APT groups: i cybercriminali più influenti e le tecniche e tattiche utilizzate nel cybercrime



Il panorama del cybercrime contemporaneo si è evoluto in una complessa architettura criminale caratterizzata da organizzazioni altamente strutturate, tecnologie sofisticate e metodologie in costante evoluzione. L'analisi delle minacce informatiche del 2025 rivela un ecosistema criminale sempre più efficiente che utilizza automazione, intelligenza artificiale e ingegneria sociale avanzata per scalare gli attacchi e massimizzare l'impatto.

La ricerca condotta dai principali organismi di sicurezza informatica evidenzia come gli attacchi ransomware siano cresciuti del 10% e le violazioni dei dati del 6%, mentre oltre 3,2 miliardi di credenziali sono state compromesse nel 2024, alimentando un'ampia gamma di attività criminali informatiche. Questo scenario delinea un paradigma criminale dove l'intelligenza artificiale generativa emerge come nuovo strumento strategico per gli attori delle minacce statali, i cybercriminali, gli hacktivisti e altri soggetti malintenzionati.

I gruppi Advanced Persistent Threat (APT) più influenti

Fancy Bear (APT28/Forest Blizzard)

Il gruppo di avversari stato-nazionali noto come FANCY BEAR (anche conosciuto come APT28 o Sofacy) opera almeno dal 2008 e

rappresenta una minaccia costante per un'ampia varietà di organizzazioni in tutto il mondo. Attribuito al servizio di intelligence militare russo GRU, questo gruppo prende di mira settori aerospaziale, difesa, energia, governo, media e dissidenti, utilizzando un impianto sofisticato e multi-piattaforma.

Le tattiche operative di Fancy Bear includono l'utilizzo di domini typosquatted che imitano strettamente quelli delle organizzazioni target, permettendo la creazione di siti di phishing convincenti. Il loro arsenale tecnologico comprende strumenti proprietari come XAgent, XTunnel, WinIDS, Foozer e DownRange, che forniscono capacità avanzate di esfiltrazione dati, evasione del rilevamento e distribuzione di malware aggiuntivo.

Cozy Bear (APT29/Midnight Blizzard)

Cozy Bear è un gruppo di hacker russi presumibilmente affiliato a una o più agenzie di intelligence russe, identificato da Mandiant come il gruppo Advanced Persistent Threat APT29. Secondo le valutazioni del Dutch General Intelligence and Security Service (AIVD), il gruppo è guidato dal Servizio di Intelligence Estera russo (SVR).

Cozy Bear è un'operazione di cyber-spionaggio ben finanziata, altamente dedicata e strutturata che si ritiene operi per la Federazione Russa almeno dal 2008 per raccogliere intelligence a supporto del processo decisionale di politica estera e di sicurezza. Il gruppo dimostra una fiducia inusuale nella propria capacità di compromettere efficacemente i propri obiettivi e di operare senza essere rilevato.

L'ecosistema Ransomware-as-a-Service (RaaS)

LockBit: l’egemonia criminale

Nel 2022, LockBit è stato il ransomware più distribuito al mondo e continua a essere prolifico nel 2023. Dal gennaio 2020, gli affiliati che utilizzano LockBit hanno attaccato organizzazioni di varie dimensioni in una serie di settori di infrastrutture critiche, tra cui servizi finanziari, alimentazione e agricoltura, istruzione, energia, governo e servizi di emergenza, sanità, produzione e trasporti.

Il modello operativo di LockBit come Ransomware-as-a-Service presenta caratteristiche innovative: gli affiliati ricevono i pagamenti del riscatto prima di inviare una percentuale al gruppo principale, una pratica che contrasta nettamente con altri gruppi RaaS che si pagano prima e poi distribuiscono la percentuale degli affiliati.

Nonostante l’Operazione Cronos del febbraio 2024, che ha portato al sequestro dell’infrastruttura di LockBit, il presunto leader di LockBit insiste che, nonostante la battuta d’arresto, non ha finito e promette di continuare la sua ondata di attacchi.

RansomHub e Cicada3301: i nuovi protagonisti

RansomHub e Cicada3301 saranno “gruppi ransomware chiave da osservare” nel 2025. Entrambi i gruppi hanno lanciato le loro operazioni RaaS nel 2024, reclutando con successo diversi team di affiliati esperti e di alto livello per supportare i loro sforzi di estorsione.

Entrambi i gruppi hanno legami con BlackCat/ALPHV, con affiliati umani sovrapposti e somiglianze nel codice nei loro payload ransomware. RansomHub ha attirato molti affiliati BlackCat dopo lo scioglimento del gruppo all’inizio del 2024, utilizzando strumenti di evasione EDR iper-adattivi e persistenti come EDRKillShifter.

