Lone Wolf e Ransomware-as-a-Service (RaaS) nell’era della commoditizzazione – L’evoluzione del panorama ransomware



Il panorama delle minacce informatiche ha subito una trasformazione radicale negli ultimi anni, caratterizzata dall’emergere di due fenomeni interconnessi che stanno ridefinendo l’ecosistema del ransomware: la proliferazione di attaccanti solitari (lone wolf) e la continua evoluzione del modello Ransomware-as-a-Service (RaaS). Questa dicotomia rappresenta una paradossale convergenza tra l’individualizzazione degli attacchi e la democratizzazione delle capacità offensive avanzate.

La crescente disponibilità di toolkit open-source e la commoditizzazione delle tecniche di attacco hanno significativamente abbassato le barriere d’ingresso per aspiranti cybercriminali, consentendo l’operatività di attori privi di legami con gruppi strutturati. Parallelamente, il modello RaaS continua a evolversi, con gruppi mid-tier che competono per reclutare affiliati attraverso regole di ingaggio sempre meno restrittive e modelli di business innovativi.

Il fenomeno dei lone wolf: democratizzazione del cybercrime

Definizione e caratteristiche operative

Gli attaccanti lone wolf rappresentano una categoria emergente di threat actor che operano in modo indipendente, senza affiliazione a gruppi ransomware strutturati. Le ricerche di Coveware indicano che il 10% di tutti gli attacchi ransomware monitorati nel secondo trimestre del 2024 proveniva da operatori solitari, rappresentando un incremento massiccio rispetto ai periodi precedenti.

Questi attori sono probabilmente ex-affiliati di gruppi come Alphv (BlackCat) o LockBit, o rappresentano individui che hanno scelto di operare indipendentemente a causa del crescente rischio di esposizione, interruzione e perdita di profitti associati ai “brand ransomware tossici”.

Fattori abilitanti

La proliferazione di attaccanti solitari è facilitata da diversi fattori tecnologici e operativi:

Toolkit open-source e builders pubblici

L’esempio più emblematico è rappresentato dal Prince Ransomware builder, uno strumento automatizzato open-source disponibile su GitHub, che ha consentito la creazione di varianti come “CrazyHunter”, utilizzato nell’attacco al Mackay Memorial Hospital di Taiwan. Il builder, scritto in linguaggio Go, permette agli attaccanti di personalizzare facilmente varianti ransomware modificando i file di configurazione, con varianti identificate come “Black (Prince)”, “Wenda” e “UwU” che differiscono solo per estensioni di file e note di riscatto.

Strumenti legittimi weaponizzati

Un caso paradigmatico è rappresentato da ShrinkLocker, un ransomware che sfrutta BitLocker, l’utility di crittografia nativa di Windows, per bloccare l’accesso ai dati delle vittime. ShrinkLocker è inusuale per due ragioni: è scritto in

VBScript e sfrutta BitLocker per crittografare e bloccare i sistemi delle vittime, un approccio atipico per il ransomware moderno che suggerisce una strategia unica o un threat actor meno sofisticato.

Il malware opera attraverso un processo sofisticato:

1. Verifica la presenza di BitLocker sul sistema e, se non presente, lo installa utilizzando ServerManagerCmd o PowerShell
2. Modifica le chiavi di registro per configurare il sistema per l'esecuzione di BitLocker con le impostazioni richieste dall'attaccante
3. Riduce le partizioni di sistema di 100MB utilizzando l'utilità diskpart per creare spazio per una nuova partizione di boot
4. Disabilita e rimuove tutti i protettori BitLocker predefiniti per impedire il recupero delle chiavi

Impatto operativo e sfide investigative

L'attribuzione di tali attacchi a specifici affiliati ransomware o collettivi è particolarmente impegnativa a causa della diffusa disponibilità e utilizzo di questi strumenti open-source che abilitano attaccanti lone wolf. Nel 2024, WithSecure non è riuscita ad attribuire il 38% dei suoi incidenti ransomware a franchise Ransomware-as-a-Service identificabili, indicando l'aumento di eventi ransomware lone wolf abilitati da strumenti offensivi facilmente disponibili.

Il modello RaaS: evoluzione e strategie competitive

Architettura del modello di business

Il Ransomware-as-a-Service è un modello di business tra operatori ransomware e affiliati in cui gli affiliati pagano per lanciare attacchi ransomware sviluppati dagli operatori. I

kit RaaS sono pubblicizzati sui forum del dark web attraverso l'ecosistema underground, e alcuni operatori ransomware reclutano attivamente nuovi affiliati, investendo milioni in campagne di marketing.

