DARK MIRROR - OSSERVATORIO DELLE MINACCE RANSOMWARE

REPORT H1 2025

DARKLAB
RHC INTELLIGENCE LABORATORY

Il collettivo **DarkLab** e' un *sotto gruppo della community di Red Hot Cyber* specializzato al monitoraggio delle minacce informatiche. Il RHC dark lab nasce con l'obiettivo principale di diffondere la conoscenza sulle minacce informatiche per migliorare la consapevolezza e le difese digitali del paese.

INTRODUZIONE

Il 2024 e' stato un anno di grandi cambiamenti per l'ecosistema che alimenta il ransomware ed altre minacce digitali. Operazioni da parte di agenzie ed intelligence governative hanno impattato pesantemente RaaS come LockBit, campagne infostealer e Malware-as-a-Service oltre ad effettuare arresti su (parte) dei responsabili dietro a queste azioni. Il leak del backend di LockBit (oltre ad analisi sui wallet dei RaaS) ha fatto riflettere diversi analisti sul declino dei pagamenti dei riscatti che ha portato ad un incremento dei file rubati alle vittime pubblicati sui DLS dei gruppi come previsto dal modello di estorsione perpetrato dagli attaccanti, questo a portato ad uno spike sul numero di vittime (visibili) osservate dai diversi threat analysts. In tale report mostreremo la nostra analisi su tali movimenti cercando di ridimensionare la minaccia che nonostante le risposte da parte delle forze dell'ordine sembra non abbia nessuna intenzione di lasciare la scena.

Il ransomware rimane tuttora una delle minacce più persistenti ed impattanti sulla scena che riesce ad evolversi non solo a livello operativo ma anche per business model avanzando alternative per incentivare gli operatori a portare avanti le loro campagne. La nascita di realta' come DragonForce fanno emergere un approccio proattivo al compensare la decadenza di RaaS come ALPHV/BlackCat e LockBit cercando di recuperare la fetta di mercato e gli affiliati che si stanno spargendo nei RaaS esistenti o creando dei nuovi.

Collettivi come Cl0p e Hunters stanno cambiando la loro metodologia ed approccio per la monetizzazione rimuovendo l'uso del loro ransomware (Hunters) o focalizzandosi sulla scoperta, creazione ed uso di 0-day su larga scala (Cl0p). Gli attori in gioco stanno mostrando una resistenza fuori dal comune che va ben oltre il semplice rebranding alla quale eravamo abituati negli anni precedenti e questo, unito alla frammentazione dei diversi RaaS, rende difficile la protezione dalle campagne in corso vista la loro natura silenziosa e di difficile scoperta tecnico-operativa. L'altra faccia della medaglia porta l'attenzione su attori non meglio identificati che portano avanti azioni di depistaggio attivo ai RaaS (come il leak di LockBit e deface di Everest) donando alla comunità infosec materiale prezioso per le analisi.

Oggi più che mai, vista la complessità dello scenario, bisogna affiancare l'informazione sulle minacce ad ogni livello tecnico dei difensori per poter rispondere in maniera adeguata ai mutamenti del mondo ransomware. Inoltre non possiamo non appoggiare le operazioni delle forze dell'ordine che, seppur

non portino a sopprimere completamente il modello RaaS, riescono ad irrompere e sabotare le funzioni di RaaS e MaaS cercando di disincentivare o fermare i responsabili creando un clima sempre più avverso per loro. Nonostante alcuni specifici individui non possono essere raggiunti (per motivi geografici, politici o tecnici), altri componenti chiave (eg:/ sviluppatori, negoziatori, operatori, affiliati) sono stati fermati e gestiti dalla giustizia.

La prima meta' del 2025, nonostante la (apparente) decadenza nel pagamento dei riscatti e le attività di polizia/intelligence, ha messo a dura prova le minacce che seppure alcuni casi isolati siano stati disarmati riescono comunque a mantenere un ambiente florido per le loro attività sottolineando per le organizzazioni l'importanza della sicurezza informatica che deve essere presente e continuativa nel tempo.

In conclusione, il ransomware si conferma come uno dei business più consolidati e redditizi delle underground criminali, senza mostrare segnali di flessione, come evidenziato dalle tendenze di questo report. Ciò dimostra che, nonostante i consistenti sforzi messi in campo dalle organizzazioni negli ultimi anni, questa minaccia resta tra le più insidiose, con cui le aziende sono costrette a confrontarsi quotidianamente.

Alessio Stefan – Red Teamer e Membro di Dark Lab

INDICE DEI CONTENUTI

"Dark Mirror" è un report realizzato dagli esperti di Dark Lab, un sotto gruppo specializzato in Cyber Threat Intelligence (CTI) di Red Hot Cyber. Grazie al costante monitoraggio delle attività nel mondo sotterraneo digitale, abbiamo redatto un'analisi approfondita sul fenomeno ransomware in Italia, per il periodo H1-2025.

Il nostro obiettivo è informare un pubblico sempre più vasto, contribuendo a rendere l'Italia più resiliente agli attacchi informatici. Attraverso analisi dettagliate e dati raccolti, offriamo una visione chiara delle attuali sfide nella sicurezza cibernetica, promuovendo consapevolezza e misure preventive efficaci.

- **Law Enforcement**
  - Interventi delle forze dell'ordine
  - Impatti sulle operazioni ransomware
- **Initial Access Brokers**
  - Ruolo e importanza degli IAB
  - Principali attori e tecniche
- **CVE (Common Vulnerabilities and Exposures)**
  - Introduzione alle CVE
  - CVE rilevanti nel 2025
  - Mitigazione e prevenzione
  - Conclusioni
- **Dark Lab Community**

METODOLOGIA

La nostra metodologia si basa su un approccio multi-strato che integra diverse tecniche di raccolta e analisi dei dati per fornire una comprensione approfondita e aggiornata delle minacce informatiche, con un focus particolare sul ransomware.

RACCOLTA DATI

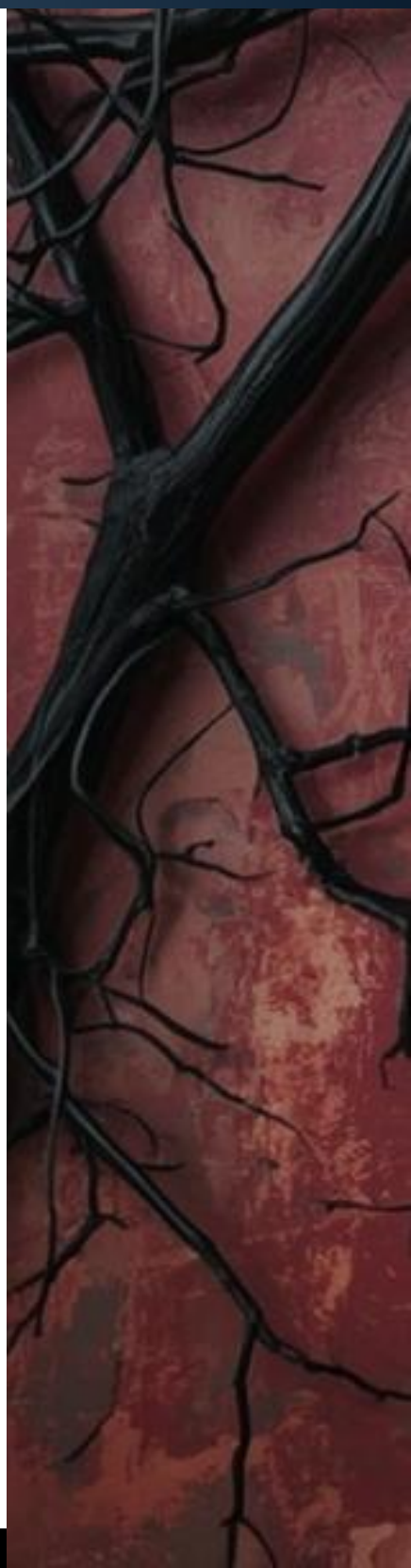
- **Monitoraggio delle Underground:** Utilizziamo strumenti avanzati per monitorare costantemente forum, mercati underground e altre piattaforme clandestine dove avvengono scambi di informazioni e strumenti legati al ransomware;
- **Threat Hunting:** Effettuiamo attività proattive di threat hunting su vasta scala per identificare nuove varianti di ransomware e metodi di attacco emergenti;
- **Partnership e Collaborazioni:** Collaboriamo con altre organizzazioni e enti governativi per condividere informazioni e rafforzare la nostra capacità di rilevamento e di analisi.

ANALISI

- **Indicatori di Compromissione (IOC):** Analizziamo gli indicatori di compromissione raccolti durante le attività di monitoraggio e threat hunting per identificare pattern e tendenze;
- **Tecniche, Tattiche e Procedure (TTPs):** Studiamo le tecniche, tattiche e procedure utilizzate dai threat actors per capire le loro strategie e prevedere le loro mosse future. Seguiamo i nuovi Threat Actors per comprendere appieno le nuove TTPs adottate;
- **Analisi Forense:** Siamo in contatto con aziende ed enti che svolgono analisi forensi su campioni di ransomware per capire le modalità di infezione e le misure di evasione adottate dai cyber criminali.

