Il ransomware gestito da operatori umani: analisi tecnica delle minacce, impatti e strategie di difesa nell’era moderna



Il ransomware gestito da operatori umani rappresenta una trasformazione fondamentale nel panorama delle minacce cyber, evolvendo da attacchi automatizzati di massa a operazioni sofisticate condotte da criminali altamente qualificati. **A differenza del ransomware automatico che si propaga indiscriminatamente attraverso vulnerabilità note, gli attacchi human-operated coinvolgono avversari attivi che conducono ricognizione estensiva, adattano le loro tattiche in tempo reale e massimizzano l’impatto attraverso deployment strategici del ransomware**. Secondo i dati di Microsoft del 2023, gli incontri con ransomware gestito da umani sono aumentati di oltre il 200% da settembre 2022, rappresentando una minaccia crescente per organizzazioni di ogni dimensione.

La distinzione critica risiede nella metodologia: mentre il ransomware tradizionale come WannaCry si diffondeva automaticamente attraverso exploit SMB, gli operatori umani impiegano tecniche di movimento laterale, furto di credenziali e persistenza tipiche degli attacchi nation-state. Questi criminali mantengono una presenza nell’ambiente vittima per settimane o mesi, studiando l’infrastruttura, identificando asset critici ed esfiltrando dati prima della cifratura finale. L’evoluzione verso modelli Ransomware-as-a-Service (RaaS) ha ulteriormente professionalizzato questo ecosistema, con gruppi specializzati che gestiscono diverse fasi dell’attacco.

Tattiche e metodologie tecniche degli attaccanti

La catena di attacco completa secondo MITRE ATT&CK

Gli operatori umani seguono una progressione metodica attraverso le fasi dell'attacco, adattando continuamente le loro tattiche basandosi su ciò che scoprono nell'ambiente target. **L'accesso iniziale avviene principalmente attraverso spearphishing (95% degli incidenti), exploit di applicazioni pubbliche come CVE-2023-3519 (Citrix ADC) o compromissione di servizi remoti non protetti da MFA**. I gruppi come Storm-0501 sono evoluti da attacchi on-premise a vettori cloud-based, mentre Black Basta utilizza tecniche di social engineering sofisticate combinando email bombing con chiamate telefoniche che impersonano il supporto IT.

La fase di esecuzione impiega pesantemente PowerShell (90% degli incidenti) con comandi codificati in Base64, Windows Management Instrumentation per l'esecuzione remota e framework come Empire o Cobalt Strike per il controllo persistente. Gli attaccanti stabiliscono persistenza attraverso modifiche al registro, creazione di account amministrativi locali e deployment di backdoor sofisticate. **Il movimento laterale sfrutta protocolli legittimi come RDP (85% degli incidenti), SMB/Windows Admin Shares tramite PsExec, e WinRM per accesso interattivo**.

Tecniche avanzate di evasione e raccolta dati

Gli operatori dedicano risorse significative all'evasione delle difese, utilizzando strumenti custom come Backstab per terminare soluzioni EDR, disabilitando Windows Defender attraverso PowerShell e iniettando codice maligno in processi legittimi. **La fase di credential access impiega Mimikatz per il dumping della memoria LSASS, LaZagne per il recupero multi-piattaforma delle credenziali e tecniche pass-the-hash per**

l’escalation dei privilegi. La discovery utilizza strumenti come BloodHound per l’analisi di Active Directory, identificando percorsi di attacco ottimali verso asset critici.

L’esfiltrazione dei dati precede sempre la cifratura negli attacchi moderni, con gli operatori che utilizzano Rclone per la sincronizzazione verso cloud storage, AWS S3 buckets per upload diretti e strumenti specializzati come Exmatter o StealBit per la collezione automatizzata. **I dati vengono tipicamente compressi con 7-Zip o WinRAR prima dell’esfiltrazione attraverso canali C2 cifrati o servizi cloud legittimi come Mega e Google Drive**, rendendo la detection estremamente difficile.

Deployment del ransomware e massimizzazione dell’impatto

La fase finale vede il deployment strategico del ransomware per massimizzare il danno operativo. **Gli schemi di cifratura moderni utilizzano ChaCha20 con RSA-4096 (Black Basta) o Curve25519 con cifratura intermittente (RansomHub) per velocizzare il processo**. Prima della cifratura, gli attaccanti eliminano le Volume Shadow Copies tramite vssadmin.exe, terminano servizi critici di backup e disabilitano l’ambiente di recovery. Il targeting prioritario include hypervisor ESXi che ospitano migliaia di VM, domain controller e sistemi di backup, garantendo che il recovery sia estremamente difficile.

