber, well resourced	Skilled in cyber, some resource constraints	Novice cyber skills, limited resource
Reconnaissance	Moderate uplift	Moderate uplift	Uplift
Social engineering, phishing, passwords	Uplift	Uplift	Significant uplift (from low base)

Attacker in the Middle / MFA

L'Attacker in the Middle (AiTM) è una tecnica utilizzata dagli attaccanti per intercettare o manipolare i messaggi tra un utente legittimo e un servizio legittimo al fine di catturare credenziali, sessioni o token di Autenticazione a più fattori (MFA). Questa tecnica è il metodo più efficace per bypassare i controlli MFA ed è probabile che rappresenti uno dei principali vettori di attacco a cui il mercato medio europeo dovrà far fronte nel 2025.

Allo stesso tempo, le email di phishing per il furto di credenziali di base potrebbero diventare meno prevalenti come proporzione di tutti gli attacchi all'identità (in particolare gli attacchi AiTM), se l'MFA efficace diventerà il metodo predefinito e ci sarà una minore dipendenza dalle credenziali. Tuttavia, è importante notare che i nomi utente e le password non sono più l'unico metodo di autenticazione utilizzato nelle organizzazioni.

L'MFA è ancora in gran parte opzionale, non è implementato in molti processi di autenticazione e non mitiga il furto delle sessioni aperte. L'uso dell'autenticazione con passkey è ancora basso ma in aumento, con un'adozione che ha registrato un incremento del 400% nel 2024. L'uso delle Passkey è destinato a ridurre il numero degli attacchi di furto delle credenziali, ma potrebbe portare a un aumento degli attacchi di malware e ingegneria sociale. Gli attacchi AiTM che mirano specificamente all'autenticazione tramite passkey sono già stati dimostrati dai ricercatori, ma non sono ancora comuni "nel mondo reale".



Compromissione di Account Aziendali

Gli attacchi di Business Account Compromise (BAC) sono una forma di attacco phishing che sfrutta le relazioni di fiducia esistenti. Gli attacchi Business Email Compromise (BEC) rappresentano un sottoinsieme del BAC. Un attacco BAC si verifica quando un attore malevolo ottiene l'accesso a un account di messaggistica utilizzato da un'entità aziendale e lo utilizza per inviare ulteriori messaggi di phishing ai normali interlocutori di quell'account.

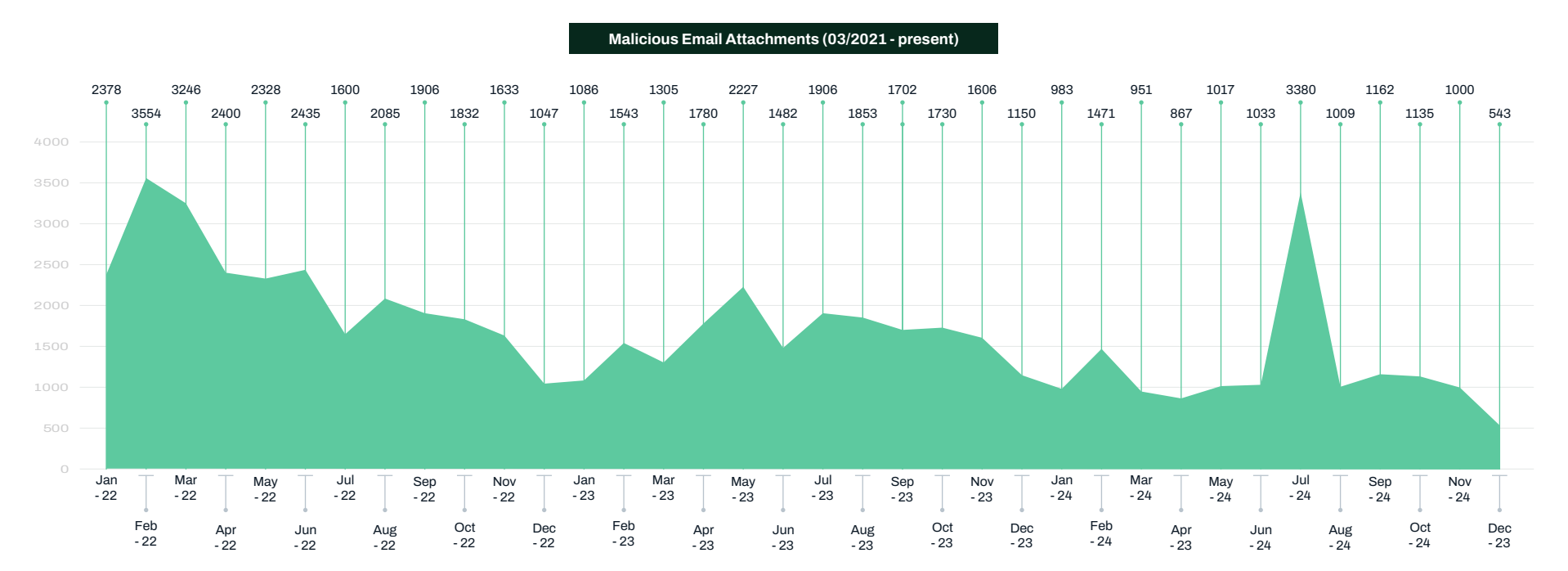
Una volta ottenuto l'accesso alla casella di posta, l'attaccante cercherà di modificare le fatture con dati bancari falsi, al fine di dirottare pagamenti legittimi. Gli attacchi BEC/BAC possono essere redditizi quanto le operazioni di ransomware, con frequenti segnalazioni di perdite a otto cifre per le organizzazioni coinvolte.