REPORTING

- **Dati Aggregati:** Utilizziamo strumenti da noi realizzati per effettuare analisi e tendenze sui dati raccolti e per aggregare e visualizzare le informazioni, facilitando l'interpretazione e la comunicazione dei risultati;
- **Case Studies:** analizziamo i pattern negli attacchi ransomware recenti per fornire esempi concreti delle minacce e delle loro conseguenze. Svolgiamo interviste ai Threat Actors per comprendere appieno le loro TTPs.
- **Tendenze e Previsioni:** Analizziamo le tendenze globali e locali nel campo del ransomware sia a livello di difesa e di attacco. Cerchiamo di offrire consapevolezza del rischio oltre che previsioni sulle future evoluzioni del panorama delle minacce ransomware.



ANALISI E TENDENZE

TENDENZE GLOBALI, TENDENZE PANORAMA ITALIANO, TRENDS

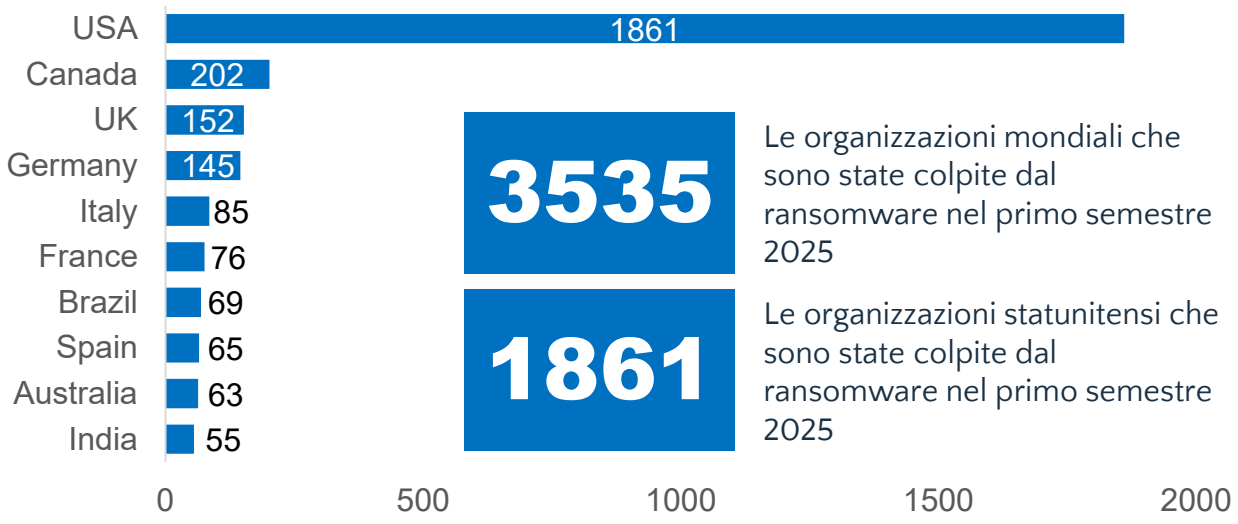
A cura di Massimiliano Brolli, Pietro Melillo e Inva Malaj

ANALISI E TENDENZE

ANALISI GLOBALI – PAESI PIU'COLPITI

Nel primo semestre del 2025, **Dark Lab** ha rilevato 3535 vittime documentate da attacchi ransomware a livello globale. È fondamentale sottolineare che questa cifra rappresenta solo una frazione degli incidenti reali, data la pratica di pubblicare solo parte dei dati rubati e l'assenza dei casi di estorsione doppia (double extortion) e dati non riportati nei leak site (DLS).

TOP10 Paesi maggiormente colpiti



Panoramica Geografica e Settoriale: Le analisi mostrano che il ransomware non conosce confini geografici, colpendo sia paesi sviluppati che in via di sviluppo. Stati Uniti: 1.861 vittime

Gli Stati Uniti registrano il numero assoluto più elevato di attacchi, ma questa cifra deve essere contestualizzata considerando le dimensioni del paese. Con una popolazione di circa 340,11 milioni di abitanti e un PIL di 29,18 trilioni di dollari, gli USA presentano un tasso di attacchi di circa 5,47 vittime per milione di abitanti. La predominanza numerica riflette principalmente la vastità dell'economia americana e l'elevato numero di organizzazioni digitalizzate, oltre all'attrattività rappresentata dalle aziende statunitensi per i cybercriminali.

ANALISI E TENDENZE

ANALISI GLOBALI – PAESI PIU'COLPITI

Analisi Geografica: I Paesi Più Colpiti

Canada: 202 vittime

Con ≈**41,29 milioni** di abitanti, il Canada mostra un tasso di circa **4,87 vittime** per milione di abitanti. Questo dato indica un livello di rischio proporzionale molto elevato, il più alto dopo gli USA, confermando l'elevata esposizione delle economie nordamericane avanzate.

Regno Unito: 152 vittime

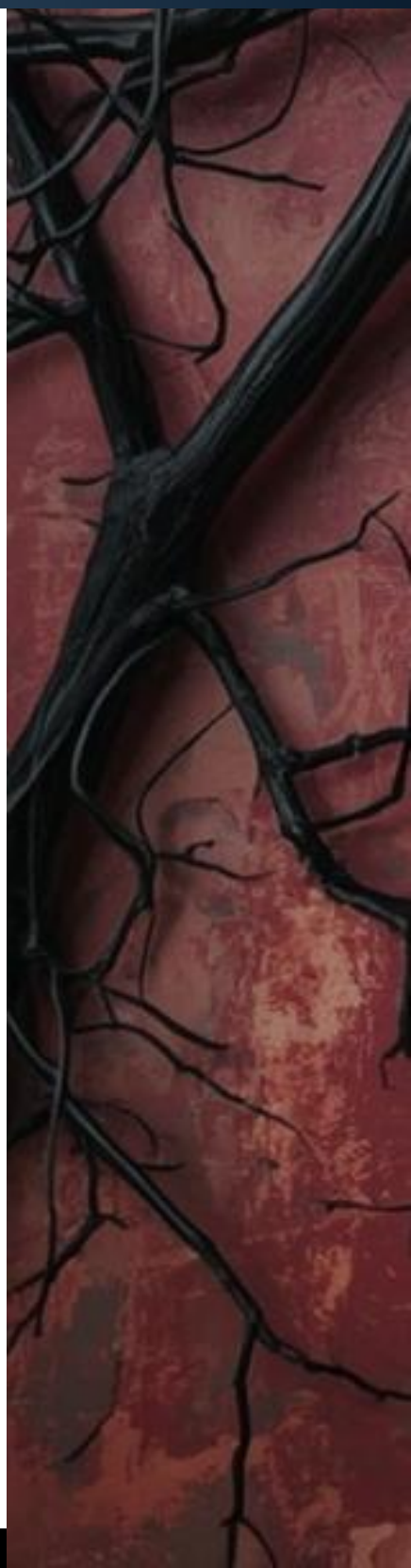
Il Regno Unito, con ≈**69,23 milioni** di abitanti, presenta un tasso di circa **2,20 vittime** per milione di abitanti. Nonostante il numero assoluto più contenuto, il tasso proporzionale rimane significativo per un'economia altamente digitalizzata.

Germania: 145 vittime

La Germania, con ≈**83,51 milioni** di abitanti, registra un tasso di circa **1,74 vittime per milione** di abitanti. Questo dato, seppur inferiore in termini proporzionali, conferma comunque la vulnerabilità delle economie europee industrializzate.

Italia: 85 vittime

L'Italia, con ≈**58,99 milioni** di abitanti, mostra un tasso di circa **1,44 vittime** per milione di abitanti. Pur essendo relativamente basso tra i primi cinque paesi, questo dato evidenzia comunque una significativa esposizione della nostra economia alla minaccia ransomware.



ANALISI E TENDENZE

ANALISI GLOBALI – PAESI PIU'COLPITI

Distribuzione Geografica degli Attacchi

Come evidenziato nel **Grafico 1 – Distribuzione per Paese**, la concentrazione geografica degli attacchi rivela pattern significativi. Gli Stati Uniti dominano con 1.861 vittime, rappresentando oltre il 52% del totale globale, seguiti da Canada (202), Regno Unito (152), Germania (145) e Italia (85).

Analisi proporzionale per popolazione e PIL:
Utilizzando i dati demografici ufficiali più recenti presi da WORLD BANK e IMF, l'analisi del rischio per popolazione rivela:
Rischio per milione di abitanti:

- **Stati Uniti**: 5,47 vittime/milione (1.861 vittime / ≈340,11 milioni abitanti)
- **Canada**: 4,87 vittime/milione (202 vittime / ≈41,29 milioni abitanti)
- **Australia**: 2,32 vittime/milione (63 vittime / ≈27,20 milioni abitanti)
- **Regno Unito**: 2,20 vittime/milione (152 vittime / ≈69,23 milioni abitanti)
- **Germania**: 1,74 vittime/milione (145 vittime /≈83,51 milioni abitanti)
- **Italia**: 1,44 vittime/milione (85 vittime / ≈58,99 milioni abitanti)
- **Spagna**: 1,33 vittime/milione (65 vittime / ≈48,81 milioni abitanti)
- **Francia**: 1,11 vittime/milione (76 vittime / ≈68,52 milioni abitanti)
- **Analisi per intensità economica (vittime per trilione di PIL):**
- **Canada**: 90,2 vittime/trilione USD (202 vittime / 2,24 trilioni USD)
- **Stati Uniti**: 63,8 vittime/trilione USD (1.861 vittime / 29,18 trilioni USD)
- **Regno Unito**: 41,8 vittime/trilione USD (152 vittime / 3,64 trilioni USD)
- **Australia**: 36,0 vittime/trilione USD (63 vittime / 1,75 trilioni USD)
- **Italia**: 35,9 vittime/trilione USD (85 vittime / 2,37 trilioni USD)
- **Spagna**: 35,6 vittime/trilione USD (65 vittime / 1,72 trilioni USD)
- **Germania**: 31,1 vittime/trilione USD (145 vittime / 4,66 trilioni USD)
- **Francia**: 24,1 vittime/trilione USD (76 vittime / 3,16 trilioni USD)

Questa doppia analisi evidenzia come il Canada, pur avendo meno vittime in termini assoluti, presenti il rischio più elevato per intensità economica e il secondo più alto per popolazione, suggerendo vulnerabilità specifiche dell'ecosistema digitale canadese.