Impatti organizzativi e conseguenze economiche

Costi finanziari oltre il riscatto

L’impatto economico del ransomware human-operated ha raggiunto proporzioni senza precedenti nel 2024. **Il costo totale medio di un attacco ransomware è salito a 5,13 milioni di dollari**

nel 2024, un aumento del 574% dal 2019 quando ammontava a 761.000 dollari, con il pagamento del riscatto che rappresenta solo una frazione dei costi totali. I costi di recovery, escludendo il riscatto, ammontano in media a 2,73 milioni di dollari secondo Sophos, aumentati di quasi 1 milione rispetto ai 1,82 milioni del 2023. Le richieste di riscatto superano 1 milione di dollari nel 63% dei casi, con il 30% che supera i 5 milioni.

L'analisi settoriale rivela che il settore sanitario affronta i costi più elevati con una media di 10,93 milioni di dollari per breach nel 2023, seguito dai servizi finanziari a 5,9 milioni. **Il downtime operativo rappresenta un costo significativo, con le organizzazioni che richiedono una media di 24 giorni per il recovery completo**. Solo il 35% delle organizzazioni recupera entro una settimana nel 2024, in calo rispetto agli anni precedenti, dimostrando l'efficacia crescente degli attacchi human-operated nel compromettere i sistemi di backup e rallentare il ripristino.

Disruption operativa e impatto sulla supply chain

Gli attacchi human-operated causano disruption operativa nell'86% dei casi, con impatti a cascata attraverso le supply chain. **Il caso Change Healthcare del 2024 ha dimostrato come un singolo attacco possa interrompere il 50% dell'elaborazione delle richieste mediche negli Stati Uniti, con costi totali diretti di 2,87 miliardi di dollari per UnitedHealth Group nel 2024**. Durante la crisi, UnitedHealth ha dovuto erogare oltre 9 miliardi di dollari in prestiti temporanei ai provider sanitari colpiti dalla paralisi dei sistemi di fatturazione, di cui circa 3,2 miliardi erano stati ripagati entro ottobre 2024.

Il 94% degli attacchi ransomware tenta di compromettere i backup durante l'attacco, riuscendoci nel 57% dei casi secondo i dati Sophos 2024, estendendo significativamente i tempi di recovery. L'impatto umano sui team IT è sostanziale: il 57%

del personale coinvolto nel remediation riporta stanchezza estrema, il 25% sperimenta rabbia e tristezza, e quasi il 20% considera di lasciare il proprio lavoro. **Le organizzazioni con backup non compromessi recuperano entro una settimana nel 46% dei casi, mentre quelle con backup compromessi scendono al 25%**, evidenziando l'importanza critica della protezione dei sistemi di backup.

Strategie di difesa e mitigazione

Implementazione dell'architettura Zero Trust

La difesa efficace contro il ransomware human-operated richiede un approccio Zero Trust completo che verifichi esplicitamente ogni richiesta di accesso, utilizzi privilegi minimi e assuma sempre una breach. **L'implementazione di autenticazione multi-fattore resistente al phishing utilizzando WebAuthn o PKI è essenziale, con le organizzazioni che implementano Zero Trust che mostrano una riduzione significativa nell'impatto del ransomware**. Il Privileged Access Management (PAM) deve eliminare i privilegi permanenti, implementando accesso just-in-time con elevazione temporanea basata sul contesto di rischio.

La microsegmentazione della rete è critica per limitare il movimento laterale, con soluzioni software-defined che forniscono politiche granulari a livello di workload. **Le organizzazioni con microsegmentazione completa recuperano dagli attacchi ransomware più velocemente rispetto a quelle con segmentazione minima, riducendo i tempi di ripristino di diverse ore**. I controlli est-ovest devono monitorare e limitare le comunicazioni interne, bloccando SMB non necessario (porte TCP 137-139, 445) e richiedendo SMB v3.1.1 con cifratura e firma.

Detection avanzata e risposta automatizzata

Le strategie EDR moderne devono impiegare analisi

comportamentale AI-driven, analisi della memoria per detection in-memory e rilevamento di script per PowerShell e tecniche living-off-the-land. **Microsoft Defender XDR può interrompere attacchi ransomware in pochi minuti attraverso correlazione dei segnali, mentre CrowdStrike Falcon e Sophos Intercept X hanno dimostrato tassi di detection del 100% nei test 2024 di SE Labs**. Le regole di detection devono includere monitoraggio per comandi PowerShell codificati, tentativi di credential dumping e cancellazione delle Volume Shadow Copy.