Man mano che i controlli antimalware sui canali di messaggistica diventano più efficaci, gli attacchi BAC acquisiranno un valore ancora maggiore per gli attaccanti. Questo è particolarmente vero per gli attacchi basati esclusivamente sull'ingegneria sociale, in cui non sono presenti indicatori tecnici che possano aiutare il sistema di messaggistica del destinatario a stabilire la legittimità del messaggio.

Per questo motivo, il BAC rappresenta una minaccia molto elevata per il mid-market europeo nel 2025, in quanto continuerà a offrire agli attori malevoli un modo economico e tecnicamente poco sofisticato per sottrarre somme estremamente elevate alle vittime.

Malspam

Man mano che le tecnologie e i controlli di protezione contro email e malware sono avanzati, gli attori malevoli utilizzano sempre più tecniche di ingegneria sociale per diffondere malware, anziché allegarlo direttamente all'email.



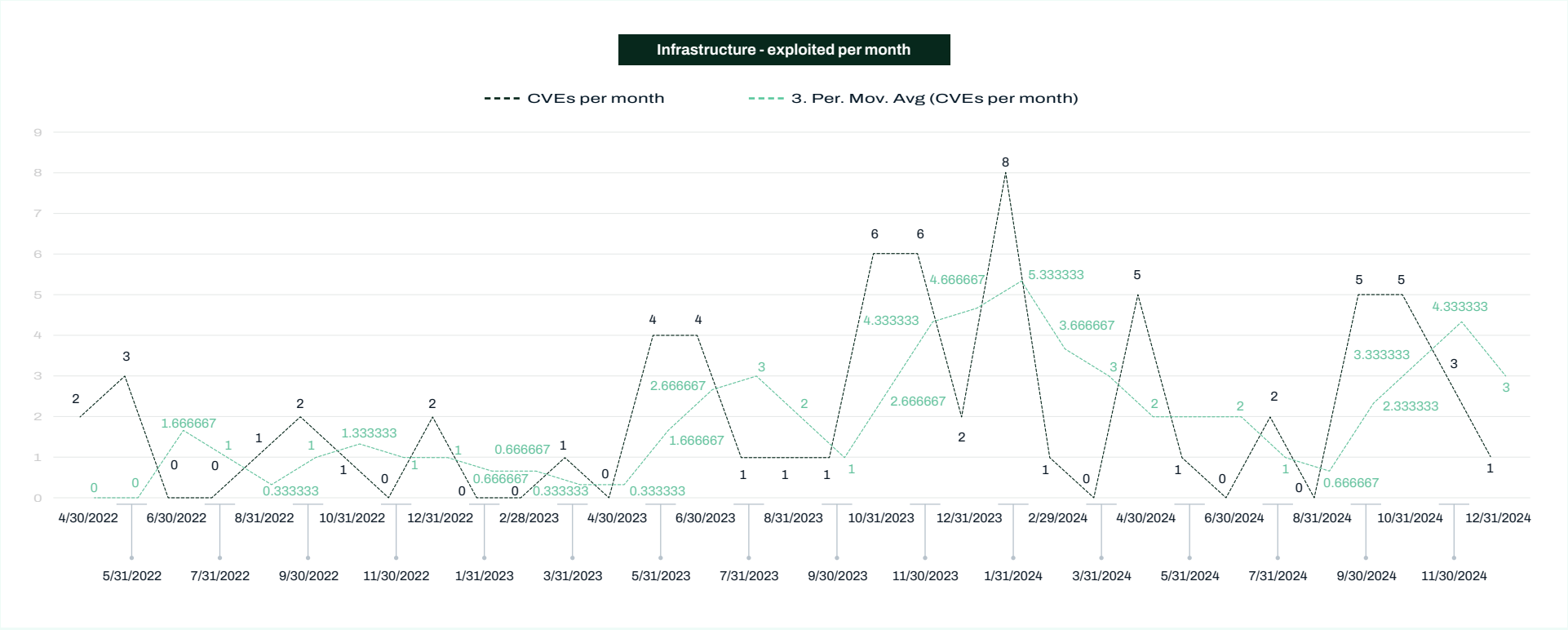
Questo può assumere la forma di allegati email apparentemente innocui che mirano a reindirizzare le vittime una o più volte prima che venga scaricato il payload finale. In generale, la separazione tra gli elementi malevoli e il messaggio iniziale dell'attaccante è progettata per impedire ai sistemi di sicurezza email di individuare con successo gli obiettivi dannosi, ma si basa su tattiche di ingegneria sociale per risultare efficace. Questo concetto è particolarmente evidente nelle campagne malware che hanno dominato il panorama degli infostealer nella seconda metà del 2024.