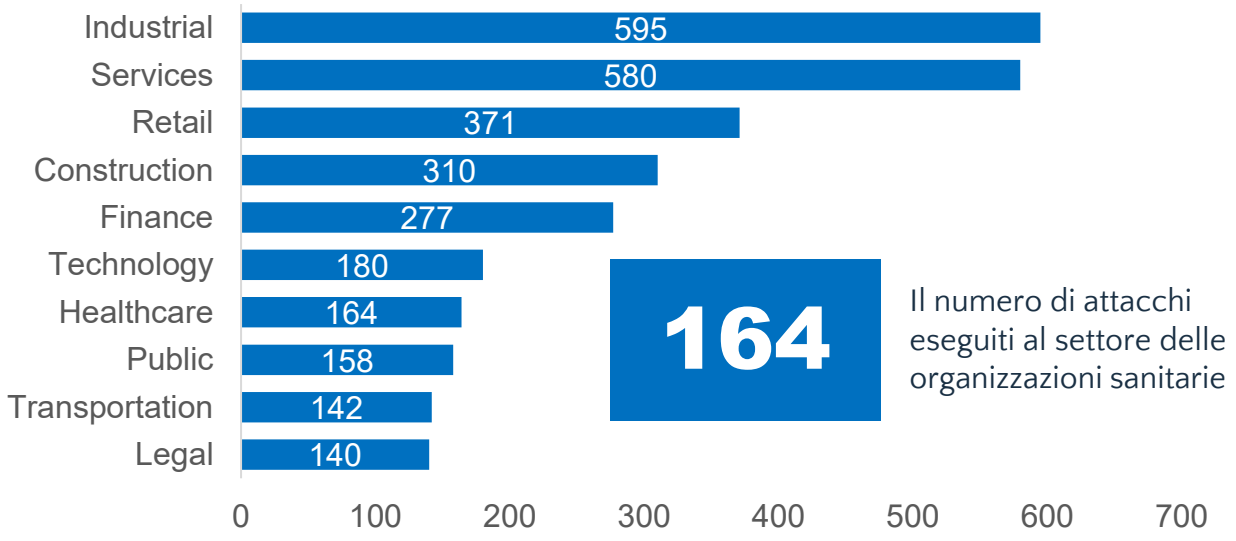
ANALISI E TENDENZE

ANALISI GLOBALI – SETTORI PIU' COLPITI

Le analisi mostrano che il ransomware non conosce confini geografici, colpendo sia paesi sviluppati che in via di sviluppo.

I settori maggiormente colpiti includono l'industria, i servizi e la tecnologia, evidenziando l'ampia portata e l'impatto devastante che questi attacchi possono avere sull'economia globale e sulla vita quotidiana delle persone.

TOP10 Settori maggiormente colpiti (Worldwide)



Settori Maggiormente Colpiti: Dall'analisi settoriale, il ransomware mostra una netta predilezione per il settore industriale, che risulta il più colpito a livello mondiale con 595 attacchi. Segue il settore dei servizi (580 attacchi) e quello retail (371 attacchi), dimostrando che gli attacchi non risparmiano le infrastrutture critiche e i servizi essenziali. Salgono tra i primi posti anche i settori della costruzione (310 attacchi) e della finanza (277 attacchi), evidenziando una preoccupazione crescente per la sicurezza e la resilienza di questi settori.

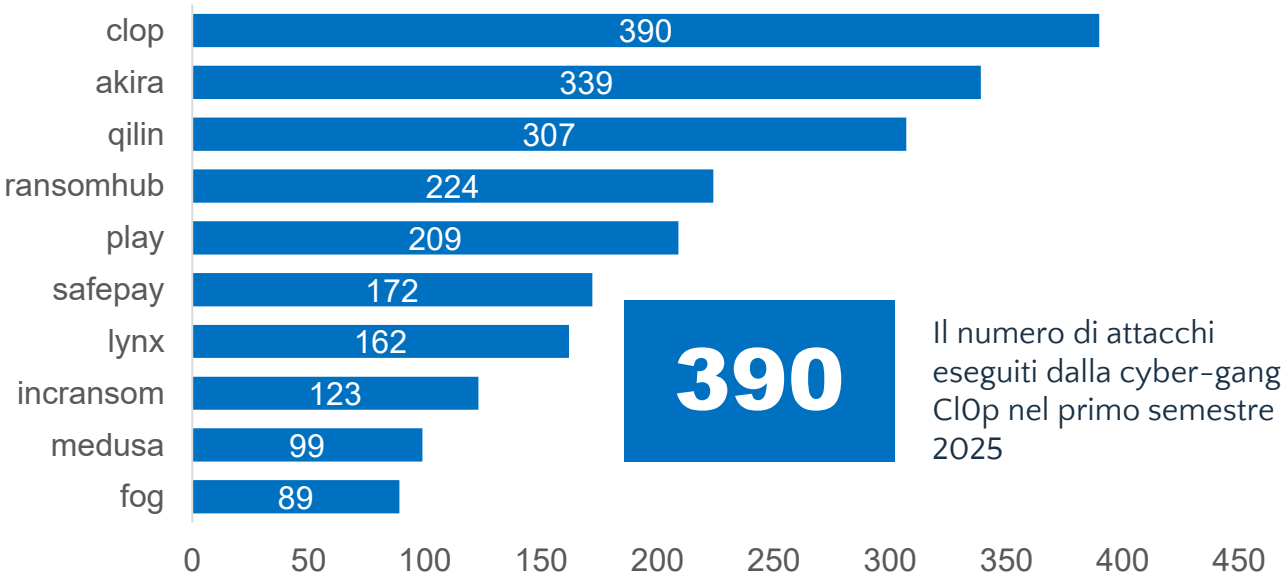
Il settore sanitario, con 164 attacchi, rimane particolarmente vulnerabile, ma è preceduto dai settori industriale, dei servizi, retail, costruzione, finanza e tecnologia (180 attacchi). Anche il settore pubblico, dei trasporti e legale sono frequentemente bersagliati, mostrando come la dipendenza dalle tecnologie digitali e la gestione dei dati siano fattori che aumentano l'attrattività per i criminali informatici.

ANALISI E TENDENZE

ANALISI GLOBALI – THREAT ACTORS PIU' ATTIVI

Il grafico evidenzia i gruppi criminali più attivi nella scena del Ransomware-as-a-Service (RaaS) nel periodo di osservazione. Nonostante le iniziative di contrasto messe in atto dalle autorità, la persistenza e la capacità evolutiva di questi threat actor restano un elemento centrale nella dinamica degli attacchi globali.

TOP10 Threat Actors maggiormente attivi (Worldwide)