L'implementazione SOAR accelera la risposta attraverso playbook automatizzati che isolano endpoint affetti, disabilitano account compromessi e bloccano IP maligni immediatamente al rilevamento. **Le tecnologie di deception forniscono early warning con quasi zero falsi positivi, deployando honeypot dinamici, honey token e sistemi esca che attraggono e ritardano gli operatori umani**. I canary file nelle directory critiche possono rilevare tentativi di cifratura prima che si diffondano.

Backup immutabili e resilienza operativa

La strategia di backup deve seguire la regola 3-2-1-1-0 evoluta: 3 copie dei dati critici, 2 tipi di storage diversi, 1 copia offsite, 1 copia immutabile e 0 errori nella verifica. **Le tecnologie di backup immutabile come AWS S3 Object Lock, Azure Immutable Blob Storage e Veeam Hardened Repository prevengono la modifica o cancellazione dei backup anche con credenziali amministrative compromesse**. Le organizzazioni con backup immutabili attraverso aree critiche multiple recuperano significativamente più velocemente rispetto agli approcci tradizionali, riducendo i tempi medi di ripristino da oltre 15 ore a circa 4 ore.

Casi studio: lezioni dal campo

MGM Resorts e la vulnerabilità del fattore umano

L’attacco del settembre 2023 a MGM Resorts dimostra come una singola chiamata telefonica possa bypassare tutti i controlli tecnici. **Scattered Spider ha ottenuto accesso attraverso social engineering dell’help desk in circa 10 minuti, fornendo poi accesso ad ALPHV/BlackCat per il deployment del ransomware su oltre 100 hypervisor ESXi**. L’incidente ha causato 100 milioni di dollari in perdite operative e circa 10 giorni di disruption, evidenziando la criticità della verifica dell’identità e della formazione del personale help desk. A differenza di Caesars Entertainment che ha pagato circa 15 milioni di riscatto in un attacco simile, MGM ha rifiutato di pagare, collaborando invece con le forze dell’ordine.

British Library: trasparenza e resilienza istituzionale

L’attacco Rhysida dell’ottobre 2023 alla British Library fornisce lezioni preziose attraverso il loro approccio trasparente post-incidente. **La mancanza di MFA su un server Terminal Services ha permesso l’accesso iniziale, con centinaia di gigabyte di dati esfiltrati prima della cifratura**. Nonostante costi di recovery significativi stimati in diversi milioni di sterline e una disruption operativa che si è estesa per mesi, l’istituzione ha dimostrato eccellenza nella risposta rifiutando il pagamento del riscatto, comunicando trasparentemente con gli stakeholder e documentando lezioni chiave per il settore culturale e accademico.

Change Healthcare: l’impatto sistemico su scala nazionale

L’attacco ALPHV del febbraio 2024 rappresenta il breach sanitario più costoso e impattante nella storia USA. **Un portale Citrix senza MFA ha fornito l’accesso iniziale il 12 febbraio, compromettendo alla fine i dati di oltre 100 milioni**

di individui (con stime successive che raggiungono 192,7 milioni) e interrompendo l'elaborazione delle richieste sanitarie nazionali per mesi.

UnitedHealth ha confermato di aver pagato un riscatto di 22 milioni di dollari ma non ha recuperato i dati. I costi totali per l'azienda hanno raggiunto 2,87 miliardi di dollari nel 2024, con proiezioni che suggeriscono costi totali superiori ai 3 miliardi considerando l'intero ciclo dell'incidente. Il caso dimostra come singoli punti di failure nell'infrastruttura critica possano avere conseguenze catastrofiche a livello di settore, con Change Healthcare che processa 15 miliardi di transazioni sanitarie annualmente.

Conclusione: evoluzione futura e imperativi strategici

Il ransomware gestito da operatori umani continua ad evolversi come minaccia dominante, con l'ecosistema RaaS che si professionalizza ulteriormente e gli attaccanti che adottano tecniche sempre più sofisticate. **Le proiezioni di Cybersecurity Ventures indicano che i costi globali del ransomware raggiungeranno 275 miliardi di dollari annualmente entro il 2031, con attacchi previsti ogni 2 secondi**. L'integrazione di capacità nation-state, l'evoluzione verso attacchi cloud-native e il targeting sistematico delle infrastrutture critiche richiederanno trasformazioni fondamentali negli approcci di cybersecurity.