Modelli di revenue

I modelli di revenue per le operazioni RaaS includono diverse varianti:

- **Modello ad affiliazione**: I profitti vengono condivisi tra operatori e affiliati, tipicamente con split del 20-30% per gli sviluppatori
- **Modello subscription**: Pagamento di una fee ricorrente mensile, talvolta ridotta a soli 40 dollari al mese
- **Licenza lifetime**: Pagamento una tantum per accesso illimitato
- **Partnership RaaS**: Split dei profitti definito al momento dell'accesso, generalmente più elevato del modello affiliato

Strategie di reclutamento e competizione

Gruppi tier-1 vs mid-tier

Intel 471 traccia oltre 25 crew RaaS, che spaziano dai gruppi "tier 1" più noti, ai gruppi "tier 2" legati a "varianti di nuova formazione sorte dai fallimenti di gruppi precedenti", fino ai "tier 3" che descrive come "varianti completamente nuove che potrebbero avere la capacità di scalzare le attuali cabale di primo livello".

Una differenza chiave tra i diversi tier di operazioni ransomware, oltre ai profitti relativi che vedono, è chi permettono di unirsi al loro programma di affiliazione. Gli operatori dietro le offerte ransomware di primo livello "sono decisamente molto più rigorosi riguardo a chi permettono nel

loro gruppo criminale”, mentre altri apparentemente non possono permettersi di essere troppo selettivi.

Innovazioni nel reclutamento

Gruppi RaaS più piccoli stanno cercando di reclutare affiliati nuovi e “displaced” di LockBit e Alphv/BlackCat rinunciando a depositi e abbonamenti a pagamento, offrendo migliori split di pagamento, supporto 24/7 e altri “vantaggi”.

Esempi specifici includono:

- **Medusa**: Offre una scala di pagamento variabile, iniziando con uno split 70/30 affiliato/core, aumentando fino a 90/10, dipendente dalla dimensione del pagamento del riscatto ottenuto
- **RansomHub**: Permette agli affiliati di raccogliere personalmente i pagamenti del riscatto prima di pagare il servizio
- **Cloak**: Opta per uno split 85/15 affiliato/core del riscatto e non richiede deposito o pagamento per l’adesione, solo un’intervista

Modelli innovativi emergenti

DragonForce: il modello “cartel”

Nel marzo 2025, DragonForce si è ribrandizzato come “cartel” e ha annunciato il passaggio a un modello distribuito che consente agli affiliati di creare i propri “brand”. In questo modello, DragonForce fornisce la sua infrastruttura e strumenti ma non richiede agli affiliati di implementare il suo ransomware.

Anubis: diversificazione dei servizi

Anubis offre tre modalità operative:

1. **RaaS tradizionale**: Crittografia dei file con affiliati

che ricevono l’80% del riscatto
2. **Data ransom**: Opzione di estorsione solo per furto dati con affiliati che ricevono il 60% del riscatto
3. **Monetizzazione degli accessi**: Servizio che aiuta i threat actor a estorcere vittime già compromesse, offrendo agli affiliati il 50% del riscatto

Implicazioni per la sicurezza informatica

Sfide per la detection e l’attribution

La commoditizzazione delle operazioni ransomware ha come aspetto positivo che le tecniche utilizzate sono condivise tra gli attori e quindi diventano più facili da rilevare su larga scala. Tuttavia, l’attribuzione di tali attacchi a specifici affiliati ransomware o collettivi è particolarmente impegnativa a causa della diffusa disponibilità e utilizzo di strumenti open-source.

Evoluzione delle superfici di attacco

Gli attaccanti Fog ransomware stanno utilizzando un toolset insolito che include utility open-source di penetration testing e software legittimo di monitoraggio dei dipendenti chiamato Syteca. Il toolset implementato dagli attaccanti è piuttosto atipico per un attacco ransomware, includendo strumenti come Adapt2x C2 (alternativa open-source a Cobalt Strike), Process Watchdog, PsExec e Impacket SMB.

Impatto economico e trend dei pagamenti

Il panorama ransomware ha sperimentato cambiamenti significativi nel 2024, con il volume totale dei pagamenti di riscatto diminuito del 35% anno su anno, guidato da maggiori azioni delle forze dell’ordine, migliore collaborazione internazionale e un crescente rifiuto delle vittime di pagare.

Il pagamento mediano è sceso del 45% nel Q4 2024 a $110.890. I pagamenti continuano a rimanere principalmente un’opzione di ultima istanza per coloro che non hanno alternative per recuperare dati critici.

Contromisure e strategie di difesa

Approcci tecnologici

Monitoraggio comportamentale

Il monitoraggio proattivo di specifici log eventi Windows può aiutare le organizzazioni a identificare e rispondere a potenziali attacchi BitLocker, anche nelle loro fasi iniziali, tracciando eventi dalla fonte “Microsoft-Windows-BitLocker-API/Management”, in particolare quelli con ID evento 776 (rimozione protettori) e 773 (sospensione BitLocker).

Principio del minimo privilegio

Assicurarsi che gli utenti abbiano solo privilegi minimi in modo che non possano abilitare funzionalità di crittografia o modificare chiavi di registro da soli.

Strategie organizzative

Gestione dei backup

Fare backup frequentemente, conservarli offline e testarli. La strategia 3-2-1 (3 copie, 2 supporti diversi, 1 offsite) rimane fondamentale.