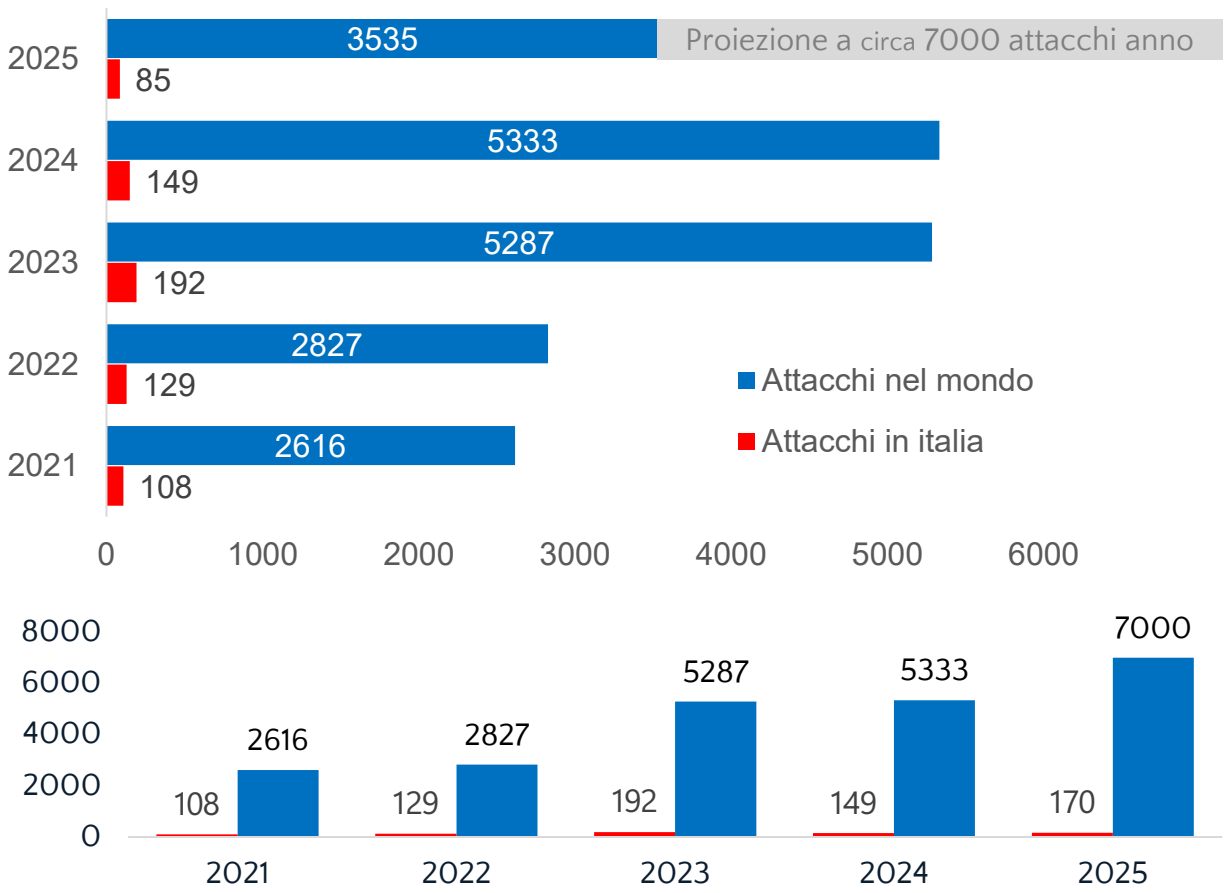
Il gruppo Clop si conferma come il principale attore ransomware del periodo, totalizzando 390 attacchi a livello mondiale. Immediatamente dietro, Akira registra 339 attacchi, dimostrando una crescita rapida e una forte pressione sulle infrastrutture prese di mira. Qilin si posiziona al terzo posto con 307 attacchi, seguito da Ransomhub che con 224 attacchi conferma una presenza costante nella scena criminale internazionale. Play mantiene una significativa attività con 209 attacchi, mentre Safepay (172 attacchi) e Lynx (162 attacchi) si distinguono come operatori molto attivi e radicati nel panorama RaaS.
Completano la classifica Incransom (123 attacchi), Medusa (99 attacchi) e Fog (89 attacchi), evidenziando come il fenomeno ransomware sia alimentato da una varietà di gruppi criminali organizzati che contribuiscono alla diffusione e all'impatto degli attacchi su scala globale.
Questi dati sottolineano l'adattabilità e la resilienza dei principali ransomware actors, che continuano a rappresentare una minaccia primaria per la sicurezza delle infrastrutture digitali a livello mondiale.

ANALISI E TENDENZE

TENDENZE

I dati relativi agli attacchi ransomware registrati negli ultimi tre semestri mostrano una situazione in costante evoluzione, con una crescita significativa a livello globale e in Italia. La tabella seguente mostra l'andamento complessivo degli attacchi ransomware pubblicati dai threat actor all'interno dei Data Leak Site (DLS) negli ultimi cinque anni, includendo una proiezione statistica per il 2025.

TREND Year to Year



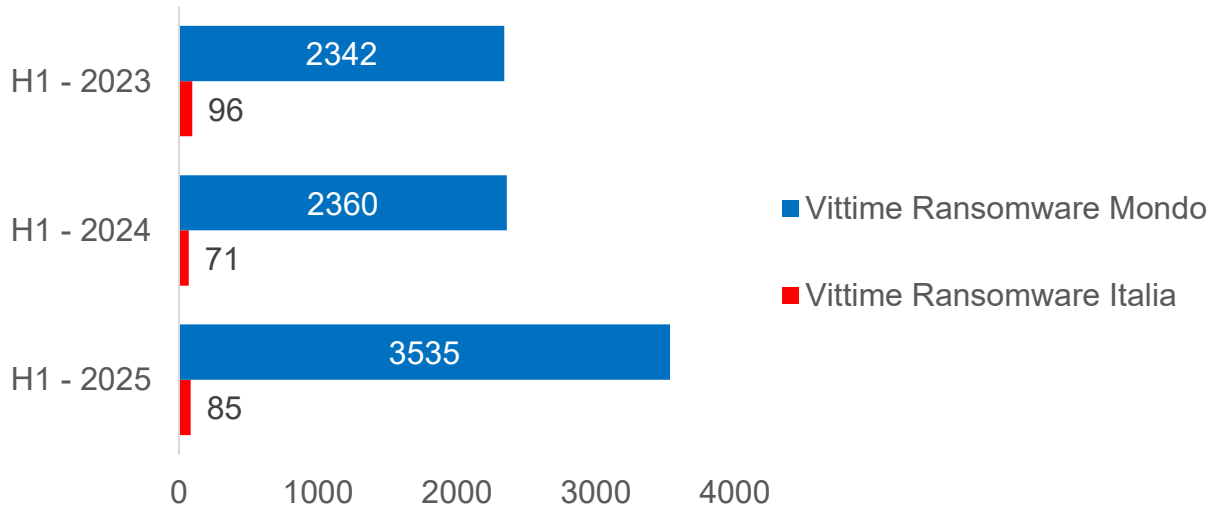
Proiettando i volumi registrati nel primo semestre del 2025 sul secondo, è plausibile che l'anno si chiuda con circa 7.000 attacchi. Un dato da non sottovalutare, soprattutto considerando l'evidente trend di crescita biennale già osservato nelle coppie 2021/2022 e 2023/2024. In conclusione, il ransomware non mostra segnali di rallentamento: al contrario, continua a confermarsi come uno dei business più solidi e radicati nell'underground criminale.

ANALISI E TENDENZE

TENDENZE

I dati relativi agli attacchi ransomware registrati negli ultimi tre semestri mostrano una situazione in costante evoluzione, con una crescita significativa a livello globale e in Italia. La tabella sottostante evidenzia il numero di vittime ransomware in Italia e nel mondo dal 2023 al 2025 su base semestrale.

TREND su base semestre



- **Nel primo semestre 2025** sono state registrate 85 vittime ransomware in Italia e 3.535 a livello mondiale.
- **Nel primo semestre 2024** le vittime sono state 71 in Italia e 2.360 nel mondo.
- **Nel primo semestre 2023** il dato italiano si attestava a 96 vittime, mentre quello mondiale era di 2.342.

Nel contesto italiano, si rileva una leggera flessione nel 2024 rispetto ai due semestri precedenti, mentre a livello mondiale la tendenza mostra un forte incremento nel primo semestre 2025, più che raddoppiando il valore rispetto al 2023.
Questa dinamica potrebbe essere attribuita a diversi fattori, quali l'evoluzione delle tecniche difensive, cambiamenti nelle strategie dei cybercriminali e una maggiore visibilità e capacità di rilevamento degli attacchi a livello globale.

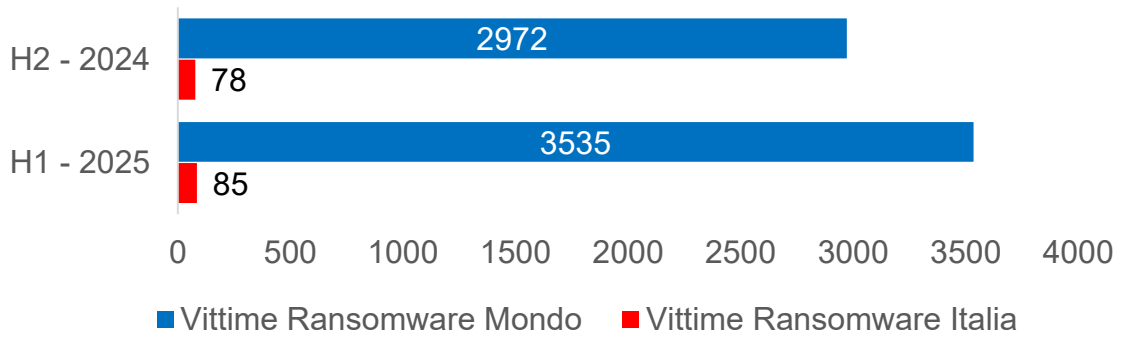
In sintesi, nonostante si osservi una diminuzione temporanea delle vittime in Italia nel 2024, il primo semestre 2025 segna una ripresa significativa degli attacchi sia a livello nazionale che internazionale, confermando che il ransomware rimane una delle principali minacce informatiche a livello globale.

ANALISI E TENDENZE

TENDENZE

L'analisi dei dati disponibili per Italia e panorama globale fornisce un quadro della situazione attuale, pur con i limiti di un confronto tra periodi non omogenei (H1 2025 vs H2 2024):

Confronto H2 2024 vs H1 2025



Crescita Italia
Nel primo semestre 2025, l'Italia registra 85 vittime ransomware, con un incremento del **+8,97%** rispetto alle 78 vittime del secondo semestre 2024.

Crescita Globale
A livello mondiale, sono state rilevate 3.535 vittime ransomware nel primo semestre 2025, segnando un aumento del **+18,94%** rispetto alle 2.972 vittime del secondo semestre 2024.