Le organizzazioni devono adottare strategie defense-in-depth che combinino Zero Trust architecture, detection comportamentale avanzata, backup immutabili e capacità di risposta agli incidenti mature. **Il successo richiederà investimenti sia in tecnologia che in persone, con particolare attenzione alla security awareness, alla resilienza operativa e alla collaborazione settoriale**. L'evidenza dai casi studio dimostra che la mancanza di MFA su sistemi critici, la

formazione inadeguata del personale e l’assenza di backup immutabili rappresentano i fattori di rischio più critici.

La natura adattiva degli operatori umani richiede strategie difensive ugualmente adattive che possano rilevare e rispondere a TTP innovative mantenendo l’efficacia operativa. Solo attraverso un approccio olistico che affronta vulnerabilità tecniche, fattori umani e resilienza organizzativa le organizzazioni possono sperare di difendersi efficacemente contro questa minaccia in evoluzione. La collaborazione internazionale tra forze dell’ordine, l’implementazione di framework normativi più stringenti e l’adozione diffusa di best practice di sicurezza saranno essenziali per invertire la tendenza attuale e ridurre l’impatto economico e sociale del ransomware human-operated.

Fonti:

Cybersecurity and Infrastructure Security Agency (CISA). (2024a). #StopRansomware: Black Basta. U.S. Department of Homeland Security.

Cybersecurity and Infrastructure Security Agency (CISA). (2024b). #StopRansomware: RansomHub Ransomware. U.S. Department of Homeland Security.

Cybersecurity and Infrastructure Security Agency (CISA). (2023). #StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability. U.S. Department of Homeland Security.

Cybersecurity and Infrastructure Security Agency (CISA). (n.d.). #StopRansomware Guide. U.S. Department of Homeland Security.

Federal Bureau of Investigation (FBI) & CISA. (2024). Joint Cybersecurity Advisory: Black Basta Ransomware. Internet Crime Complaint Center.

Microsoft Security. (2024a). Microsoft Digital Defense Report

2024. Microsoft Corporation.

Microsoft Security. (2024b). How Microsoft Copilot for Security helps defend against human-operated ransomware attacks. Microsoft Security Blog.

Microsoft Security. (2023a). Microsoft Digital Defense Report 2023. Microsoft Corporation.

Microsoft Security. (2023b). Espionage fuels global cyberattacks. Microsoft On the Issues.

Microsoft Security. (2020). Human-operated ransomware attacks: A preventable disaster. Microsoft Security Blog.

Microsoft Learn. (n.d.). What is ransomware? Microsoft Documentation.

(2024a). The State of Ransomware 2024. Sophos Ltd.

(2024b). Ransomware Payments Increase 500% In the Last Year, Finds Sophos State of Ransomware Report.

(2025). The State of Ransomware 2025. Sophos Ltd.

IBM Security. (2024). Cost of a Data Breach Report 2024. IBM Corporation.

IBM Security X-Force. (2024). X-Force Threat Intelligence Index 2024. IBM Corporation.

Cybersecurity Ventures. (2025). Global Ransomware Damage Costs Predicted To Exceed $275 Billion By 2031. Cybercrime Magazine.

(2025). The Average Cost Of Ransomware Attacks (Updated 2025).

Varonis Systems. (2024). Ransomware Statistics, Data, Trends, and Facts [updated 2024].

Check Point Software Technologies. (n.d.). Human-Operated Ransomware. Check Point Research.

Palo Alto Networks Unit 42. (2025). 2025 Unit 42 Global Incident Response Report.

HIPAA Journal. (2024). Change Healthcare Increases Ransomware Victim Count to 192.7 Million Individuals.

IBM Think. (2024a). Change Healthcare attack expected to exceed $1 billion in costs.

IBM Think. (2024b). Change Healthcare discloses USD 22M ransomware payment.

(2025). The complete story of the 2024 ransomware attack on UnitedHealth.

American Hospital Association (AHA). (2024). Change Healthcare Cyberattack Underscores Urgent Need to Strengthen Cyber Preparedness.

(2025). MGM Cyber Attack 2023: Impact, Updates, and Response by MGM Resorts.

(2024). MGM Resorts ransomware attack led to $100 million loss, data theft.

NBC News. (2023). Cyberattack cost MGM Resorts about $100 million, Las Vegas company says.

org. (n.d.). 10 Lessons from the British Library Ransomware Attack.

(2024). British Library cyberattack.

(2024). Scattered Spider.

MITRE Corporation. (n.d.). MITRE ATT&CK Framework.

National Institute of Standards and Technology (NIST). (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. U.S. Department of Commerce.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/ransomware-gestito-da-operatori-umani/