Tecniche e tattiche nel framework MITRE ATT&CK

Metodologie di accesso iniziale

L’abuso di account validi è rimasto il punto di ingresso preferito negli ambienti delle vittime per i cybercriminali nel 2024, rappresentando il 30% di tutti gli incidenti a cui X-Force ha risposto. Parallelamente, il phishing è emerso come vettore di infezione ‘ombra’ per gli attacchi di identità, con X-Force che ha osservato un aumento dell’84% delle email di phishing che distribuiscono infostealer su base settimanale.

Social engineering e manipolazione psicologica

Il 94% delle aziende ha riferito di aver subito un attacco di phishing nel 2024, con la maggior parte di esse che ha subito impatti negativi da questi attacchi. La ricerca evidenzia che il tempo mediano per gli utenti di cadere nelle email di phishing è inferiore a 60 secondi, con un tempo mediano di 21 secondi per cliccare su un link malevolo dopo l’apertura dell’email.

Tecniche di evasione e persistenza

I cybercriminali impegnati in attacchi di tipo intrusione hanno fatto un uso limitato dell’intelligenza artificiale. La maggior parte dell’uso dell’IA generativa da parte dei cybercriminali si è concentrata su compiti di ingegneria sociale: creazione di immagini, video e testi per profili falsi, e per l’uso nella comunicazione con gli obiettivi per mascherare problemi di fluenza linguistica e identità.

Evoluzione delle minacce e intelligenza artificiale

Impatto dell’IA generativa sul cybercrime

Da profili fittizi a email e siti web generati dall’IA, avversari come FAMOUS CHOLLIMA stanno utilizzando l’IA generativa per potenziare le minacce interne e l’ingegneria sociale. Con l’inganno potenziato dall’IA che diventa più convincente, le organizzazioni devono evolvere le loro difese.

L’IA generativa sta emergendo come una nuova e crescente aggiunta alla cassetta degli attrezzi degli attori delle minacce sostenuti da stati-nazione, cybercriminali, hacktivisti e altri. Questi avversari sono adottatori entusiasti, specialmente quando lanciano campagne di ingegneria sociale e operazioni informative ad alto ritmo.

Infostealer e compromissione delle credenziali

I malware infostealer hanno rappresentato il 75% delle credenziali rubate nel 2024, infettando oltre 23 milioni di dispositivi in tutto il mondo. Questa tendenza alimenta direttamente l’ecosistema ransomware, poiché i gruppi ransomware-as-a-service (RaaS) sono responsabili di quasi la metà di tutti gli attacchi.

Analisi settoriale delle minacce

Infrastrutture critiche e sanità

La ricerca mostra che LockBit, Conti, SunCrypt, ALPHV/BlackCat e Hive sono emersi come i principali cinque gruppi ransomware-as-a-service (RaaS) che hanno impattato il settore sanitario e della salute pubblica durante i primi tre mesi dell’anno.

Targeting geografico e geopolitico

A livello globale, gli attacchi informatici contro la sicurezza pubblica sono aumentati del 64% nel 2023, mentre gli attacchi ransomware alle organizzazioni di sicurezza pubblica statunitensi sono aumentati del 63% nel 2023, guidati da un

aumento del 157% nel numero di gruppi di estorsione che conducono tali attacchi.

Metodologie di difesa e mitigazione

Implementazione del framework MITRE ATT&CK

Il framework MITRE ATT&CK cataloga le tattiche, tecniche e procedure (TTP) dei cybercriminali attraverso ogni fase del ciclo di vita dell'attacco informatico, dalla raccolta iniziale di informazioni e dai comportamenti di pianificazione dell'attaccante, fino all'esecuzione finale dell'attacco.

Il framework organizza 14 tattiche principali che includono ricognizione, sviluppo delle risorse, accesso iniziale, esecuzione, persistenza, escalation dei privilegi, evasione delle difese, accesso alle credenziali, scoperta, movimento laterale, raccolta, comando e controllo, esfiltrazione e impatto.

Strategie di threat hunting

Il framework MITRE ATT&CK serve come strumento fondamentale per la caccia alle minacce, in particolare nell'analisi del traffico di rete, nell'analisi dei log di sistema e nella modellazione dei grafi di attacco. La ricerca evidenzia l'integrazione di tecnologie di elaborazione del linguaggio naturale (NLP) e machine learning (ML) con ATT&CK per migliorare il rilevamento del comportamento avversario e la risposta alle minacce.