Posizionamento nel Contesto Globale
Nel **H1 2025**, l'Italia rappresenta il **2,4%** delle vittime globali, in calo rispetto al **2,62%** di H2 2024. Questo dato esprime una presenza significativa, pur evidenziando una leggera diminuzione della quota italiana sul totale mondiale.

Analisi delle Dinamiche di Crescita
La crescita delle vittime ransomware in Italia segue la dinamica mondiale:

- Le difese nazionali non risultano ancora più efficaci rispetto alla media globale.
- L'Italia rimane un mercato costantemente coinvolto dagli attacchi ransomware.

Trend Osservati
La diminuzione della quota italiana dal 2,62% al 2,4% può essere interpretata come un segnale positivo, pur mantenendo numeri assoluti rilevanti.

ANALISI E TENDENZE

ANALISI GLOBALI – THREAT ACTORS PIU' ATTIVI

Distribuzione Settoriale per Gruppo Ransomware

Heatmap – Distribuzione Attacchi Ransomware Top10 Gruppi (H1 2025)
La heatmap offre una lettura immediata sulla concentrazione e la diversificazione delle campagne ransomware condotte dai dieci principali gruppi criminali nel primo semestre 2025.

Settore	clop	akira	qilin	ransomhub	play	safepay	lynx	incransom	medusa	fog	Totale
Industrial	59	69	53	39	48	32	38	8	15	10	371
Services	50	56	47	35	28	26	20	12	24	17	315
Retail	119	38	30	22	26	15	14	8	3	5	280
Construction	9	39	31	32	36	18	22	4	11		202
Finance	14	37	24	15	17	10	12	3	6	5	143
Unknown	19	21	21	5	7	19	6	10	1	7	116
Transportation	46	8	15	7	11	6	7	1	2	1	104
Technology	26	13	13	9	7	2	4	2	4	13	93
Healthcare	6	6	17	9		11	1	28	9	1	88
Public	2	2	14	10		7	8	26	8	4	81
Education	2	3	15	9	1	12	2	12	6	17	79
Legal		17	9	13	7	7	11	1	1	1	67
Media	8	10	7	7	5	2	5	2	7	5	58
Energy	7	11	3	4	9	1	9	2		1	47
Agriculture	16	6	4	1	3	2	2	2			36
Consumer	7	3	2	4	3	2				2	23
Entertainment			2	3	1		1	2	2		11
Totale	390	339	307	224	209	172	162	123	99	89	

Trend Settoriali: Focus sulle Industrie a Maggior Rischio

Comparto Industrial e Servizi:

Il settore industriale emerge come bersaglio primario, con oltre 350 incidenti rilevati. Segue il mondo dei servizi, anch'esso sotto intensa pressione, a conferma della crescente interconnessione tra produzione e funzioni strategico-operative. La compromissione di questi ambiti può portare a impatti estesi su supply-chain, business continuity e reputazione.

Retail:

Colpisce la spiccata aggressività verso il retail, settore digitale e ad alta esposizione, dove Clop domina con volume massimo (119 attacchi), seguito da Akira, Qilin e altri gruppi. La vulnerabilità alle minacce è legata all'elevato volume di dati sensibili e transazionali trattati.

Trend di Settore

Finance, Construction, Technology, Healthcare:
Questi comparti mostrano una costante e trasversale esposizione agli attacchi, con numeri rilevanti distribuiti tra più attori ransomware. In particolare, finance (Akira, Lynx, Qilin) e construction (Akira, Play, Ransomhub) confermano l'interesse criminale per i dati economici, gestionali e per le infrastrutture digitali sempre più diffuse.
Gang Ransomware: Leadership e Modelli Operativi
Clop, Akira, Qilin:
Si distinguono come operatori "ad ampio spettro", con la capacità di colpire trasversalmente quasi tutti i settori e con una predilezione per obiettivi strategici e ad alto ROI. Volume, intensità e varietà dei target riflettono modelli RaaS evoluti, intelligenza operativa e forte propensione al ricatto.
Ransomhub, Play, Lynx, Safepay:
Questi gruppi mantengono una pressione articolata su vari ambiti e consolidano la propria presenza attraverso attacchi ripetuti e diversificati. L'agilità tattica consente di sfruttare opportunità anche in segmenti meno tradizionali.
Gruppi minori (IncRansom, Medusa, Fog):
Pur con numeri assoluti inferiori, dimostrano efficacia nell'operare su settori specifici o nella gestione di campagne mirate, sottolineando il rischio di fenomeni "long tail" e di attori specializzati.
Settori "Unknown": Limitazioni dell'Intelligence
Una quota non trascurabile di incidenti (116 attacchi) viene registrata sotto la categoria "Unknown", a testimonianza delle difficoltà persistenti nel tracciare con precisione i target e l'effettivo impatto settoriale di molte campagne.

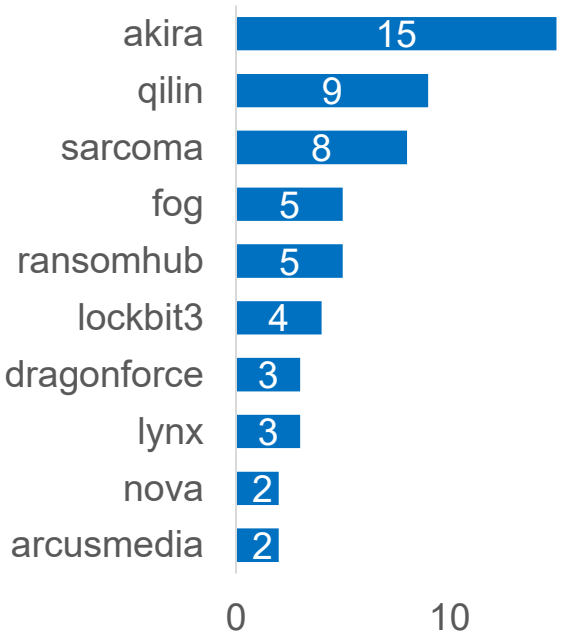
L'evoluzione della minaccia ransomware richiede oggi una sinergia fra tecnologia, processi e cultura organizzativa, per garantire resilienza e protezione degli asset critici in un landscape criminale sempre più sofisticato ed eterogeneo.

ANALISI E TENDENZE

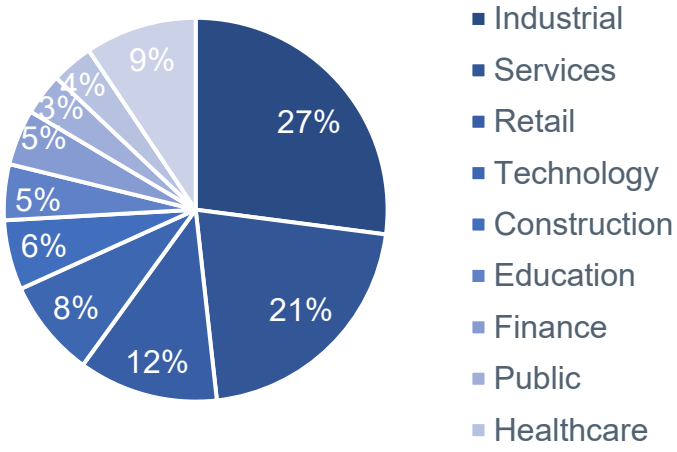
ANALISI COMPARTO ITALIA

Nel periodo di osservazione sono stati documentati 85 attacchi ransomware in Italia, sottolineando l'urgenza di rafforzare la sicurezza nei settori più vulnerabili. L'attività ransomware si concentra principalmente nei comparti industriale e dei servizi, considerati priorità dai threat actor, mentre pubblica amministrazione, sanità ed educazione, pur meno colpiti, restano a rischio. Pochi gruppi dominano il panorama, con Akira in testa e altri come Qilin e Sarcoma attivi in modo significativo, accompagnati da una serie di attori meno frequenti ma costanti.

TOP10 Threat Actors maggiormente attivi



TOP10 Settori più colpiti



TOP10 Threat Actors maggiormente attivi

Il gruppo Akira si distingue come il threat actor più attivo, responsabile di 15 attacchi. Seguono Qilin con 9 attacchi, Sarcoma con 8, quindi Fog e Ransomhub entrambi con 5 attacchi. Lockbit3 totalizza 4 attacchi, mentre Dragonforce e Lynx si attestano su 3 attacchi ciascuno. Nova e Arcusmedia chiudono la classifica con 2 attacchi ciascuno.

TOP10 Settori maggiormente colpiti

Le percentuali del grafico a torta mostrano che il settore industriale è il più bersagliato dagli attacchi ransomware, rappresentando il 27% del totale. Seguono i servizi (21%) e il retail (12%). La tecnologia registra l'8% degli incidenti, mentre costruzione, education e finanza si attestano rispettivamente al 6%, 5% e 5%. Il settore pubblico e quello sanitario sono meno coinvolti, con il 4% e il 3% degli attacchi. Infine, la categoria "Other" raccoglie il restante 9%.