Network segmentation

L’incidente dell’ospedale Mackay Memorial evidenzia anche l’importanza di proteggere i punti di accesso fisico come le porte USB e implementare robuste misure di protezione degli endpoint. Le organizzazioni devono dare priorità alla segmentazione di rete, al monitoraggio continuo e agli aggiornamenti tempestivi.

Conclusioni e prospettive future

Il panorama ransomware nel 2025 dovrebbe continuare a evolversi con un aumento della sofisticazione e adattabilità da parte dei threat actor. Con un Q4 2024 da record, che ha registrato 1.827 incidenti ransomware, i gruppi ransomware probabilmente intensificheranno le loro operazioni, prendendo di mira industrie ad alto valore e sfruttando tecnologie avanzate come l'intelligenza artificiale per migliorare l'efficacia dei loro attacchi.

La convergenza tra attaccanti lone wolf e modelli RaaS sempre più sofisticati rappresenta una sfida multidimensionale per i professionisti della sicurezza informatica. L'abbassamento delle barriere tecniche, combinato con l'innovazione continua nei modelli di business criminali, richiede un approccio olistico che integri tecnologie avanzate di detection, strategie di threat intelligence e robuste pratiche di cyber hygiene.

La proliferazione di piattaforme RaaS complica ulteriormente gli sforzi delle forze dell'ordine abilitando una gamma più ampia di individui a partecipare ad attività illecite, causando l'aumento del numero di attacchi e la decentralizzazione delle reti criminali ransomware.

Il futuro della sicurezza informatica dipenderà dalla capacità delle organizzazioni di adattarsi a questa evoluzione del panorama delle minacce, implementando strategie difensive proattive che possano contrastare efficacemente sia gli attacchi individuali sofisticati che le campagne massive orchestrate attraverso modelli RaaS.

Fonti

Kaspersky. (2024). *How ShrinkLocker ransomware leverages BitLocker*. https://www.kaspersky.com/blog/shrinklocker-ransomware-encrypt

s-with-bitlocker/51462/

Coveware. (2025). *Will Law Enforcement success against ransomware continue in 2025?*. https://www.coveware.com/blog/2025/1/31/q4-report

Arctic Wolf. (2024). *RaaS Will Grow In 2024*. https://arcticwolf.com/resources/blog/ransomware-as-a-service-will-continue-to-grow-in-2024/

Chainalysis. (2025). *Crypto Ransomware 2025: 35.82% YoY Decrease in Ransomware Payments*. https://www.chainalysis.com/blog/crypto-crime-ransomware-victim-extortion-2025/

Cyberint. (2025). *Ransomware Annual Report 2024*. https://cyberint.com/blog/research/ransomware-annual-report-2024/

Splunk. (2024). *ShrinkLocker Malware: Abusing BitLocker to Lock Your Data*. https://www.splunk.com/en_us/blog/security/shrinklocker-malware-abusing-bitlocker-to-lock-your-data.html

Bitdefender. (2024). *ShrinkLocker (+Decryptor): From Friend to Foe, and Back Again*. https://www.bitdefender.com/en-us/blog/businessinsights/shrinklocker-decryptor-from-friend-to-foe-and-back-again

Kaspersky. (2024). *How ransomware abuses BitLocker*. https://securelist.com/ransomware-abuses-bitlocker/112643/

BankInfoSecurity. (2024). *Ever More Toxic Ransomware Brands Breed Lone Wolf Operators*. https://www.bankinfosecurity.com/blogs/ever-more-toxic-ransomware-brands-breed-lone-wolf-operators-p-3682

WithSecure Labs. (2025). *CrazyHunter: The Rising Threat of Open-Source Ransomware*. https://labs.withsecure.com/publications/crazyhunter-ransomwar

e

GBHackers. (2025). *Prince Ransomware – An Automated Open-Source Ransomware Builder Freely Available on GitHub*. https://gbhackers.com/prince-ransomware-an-automated-open-source-ransomware/

BankInfoSecurity. (2021). *More Ransomware-as-a-Service Operations Seek Affiliates*. https://www.bankinfosecurity.com/more-ransomware-as-a-service-operations-seek-affiliates-a-15378

Help Net Security. (2024). *RaaS groups increasing efforts to recruit affiliates*. https://www.helpnetsecurity.com/2024/03/20/raas-recruit-affiliates/

Secureworks. (2025). *Ransomware Groups Evolve Affiliate Models*. https://www.secureworks.com/blog/ransomware-groups-evolve-affiliate-models

ISACA. (2024). *The Commoditization of Ransomware as a Service*. https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2024/volume-4/the-commoditization-of-ransomware-as-a-service

CrowdStrike. (2025). *What is Ransomware as a Service (RaaS)?* https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/ransomware-as-a-service-raas/

IBM. (2025). *What Is Ransomware-as-a-Service (RaaS)?* https://www.ibm.com/think/topics/ransomware-as-a-service

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/lone-wolf-raas/