Tendenze emergenti e previsioni per il 2025

Supply chain attacks e compromissioni della catena di fornitura

Gli attacchi informatici alla catena di fornitura sono emersi

come una delle minacce più significative alla sicurezza informatica globale nel 2024, aumentando del 68% rispetto al 2023. Il costo globale degli attacchi alla catena di fornitura software è previsto aumentare da 46 miliardi di dollari nel 2023 a 138 miliardi di dollari entro il 2031.

Vulnerabilità IoT e 5G

Con l'accelerazione dell'adozione del 5G, i cybercriminali stanno spostando la loro attenzione sulle vulnerabilità dell'Internet delle Cose (IoT), sfruttando i dispositivi intelligenti non sicuri per ottenere l'accesso alla rete. La rapida espansione dei dispositivi abilitati al 5G significa più endpoint connessi, aumentando le superfici di attacco per le minacce informatiche.

Raccomandazioni strategiche per la cyber resilienza

Autenticazione multi-fattore e controlli di identità

È necessario espandere significativamente l'uso dell'MFA: dare priorità all'MFA per tutti i dipendenti e partner che accedono ai sistemi. Questo fornisce un livello extra di protezione per applicazioni e servizi di rete, anche se le password sono compromesse.

Intelligenza delle minacce proattiva

Il rapporto GTIR 2025 di Flashpoint raccomanda una strategia di sicurezza proattiva e guidata dall'intelligence per rimanere avanti rispetto alle minacce. Le organizzazioni devono implementare un monitoraggio continuo dei mercati illeciti online e dei forum per le credenziali aziendali compromesse.

Conclusioni e prospettive future

L’analisi del panorama del cybercrime del 2025 rivela un ecosistema criminale in rapida evoluzione, caratterizzato da una crescente sofisticazione tecnica e organizzativa. La convergenza tra attori stato-nazionali e gruppi criminali, l’integrazione dell’intelligenza artificiale nelle tattiche di attacco e la proliferazione del modello RaaS stanno ridefinendo le dinamiche delle minacce informatiche.

La necessità di collaborazione tra team di sicurezza del settore privato, agenzie governative e organizzazioni di intelligence globali non è mai stata così grande. Le organizzazioni devono adottare un approccio olistico alla sicurezza informatica che integri intelligence delle minacce, monitoraggio in tempo reale e strategie difensive adattive.

Il framework MITRE ATT&CK emerge come strumento fondamentale per standardizzare la comprensione delle tattiche avversarie e facilitare la condivisione di intelligence tra settori. L’implementazione di controlli di sicurezza basati su evidenze, combinata con tecnologie di rilevamento comportamentale e analisi predittiva, rappresenta la frontiera della cyber resilienza organizzativa.

La sfida principale per il 2025 risiede nella capacità delle organizzazioni di anticipare e mitigare minacce in costante evoluzione, mantenendo un equilibrio tra innovazione tecnologica e sicurezza operativa. Solo attraverso un approccio proattivo, collaborativo e scientificamente informato sarà possibile contrastare efficacemente l’escalation del cybercrime contemporaneo.

Fonti

CrowdStrike 2025 Global Threat Report. https://www.crowdstrike.com/en-us/global-threat-report/

KELA Cyber Threat Intelligence, The State of Cybercrime 2025 Report. https://www.kelacyber.com/resources/research/state-of-cybercrime-2025/

CyberProof 2025 Global Threat Intelligence Report. https://www.cyberproof.com/blog/cyberproof-2025-global-threat-intelligence-report-mapping-threats-and-trends/

IBM X-Force 2025 Threat Intelligence Index. https://www.ibm.com/reports/threat-intelligence

Flashpoint 2025 Global Threat Intelligence Report. https://www.hstoday.us/subject-matter-areas/cybersecurity/2025-global-threat-intelligence-report-highlights-rising-cybersecurity-challenges/

CISA Understanding Ransomware Threat Actors: LockBit. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a

MITRE ATT&CK Framework. https://attack.mitre.org/

Sophos Annual Threat Report: Cybercrime on Main Street 2025. https://news.sophos.com/en-us/2025/04/16/the-sophos-annual-threat-report-cybercrime-on-main-street-2025/

Australian Cyber Security Centre Annual Cyber Threat Report 2023-2024. https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024

US Defense Intelligence Agency 2025 Worldwide Threat Assessment. https://industrialcyber.co/reports/us-dia-2025-threat-assessment-warns-of-growing-complexity-in-global-threats-national-security/

Condividi sui Social Network: https://www.ictsecuritymagazine.com/articoli/apt-groups/