THREAT ACTORS

PANORAMICA GRUPPI 2025

A cura di Alessio Stefan

I THREAT ACTORS

PANORAMICA GRUPPI 2025

Codefinger - Amazon

Nei primi giorni del mese di Gennaio 2025 è stato scoperta una nuova minaccia specifica per i sistemi AWS. Rinominata da Halcyon come "Codefinger", questa nuovo ceppo permette di abusare dei servizi nativi AWS di server-side encryption (SSE-C) per criptarne i dati tramite una chiave AES-256. Assieme alla ransom note posta all'interno dei bucket S3 è stato notato l'utilizzo dei marker (grazie alle lifeycle policies) sui file criptati forzandone l'eliminazione dopo 7 giorni dall'attacco. Tale modalità rende impossibile il recupero dei dati senza la chiave AES in chiaro (ottenibile solo tramite pagamento) essendo che solamente l'HMAC di quest'ultima viene loggata all'interno dei Bucket S3. Gli attori dietro CodeFinger ottengono le chiavi AWS delle vittime tramite compromissione o disclosure. Si consiglia di restringere l'utilizzo di SSE-C assieme ad un controllo delle chiavi AWS per poter mitigare le capacità di questa minaccia.

STAC5143 & STAC5777

Sophos ha pubblicato un report esaustivo riguardo a 15 incidenti che hanno coinvolto i due gruppi di attacanti **STAC5143** e **STAC5777**, entrambi appartenente ad un nuovo cluster proveniente da **Storm-1811**. I due gruppi hanno approcciato direttamente le vittime cercando di eluderli nell'installazione di software RMM tramite la combinazione **Vishing-Mail Bombing**. Gli attaccanti operano dai loro tenant Microsoft Office 365 dalla quale comunicano tramite Teams con i loro bersagli. In tutti gli incidenti è stato notata la seguente metodologia : in primo luogo vengono inviate fino a 3000 mail in un'ora all'indirizzo email della vittima dopodichè gli attori si mettono in contatto sfruttando le impostazioni default di Microsoft Teams che permettono ad utenti di una rete interna di potersi connettere con altri esterni. Gli attaccanti si fingono supporto IT o HelpDesk della azienda convincendo ad installare software RMM/RDP dalla quale connettersi ed iniziare le loro operazioni nella rete interna dell'organizzazione. **STAC5143** si affida a tool personalizzati che permettono operazioni automatizzate mentre STAC5777 sembrerebbe preferire un approccio hands-on-keyboard. In uno degli incidenti analizzati è stato utilizzato il ransomware **BlackBasta.**

I THREAT ACTORS

PANORAMICA GRUPPI 2025

RAWorld meets the dragon

Grazie ad una indagine del dipartimento di Cyber Threat Intelligence di Symantec iniziato a fine 2024 ha rivelato l'utilizzo della backdoor PlugX/Korplug in campagne ransomware di RA World. Tale malware non è pubblico ed è stato associato solamente ad APT cinesi (come APT41, APT3, GALLIUM, Mustang Panda, Emperor Dragonfly) responsabili di operazioni di spionaggio. Nei casi studiati da Symantec le vittime di RA World in questione sarebbero un ministero degli esteri dell'europa sudest non meglio specificata e due aziende asiatiche (con pagamento richiesto di $2 MLN). Tre le varie ipotesi due sono le più plausibili : un ulteriore modello di monetizzazione per attori APT oppure utilizzare il malware dei RaaS come diversivo per le operazioni di spionaggio.

Medusa still in the maze

Il RaaS Medusa ha concluso con successo più di 300 operazioni in organizzazioni USA inclusi settore healthcare e infrastrutture pubbliche. La CISA ha prontamente pubblicato un advisory interamente dedicato al gruppo. Medusa sta facendo un forte un uso dello spear phishing su indirizzi Gmail e Outlook per poter ottenere l'accesso iniziale all'interno delle reti. E' stata identificata anche una forte connessione tra il RaaS e diversi Initial Access Broker (IAT) per la compravendita di credenziali di VPN, servizi Email ed altri profili necessari per poter portare a termine le loro attività. Il pagamento agli IAT vanno da un range di $100 fino a $1MLN.

I THREAT ACTORS

PANORAMICA GRUPPI 2025

Qilin - Legal Evil

Qilin continua ad affermarsi come uno dei servizi ransomware più impattanti tra la concorrenza, da inizio 2024 il gruppo si sta lentamente trasformando in una piattaforma che va ben oltre l'offerta di un semplice modello di affiliazione ransomware. Gli affiliati di Qilin troveranno ora disponibile sul loro panel il pulsante "**Call Lawyer**" che permette di contattare uno degli "esperti" (così descritti) del team legale di Qilin per consulenze riguardo alle loro vittime. Le figure messe a disposizione dal RaaS possono partecipare direttamente alle chat di negoziazione per generare ulteriore pressione alla vittima alla quale viene chiesta l'estorsione. Ricordiamo che l'attacco di Qilin ai danni del NHS britannico (2024) ha portato alla morte di un paziente causata dai diversi disservizi ottenuti dopo l'esecuzione del ransomware sui sistemi del provider healthcare. Qilin rimane una delle minacce con un forte interesse nella monetizzazione andando ad impattare settori critici in maniera indiscriminata, King's College Hospital ha confermato nel mese di Giugno che l'attacco effettuato da Qilin al servizio di blood testing NHS ha portato alla morte di un paziente lasciando quesiti su questo tipo di attacchi su settori critici.

Scattered Spider - Can't Stop, Won't Stop

Nonostante la serie di arresti sul gruppo, Scattered Spider è ben lontano dal cessare le sue attività mantenendo un ruolo chiave nelle operazioni della quale fanno parte. Il modus operandi del collettivo sembra rimanere invariato dando priorità a settori specifici in periodi medio-lunghi, nella prima parte del 2025 è stato il turno del settore vendita e retailing. Marchi come Dior e Harrods hanno subito la kill-chain di Scattered Spider inclusa la fase di social engineering tramite chiamate al supporto IT aziendali e helpdesk. Nonostante il loro meticoloso approccio di scelte delle vittime, sono stati osservati casi in cui Scattered Spider attaccare vittime non incluse nel settore preso di mira in quel specifico lasso temporale. Dopo la chiusura di ALPHV/BlackCat si è osservato l'utilizzo del ransomware DragonForce nelle operazioni del collettivo, sottolineando uno spostamento continuo tra i diversi RaaS senza una precisa preferenza, adattandosi alle diverse offerte disponibili sul momento. Scattered Spider insegna che un uso intelligente dell'ingegneria sociale permette una persistenza sul campo nonostante un uso diverso di strumenti e malware.

I THREAT ACTORS

PANORAMICA GRUPPI 2025

AKIRA - Il sasso nello stivale (???)

AKIRA ha causato un picco rilevante di vittime italiane andando a smantellare principalmente aziende del nord-est. Come abbiamo segnalato in un report apposito, sembrerebbe che affiliati di BlackBasta abbiano portato con sé il tool BRUTED durante la transizione da un modello di affiliazione all'altro. Questo unito al declino di RansomHub e LockBit hanno reso AKIRA un modello attraente per attori in cerca di alternative per mantenere vivo il loro progetto di monetizzazione. Gli operatori di AKIRA sono migliorati nel tempo sia a livello di impatto che di velocità d'esecuzione prospettando un ulteriore boost in termini di risultati, la recente attenzione data alle organizzazioni italiane può essere un primo indizio in un aumento di campagne malevole future nel nostro territorio.

DragonForce & NOVA - New Business, Old Money

La mutazione da RaaS a "Ransomware Cartel" lascia il segno come una delle innovazioni più interessanti dalla nascita del fenomeno ransomware globale. DragonForce, a costo di una commissione del 20% dei riscatti, offre ai propri clienti un'infrastruttura per avere presenza online, server FTP, ransomware ed altri strumenti necessari per le loro operazioni inserendo un logo/brand deciso dal cliente stesso. Admin Panels, manutenzione e gestione dei DLS/blog sta tutta in mano a DragonForce lasciando ai suoi affiliati il compito del deployment del loro ransomware. Tale offerta è sicuramente un qualcosa di inedito e che si e' riproposta da parte di NOVA ransomware nello stesso periodo dell'anno (gruppo che è stato intervistato dal team di **DarkLab**). NOVA ransomware ha attirato molte attenzioni all'interno del territorio italiano grazie alla pubblicazione del Comune di Pisa nel loro DLS, il gruppo ha inoltre recentemente attaccato Eurofins (azienda di Life Science con residenza in Lussemburgo) segnando il secondo attacco ransomware a danni dell'azienda dopo il precedente uso di ransomware all'interno dei loro sistemi nel 2019. Nell'intervista fatta a NOVA ransomware l'admin del gruppo ha voluto pubblicizzare i loro servizi che, oltre all'accesso a panel e al loro locker, include supporto per la creazione del "crypto business" dei loro affiliati. La nascita di questo nuovo tipo di servizi all'interno dell'ambito ransomware mira a ridurre ulteriormente l'asticella tecnica necessaria alla creazione di gruppi RaaS che potranno affidarsi a gruppi come DragonForce per ottenere un'identità nell'ambiente con un costo relativamente basso.