Gli attori stanno impiegando esche più innovative come i falsi "click per risolvere" o i "fake CAPTCHA" – a dimostrazione della necessità di utilizzare tecniche di ingegneria sociale sempre più creative – che spesso si rivelano efficaci. Per questo motivo, è quasi certo che la minaccia rappresentata dalle campagne malware su larga scala basate su messaggi sia bassa per le organizzazioni dotate di strumenti di sicurezza adeguati. Tuttavia, i servizi di messaggistica verranno comunque utilizzati per coinvolgere il mid-market europeo in campagne di ingegneria sociale che potrebbero comunque portare all'infezione con gli stessi malware.

Infrastructure Service Exploitation

I servizi di Edge e Infrastruttura sono definiti come quei servizi esposti a Internet, progettati per facilitare l'ingresso/l'uscita di utenti, dati o istruzioni. I dispositivi di infrastruttura possono anche essere considerati l'hardware di rete che supporta l'infrastruttura IP. Nel corso del 2024, le vulnerabilità nei servizi Edge/Infrastruttura sono state citate come il principale vettore di accesso iniziale, laddove il vettore era noto.

Nel 2024, WithSecure Threat Intelligence ha pubblicato una valutazione sulla minaccia rappresentata dagli attori in grado di sfruttare vulnerabilità nei servizi edge, spesso su larga scala. La ricerca ha rilevato che, dal 2022 fino al 2024, il numero di vulnerabilità di infrastruttura attivamente sfruttate è aumentato mediamente ogni anno. Sebbene il volume di vulnerabilità sfruttate abbia raggiunto il picco all'inizio del 2024, l'elevata frequenza di tali campagne di sfruttamento può ora essere considerata la nuova normalità per il 2025.



La minaccia derivante dallo sfruttamento delle infrastrutture è così grave che, a dicembre 2024, si riporta che gli Stati Uniti stanno considerando il divieto di un particolare marchio di apparecchiature di routing, TP-Link. Questo è quasi certamente dovuto al numero di vulnerabilità di sicurezza presenti nei dispositivi, alla percezione di una scarsa collaborazione con i ricercatori di sicurezza e alla debole risposta nella risoluzione di tali problemi.

Numerosi commentatori hanno sollevato preoccupazioni riguardo alla qualità del codice in molti servizi di infrastruttura aziendale. Quando ciò si combina con la presenza di numerosi attori delle minacce e ricercatori di sicurezza che conducono attivamente ricerche sulle vulnerabilità di tali dispositivi, esiste quasi certamente un'ampia superficie di attacco e un numero crescente di attori con capacità e intenzione di sfruttarla.

Il targeting delle infrastrutture è spesso indiscriminato ed è parte integrante della kill chain degli attori motivati finanziariamente. Si tratta, quindi, di una minaccia significativa per il mid-market europeo.

Supply Chain

L'incidente SolarWinds del 2020 ha portato la minaccia alla supply chain all'attenzione dell'opinione pubblica. Da allora, ci sono stati numerosi attacchi alla supply chain con un impatto significativo, per lo più rivolti al processo di build di software legittimo, che viene poi distribuito e firmato come software autentico agli utenti.

Un'altra forma di attacco alla supply chain consiste nel colpire servizi esternalizzati in modo da influenzare le organizzazioni "a valle". Un esempio rilevante è rappresentato dalla campagna MOVEit del 2023, in cui servizi di trasferimento file gestiti sono stati attaccati su larga scala, portando al furto di dati da parte di centinaia di organizzazioni in tutto il mondo.

Questo attacco in particolare è stato condotto da un collettivo ransomware, che continuerà anche nel 2025 a prendere di mira servizi esposti pubblicamente, come le soluzioni per il trasferimento di file.

Service providers

Il targeting dei fornitori di servizi (inclusi i provider di servizi cloud) rappresenta un metodo efficace per colpire un'organizzazione. In generale, la minaccia per un'organizzazione europea "tipica" di fascia media derivante da un attacco altamente mirato a fornitori di servizi specifici è bassa, poiché questi attacchi sono solitamente riservati agli attori più capaci. Un esempio è il caso Microsoft, scoperto a gennaio 2024.

Tuttavia, numerose piccole e medie imprese sono state impattate indirettamente attraverso attacchi alla supply chain non mirati. Due esempi rilevanti sono:

La compromissione di Okta nel 2023, un fornitore di servizi di identità.

Una campagna contro una vulnerabilità in ScreenConnect, uno strumento di gestione remota, utilizzato dai fornitori di servizi gestiti. Questo attacco ha colpito molti clienti WithSecure ed è stato di tipo opportunistico.

Esiste un livello di fiducia intrinseco tra fornitori di servizi e clienti, ed è quasi certo che esistano vulnerabilità intrinseche nei prodotti dei fornitori di servizi (inclusi quelli SaaS) che saranno sfruttate nel 2025.

Sebbene non sia possibile prevedere con certezza quali prodotti specifici saranno presi di mira, si può affermare con alta confidenza che la minaccia di attacchi alla supply chain per il mid-market europeo nel 2025 è elevata.

Software Supply Chain

Verso la seconda metà del 2024, WithSecure Threat Intelligence ha osservato un aumento delle segnalazioni relative a supply chain del software compromesse. Attraverso attacchi in stile pseudo-watering hole, gli attori malevoli stanno prendendo di mira sviluppatori e, in misura minore, settori specifici, pre-posizionando librerie software che possono essere importate ed eseguite dagli sviluppatori stessi.

Questo consente agli attaccanti di eseguire codice dannoso in un modo che aggira alcuni strumenti anti-malware e meccanismi di application allowlisting. Inoltre, rappresenta un metodo per colpire in modo relativamente indiscriminato utenti ad alto privilegio (come gli sviluppatori) e gli ambienti di sviluppo.

Sono stati scoperti numerosi pacchetti software malevoli in repository open-source, in particolare PyPi e NPM, ed è quasi certo che altri verranno scoperti nel 2025. Questi pacchetti contengono spesso elementi infostealer, volti a rubare credenziali e chiavi di ambiente.

Il vero impatto di questa minaccia potrebbe non essere ancora pienamente compreso, poiché è estremamente difficile attribuire con certezza gli impatti successivi — derivanti dall'uso di materiale rubato — al pacchetto malevolo originario.

La vulnerabilità Log4j del 2021 ha evidenziato chiaramente che molte organizzazioni non hanno piena consapevolezza delle librerie software open-source vulnerabili (o dannose) presenti nel proprio software aziendale.

Pertanto, è probabile che la minaccia alla supply chain software per il mid-market europeo sarà significativa nel 2025.