I THREAT ACTORS

PANORAMICA GRUPPI 2025

Cl0p - From 0 to 100

Dopo un periodo di stasi Cl0p ha ripreso le operazioni verso la fine del 2024 inaugurando il 2025 con ben 60 vittime pubblicate sul loro DLS nel mese di Gennaio, il gruppo ha dichiarato che tali organizzazioni sono state impattate tramite la campagna di sfruttamento della vulnerabilità 0-day del software Cleo (CVE-2024-50623). Nel solo mese di Febbraio invece, sempre grazie alla stessa CVE, sono state aggiunte 80 organizzazioni contenenti aziende di telecomunicazioni e asset healthcare con conseguente esfiltrazione di dati sensibili oltre alla cifratura delle reti interne. Cl0p ha raggiunto la top 3 dei gruppi del primo half 2025 evidenziando la loro tattica che potrebbe ripetersi nei periodi futuri, scoperta e sfruttamento di vulnerabilità 0 day da usare su larga scala. Tale gruppo ci ricorda come il patch management sulla superficie di attacco rimane tanto fondamentale quanto sottovalutata nelle organizzazioni in essere.

ANUBIS - Wipe them all

Il RaaS Anubis ha introdotto nella prima metà del 2025 la funzione “wipe mode” all’interno del suo ransomware che permette l’eliminazione completa dei file come alternativa alla cifratura a chiave asimmetrica. Utilizzare tale feature comprometterebbe il modello di estorsione tipicamente utilizzato dagli affiliati ma risulta utile per l’eliminazione di backup. ANUBIS ha inoltre introdotto nuovi schemi di monetizzazione oltre al semplice modello RaaS (80-20) includendo servizi di data extortion (60-40) e vendita di initial access (50-50).

I THREAT ACTORS

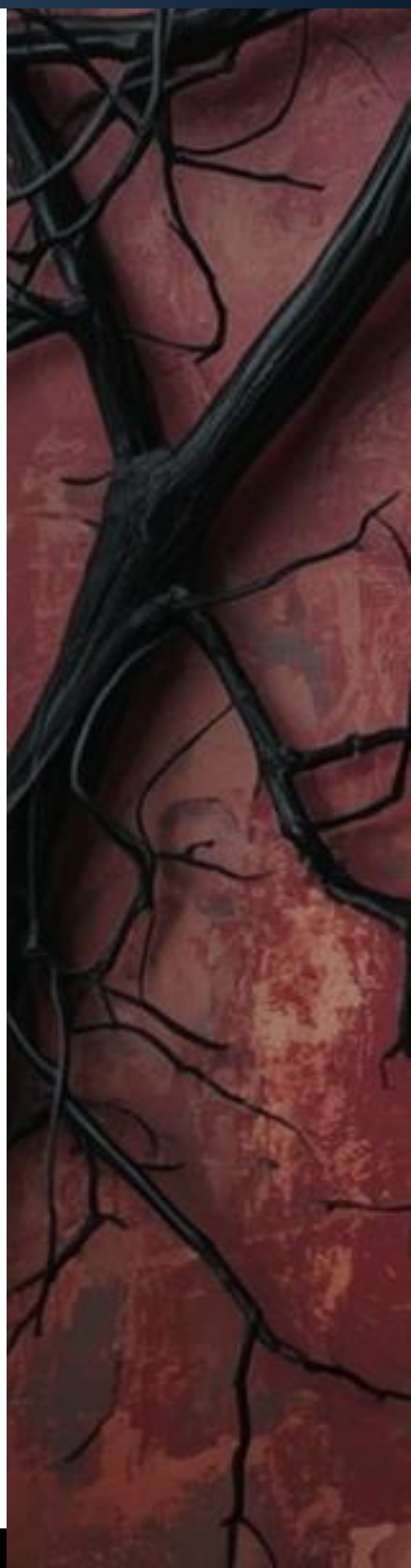
PANORAMICA GRUPPI 2025- NUOVI GRUPPI

FOG

Gli operatori di FOG hanno implementato all'interno delle loro campagne tool "esotici" come Syteca (software usato per keylogging e screen recording di dipendenti) e GC2 un C2 che utilizza google drive per eseguire comandi sulle macchine infettate. Inoltre Process WatchDog è stato utilizzato per restartare processi rilevanti, il tool Stowaway per tunneling e il C2 open source AdaptixC2 come alternativa a Cobalt Strike. Questa serie di tool non viene solitamente associata ad operazioni ransomware (ad esempio il tool GC2 è stato osservato durante operazione di APT41 di origine cinese) permettendo agli affiliati FOG di ottenere un buon livello di evasione.

XOXO from Prague

Il DLS di Everest ha subito un deface nel mese di Aprile sostituendo il contenuto della gang con un semplice testo HTML contenente "Don't do crime CRIME IS BAD xoxo from Prague", dopo poco tempo il DLS risultò offline. LockBit ha ricevuto un trattamento simile nel mese di Maggio dove un mirror del panel per gli affiliati è stato sostituito con lo stesso messaggio con in aggiunta la possibilità di scaricare un dump SQL contenente chat, wallet, username e altri valori contenuti nel backend del panel. Non è stato chiarito il soggetto od ente dietro a queste operazioni ma queste azioni riaprono il dibattito riguardo le operazioni "hacking back" ai danni dei gruppi RaaS e similari.



I THREAT ACTORS

PANORAMICA GRUPPI 2025- NUOVI GRUPPI

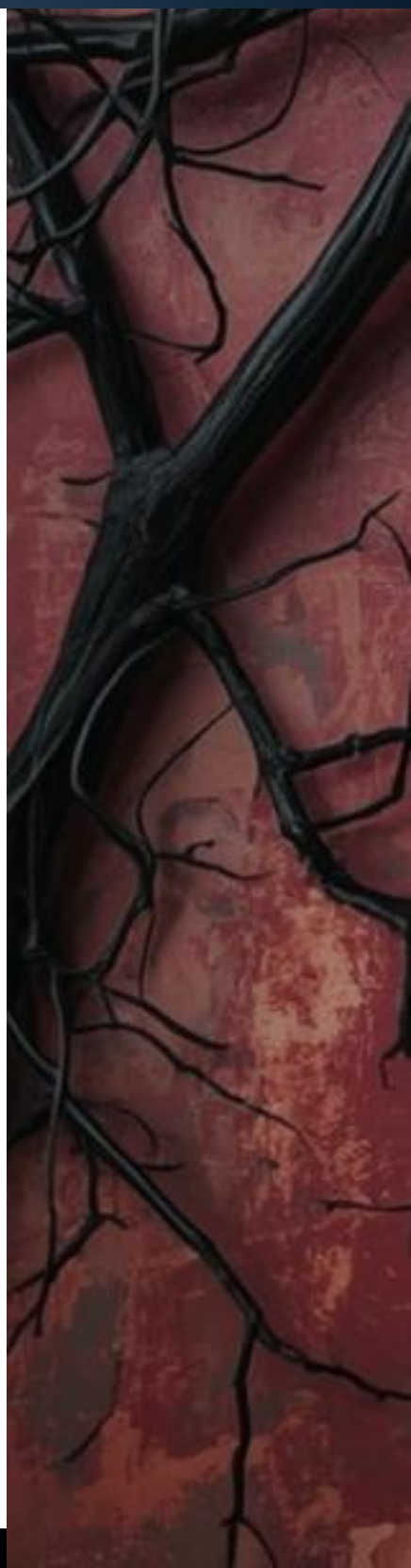
DIRE WOLF

Grazie al loro ransomware (programmato in Golang) Dire Wolf si presenta al pubblico nel mese di Maggio. Il loro tool ha un focus sul disinibire il log di Windows mentre le loro operazioni si spingono sui settori tech e manifatturiero (USA e Taiwan). Le vittime di Dire Wolf si espandono su 11 nazioni diverse continuando a pubblicare vittime nel mese di Giugno e Luglio.

.

ARKANA

Arkana Security ha messo piede nel settore ransomware nel Gennaio 2025 dove nella sezione “About” del loro DLS troviamo il logo di Qilin lasciando intendere una sorta di collaborazione tra i due soggetti (oppure un’estensione del network di Qilin). Non sono state scoperte istanze dove il gruppo ha utilizzato ransomware per la cifratura dei file mentre le attivita’ tracciate sono quelle di credential harvesting tramite infostealer e furto di dati con la quale premono le vittime al pagamento. Nonostante il collettivo sia recente e’ comunque riuscito ad impattare vittime di livello come “WOW!” (WideOpenWest azienda telco americana) ed ottenere accessi critici a backend di servizi come AppianCloud e Symphonica.