Legitimate Tooling

Nel corso del 2024, WithSecure Threat Intelligence ha osservato un aumento nell'uso di strumenti legittimi per scopi illegittimi. Questo non è una tattica nuova adottata dagli attori malintenzionati; da tempo, infatti, vengono sfruttate le funzioni di risposta alle abusi inadeguate dei servizi di distribuzione dei contenuti (come Cloudflare) per ospitare e offuscare l'infrastruttura utilizzata. Strumenti legittimi di Remote Management and Monitoring (RMM) sono ora frequentemente utilizzati nelle operazioni di ransomware. Questo trend continuerà anche nel 2025, quasi certamente a causa del fatto che tali strumenti sono legittimamente utilizzati. Sebbene uno strumento RMM svolga gli stessi compiti dei remote access trojans (RAT), esso può bypassare gli strumenti di sicurezza anti-malware, funziona bene con il comune lancio di phishing legato al supporto IT e, in alcune versioni di Windows, è addirittura preinstallato.

Questa crescente adozione di strumenti legittimi a scopi dannosi è una tendenza che continuerà a presentare sfide significative nella protezione delle organizzazioni, poiché la difficoltà nel rilevare tali strumenti da parte delle difese tradizionali li rende particolarmente attraenti per i malintenzionati.

Cloud services

Questa tattica è destinata a espandersi nel 2025, poiché le infrastrutture compromesse o nuovamente create sui servizi Cloud più comuni inizieranno a sostituire molti domini appena registrati o infrastrutture virtuali basate su IP grezzi. Ciò rappresenta una sfida significativa per i difensori delle reti, poiché mina il rilevamento di domini maligni basato sugli attributi di tali domini. È molto più difficile per un analista umano identificare un URL maligno che fa parte di un'infrastruttura conosciuta, utilizzata e legittima. I Cloud Service Providers (CSP) invitano gli utenti a fidarsi esplicitamente della loro infrastruttura di archiviazione, il che diventa problematico quando istanze compromesse o maligne di tali servizi vengono sfruttate in attacchi.

Questa tattica è stata osservata almeno dal 2018, tuttavia, in generale, con l'aumento dell'adozione del cloud, l'abuso di questi stessi servizi aumenterà di pari passo. È quasi certo che questo vettore sarà in parte mitigato grazie alle capacità di fiducia e sicurezza interne dei principali CSP, ma rappresenta comunque un altro esempio di outsourcing involontario della visibilità e delle capacità di sicurezza informatica.

Man mano che i servizi Cloud diventano sempre più diffusi nel mercato medio nel 2025, gli attori delle minacce sfrutteranno sempre di più le capacità che questi servizi offrono nelle loro reti per eseguire altre attività illecite. Piuttosto che introdurre strumenti errati (come RClone/MEGAsync), è stato osservato che gli attori del ransomware utilizzano capacità native del cloud, come nel caso di Azure Storage Explorer, per esfiltrare dati verso tenant controllati dagli attaccanti. Questo principio può essere esteso a molte funzionalità legittime dei servizi cloud, e sebbene ciò fornisca capacità efficaci e furtive per gli attaccanti, rimarrà un vettore di attacco valido e sempre più popolare.

Outsourcing control

Un modo relativamente nuovo per colpire un'organizzazione è attraverso il targeting del loro Cloud Service Provider. Questo è stato realizzato nel 2024, quando le organizzazioni sono state impattate dalla compromissione di Microsoft da parte di un gruppo di intrusione russo. Le vittime sono quasi interamente incapaci di mitigare questo rischio in modo isolato e, in alcuni casi, non avevano un valore contrattuale sufficientemente alto da consentire loro l'accesso ai log necessari per fare audit su chi avesse avuto accesso ai loro dati.

Seppure questo rappresenti un problema allarmante per alcune organizzazioni e debba servire da promemoria che l'utilizzo dei servizi cloud outsourcing il controllo, è improbabile che rappresenti una minaccia sistemica per il mercato medio europeo nel 2025. Questo perché gli attori che sono in grado di portare un tale livello di capabilità sono quasi sicuramente più concentrati su obiettivi specifici, mirando a organizzazioni particolari.

Le organizzazioni nel mercato medio europeo che potrebbero essere targetizzate da tali attori sono outliers e dovrebbero adottare propri processi di modellizzazione delle minacce per mitigare questo rischio.

Social Engineering

C'è stato un impegno concertato e costante per formare gli utenti a comprendere e riconoscere azioni non sicure o social engineering (ad esempio, riconoscere una email di phishing). Sebbene questo rimanga un problema persistente, i successi in quest'area sono basati sul fatto che gli utenti hanno una comprensione adeguata (anche se ancora estremamente limitata) del funzionamento di un sistema operativo moderno.

Con il passaggio ai servizi Cloud, dove la complessità è nascosta all'utente, questo sforzo di educazione degli utenti è in qualche modo compromesso. Gli utenti che ora possono riconoscere email di phishing relative alle password, potrebbero non essere in grado di definire o riconoscere il consent phishing. Questo aumenterà la capacità degli attori di compiere attacchi di social engineering man mano che i servizi Cloud saranno adottati sempre di più nel 2025 e oltre.

Driver vulnerabili e strumenti AV

L'uso di driver legittimi, ma intrinsecamente vulnerabili, con l'intento di disabilitare gli strumenti di sicurezza, è noto come attacco Bring Your Own Vulnerable Driver (BYOVD). Questo è stato un vettore comune nel corso del 2024 da parte degli attori ransomware, che cercavano di manomettere i prodotti EDR. Strumenti legittimi e gratuiti per la rimozione di rootkit sono stati anch'essi utilizzati per fermare i servizi EDR.

Questo rappresenta una sfida per gli strumenti di sicurezza, poiché tali driver erano spesso software legittimi, firmati, il che significa che la rilevazione dipende spesso da misure euristiche che potrebbero non essere complete come altre logiche di rilevazione ad alta fedeltà.

Malware

Infostealers

Questo rapporto ha osservato l'emergere degli infostealers come una minaccia principale del malware, catalizzata dal cambiamento dei servizi off-premises che spostano il campo di battaglia verso l'identità. Gli infostealers sono facilmente disponibili per i criminali, spesso "licenziati" per una quota mensile relativamente esigua. Gli infostealers sono in costante sviluppo, con regolari miglioramenti in termini di furtività e funzionalità.

Gli attori degli infostealers hanno frequentemente mostrato modi innovativi e progressivi per infettare il computer di una vittima, utilizzando tecniche di social engineering nuove e infezioni in stile watering hole (esplorato sotto la sezione 'Attacchi in stile Watering Hole').

WithSecure ha notato infezioni frequenti e di successo di malware infostealer tra i suoi clienti. È altamente probabile che la maggior parte dei sistemi EDR/EPP aziendali sia abbastanza efficace da rilevare e prevenire la maggior parte delle attività degli infostealer. Tuttavia, questo dipende spesso dalla copertura completa di EDR/EPP e dall'azione tempestiva su ogni "alert". È spesso molto difficile associare un incidente (ad esempio, un evento di ransomware) a un evento iniziale di furto delle credenziali, rendendo difficile applicare una quantificazione generale all'impatto del furto dei materiali di autenticazione.

In-browser

Gli attacchi ai browser sono sempre più comuni poiché essi rappresentano a) un deposito prezioso di materiale sensibile e b) vengono utilizzati sempre più frequentemente come interfaccia con ambienti SaaS (client leggeri). I plugin dei browser possono esistere al di fuori della visibilità degli strumenti di sicurezza e hanno la capacità di accedere e compiere una serie di attività dannose, come la raccolta di dati sensibili, l'installazione di malware o il reindirizzamento degli utenti. Come estensione del principio della supply chain del software, le estensioni dei browser possono anche essere installate da repository non affidabili, dando agli attori delle minacce l'opportunità di distribuire elementi eseguibili maligni che potrebbero eludere controlli come la whitelisting delle applicazioni.

Social Engineering

Gli strumenti di sicurezza sono in fase di sviluppo attivo da molti anni e sono sempre più capaci di contrastare le tecniche di accesso iniziale più comuni e conosciute. Questo lascia agli attori delle minacce due principali opzioni per aggirare gli strumenti di sicurezza: 1.) cercare di disabilitare o eludere gli strumenti di sicurezza, 2.) impiegare tecniche di ingegneria sociale.

Per quanto riguarda l'accesso iniziale, il tradizionale approccio era la consegna tramite malspam. Questo è diventato in gran parte inefficace, poiché i progressi negli strumenti di sicurezza delle email e anni di formazione degli utenti hanno ridotto la capacità di tali allegati email di raggiungere l'utente finale. È probabile che nel 2025 continueremo a osservare un cambiamento di paradigma, da un modello in cui un elemento maligno (come un file binario, un link, ecc.) viene "spinto" verso una vittima, a uno in cui la vittima è "indotta" a prelevare un elemento maligno dall'attaccante, tramite tecniche di ingegneria sociale. Questi attacchi possono essere paragonati a quelli watering hole, in cui le vittime vengono indirizzate verso risorse maligne preesistenti.

‘Watering hole’ Style Attacks

Gli attori delle minacce sono stati osservati da WithSecure nel distribuire pagine web che si spacciano per pagine di download di software gratuito o open source. Le vittime potenziali vengono indirizzate verso queste pagine utilizzando vari metodi, tra cui, ma non limitati a: offerte di lavoro false, annunci maligni, commenti su forum/video o attraverso l'uso di ottimizzazione per i motori di ricerca.

La supply chain di software è una tattica preoccupante di proliferazione del malware che possiamo considerare uno stile "watering hole", trattato in dettaglio nella sezione Supply Chain. Gli attori delle minacce sono stati osservati nel tentativo di costringere le vittime ad eseguire involontariamente tale codice tramite il typo squatting (utilizzo di nomi di pacchetti errati) o suggerendo aggiunte o correzioni al codice su piattaforme/forum di coding collaborativo.

Conclusioni

Il cyberspazio è stato estremamente turbolento nel 2024, e il modo in cui le minacce operano e si manifestano è in costante cambiamento ed evoluzione. Questi cambiamenti ed evoluzioni sono guidati da stimoli legati a fattori politici, economici, ideologici e tecnologici. Con l'avvicinarsi del 2025, è quasi certo che tutti questi fattori saranno cambiati e si saranno evoluti rispetto all'ambiente in cui ci troviamo attualmente a dicembre 2024.

Il crimine informatico rappresenta la terza economia più grande al mondo, le vittime di ransomware sono probabilmente in aumento, e le relazioni geopolitiche sono tese. La società sta diventando sempre più digitalizzata e interconnessa. Non sorprende che il CEO del NCSC del Regno Unito abbia dichiarato pubblicamente che il rischio che affronta il Paese è "ampiamente sottovalutato". Lo stesso vale anche per altri Paesi europei.

Le organizzazioni del mercato medio europeo si trovano ad affrontare un ampio spettro di minacce, con obiettivi diversi, tecniche, tattiche e procedure differenti, e vari gradi di sofisticazione. Per restare al passo con queste minacce, i team di sicurezza devono assicurarsi di poter operare nel modo più proattivo possibile, per garantire che le contromisure adottate contro minacce in continua evoluzione non diventino progressivamente obsolete.

Informazioni su WithSecure™

WithSecure™, precedentemente nota come F-Secure Business, è il partner europeo di riferimento per la cybersicurezza. È un marchio di fiducia per i fornitori di servizi IT, MSSP e aziende di tutto il mondo, offrendo soluzioni di cybersicurezza orientate ai risultati, pensate per proteggere le aziende di medie dimensioni. Con un forte impegno verso il modello europeo di protezione dei dati, WithSecure™ pone al centro la privacy, la sovranità dei dati e la conformità normativa.

Con oltre 35 anni di esperienza nel settore, WithSecure™ ha sviluppato un portfolio pensato per affrontare il cambiamento di paradigma dalla cybersicurezza reattiva a quella proattiva. In linea con il proprio impegno verso una crescita collaborativa, offre ai propri partner modelli commerciali flessibili, assicurando un successo reciproco nel dinamico panorama della sicurezza informatica.

Al cuore delle soluzioni innovative di WithSecure™ c'è Elements Cloud, una piattaforma che integra perfettamente tecnologie basate sull'intelligenza artificiale, competenze umane e servizi di co-security. Questa soluzione consente alle aziende del mid-market di accedere a funzionalità modulari che includono la protezione degli endpoint e del cloud, il rilevamento e la risposta alle minacce, e la gestione dell'esposizione.

WithSecure™ Corporation è stata fondata nel 1988 ed è quotata alla borsa NASDAQ OMX di Helsinki.