I THREAT ACTORS

PANORAMICA GRUPPI 2025- NUOVI GRUPPI

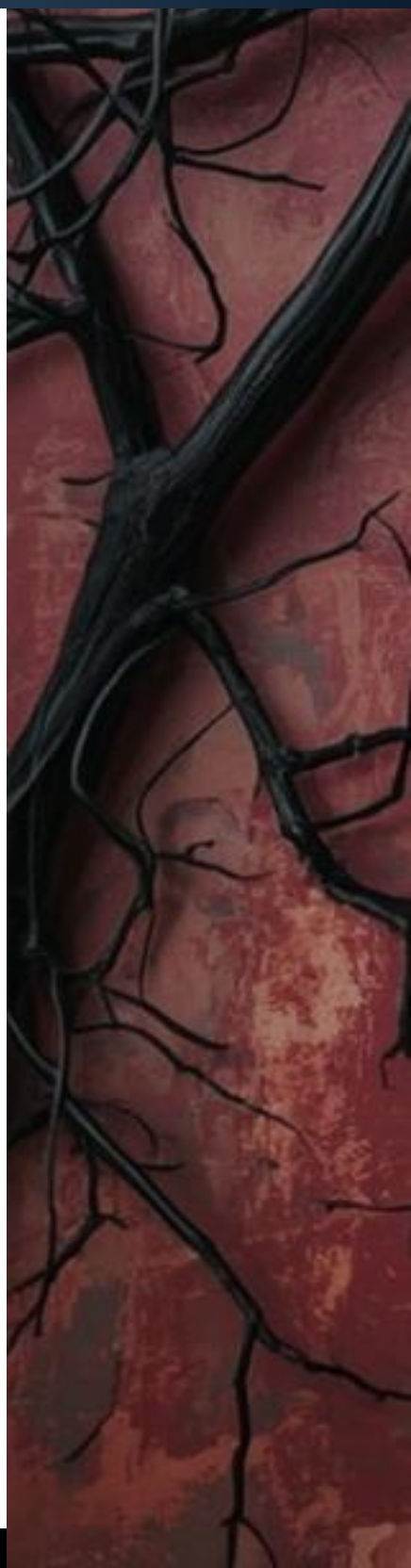
DARKGABOON

Tra tutti i gruppi emergente di questo H1 2025 DarkGaboon spicca rispetto alla concorrenza per la vittimologia scelta ovvero aziende localizzate in Russia. Tipicamente la regola non scritta “NO-CIS” rimane attiva nell’ambiente ransomware (escluse delle eccezzioni come BlackBasta e LockBit) ma questo gruppo ha deciso di agire indipendentemente da queste “tradizioni”. DarkGaboon e’ stato osservato per la prima volta ad Ottobre 2024 mostrando campagne di distribuzione di Revenge RAT ad aziende russe con più di 10 build diverse. Nel periodo primaverile il gruppo ha deciso di adottare una versione modificata del ransomware LockBit 3.0 (leakato nel 2022) per la cifratura dei dati senza pero’ evidenza di esfiltrazione. Attualmente non appare nessun DLS visto che le ransom note lasciate sulle macchine delle vittime includono indirizzi email per le negoziazioni.

FRAG

Con all’attivo 28 vittime (25 statunitensi, 1 olandese, 1 canadese ed 1 dal Singapore) da Febbraio 2025, Frag ransomware e’ riuscito ad ottenere una crescita notevole partendo da zero in maniera rapida. Frag ha fin da subito utilizzato la vulnerabilita’ CVE-2024-40711 di Veam Backup precedentemente usata da Akira per ottenere RCE sugli edge device vulnerabili. Le vittime di Frag contengono differenti organizzazioni appartenenti al settore sanitario. Le TTPs del gruppo includono l’utilizzo del tool RogueKiller (virus cleaner) per forzare la chiusura di programmi responsabili per la sicurezza degli endpoint

.



I THREAT ACTORS

PANORAMICA GRUPPI 2025- NUOVI GRUPPI

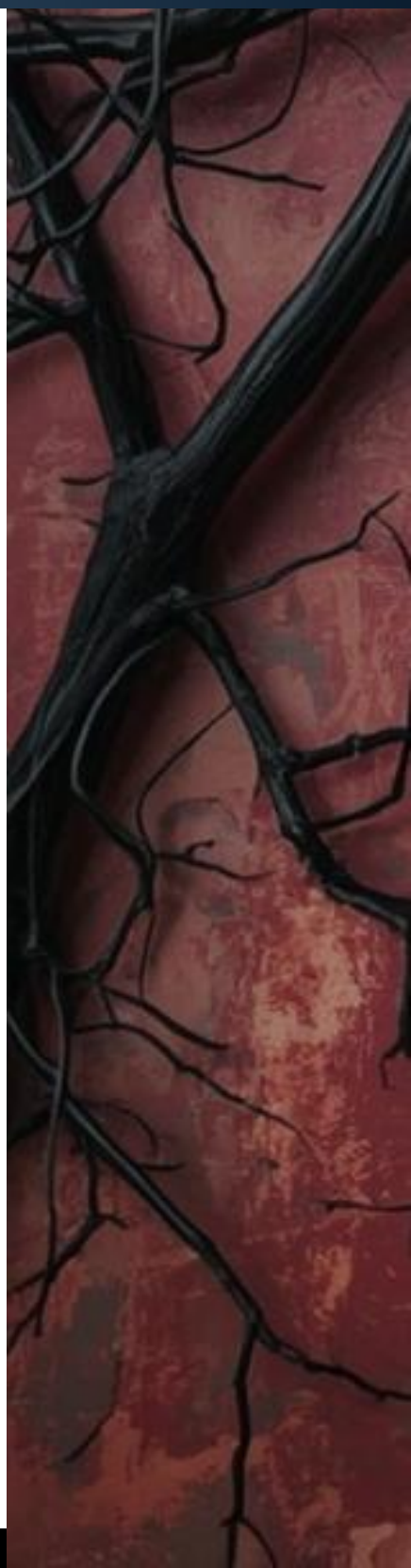
ELENOR-corp

Nell'Aprile 2025 l'uso di una variante di Mimic ransomware e' stato individuato ed attribuito ad una nuova minaccia chiamata ELENOR-corp. Il gruppo ha impattato il settore sanitario con un toolset creato ad-hoc per le necessita' del gruppo incluso un clipper hijacker e infostealer entrambi scritti in Python. Per poter evadere le difese ed ottenere persistenza (oltre ad eseguire il loro ransomware) ELENOR-corp utilizza il software legittimo NSSM (Non-Sucking Service Manager) per poter aggiungere/modificare services in Windows.

SUPERBLACK

La minaccia Mora_001 (etichettata da Forescout) ha implementato l'uso di una variante di LockBit3.0 (leakata nel 2022) all'interno delle sue operazioni basate sull'accesso iniziale tramite vulnerabilita' di Fortinet. Forescout ha chiamato questa nuova variante SuperBlack ed ha notato come nelle ransom note del malware mancasse il nome di LockBit ma mantenesse lo stesso TOX ID per le comunicazioni, gli analisti ipotizzano una relazione diretta tra SuperBlack e LockBit. All'interno del ransomware sono state cambiate delle componenti interne ed aggiunte delle altre quali l'inclusione dell'exfiltration tool di Mora_001. Oltre al ransomware e' stato uploadato sulle macchine delle vittime un wiper denominato "WipeBlack" precedentemente attribuito a BrainChiper e LockBit, nelle fasi di reverse engineering si e' notata una somiglianza tra il builder di LockBit3.0 e quello wiper in discussione. Tale tool e' utilizzato dagli operatori per rimuovere evidenze, file e log delle loro azioni sulle macchine andando a ripulire gli endpoint e complicare le fasi di incident response.

.

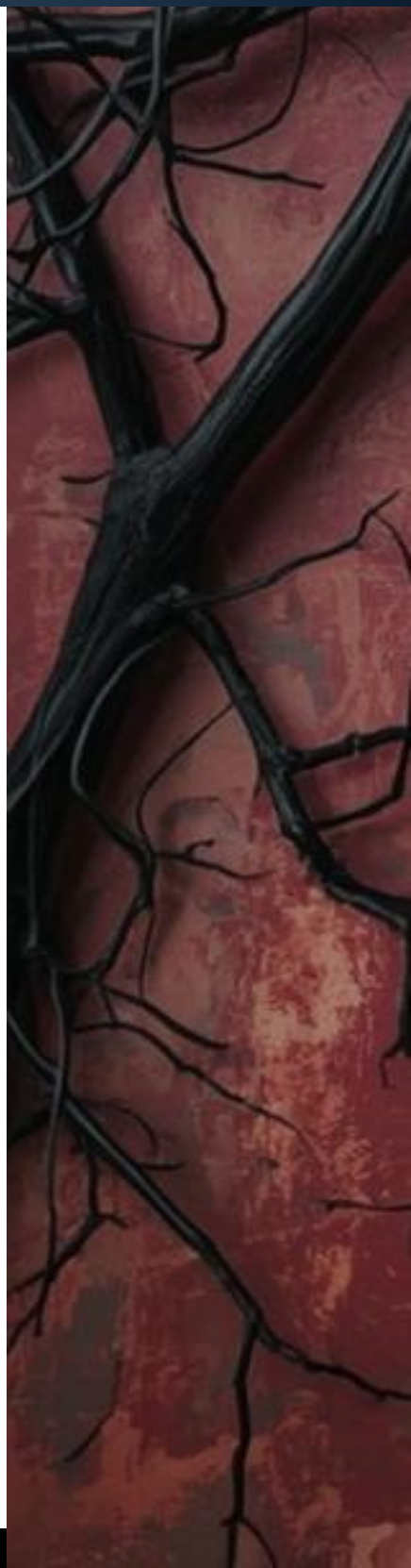


I THREAT ACTORS

PANORAMICA GRUPPI 2025- NUOVI GRUPPI

WARLOCK

Dopo la chiusura di BlackBasta nel Febbraio 2025 un nuovo gruppo ha pubblicato due vittime precedentemente pubblicate sul DLS di BB, tale gruppo si chiama Warlock con prima apparizione nel mese di Giugno. Quasi metà delle vittime di Warlock (circa 20) appartengo al settore pubblico ed energetico sparse nel continente americano e sud asiatico. Secondo gli analisti dietro a Warlock potrebbe esserci un gruppo che fu affiliato sia a BlackBasta che LockBit etichettato come Storm-2063 che avrebbe origini cinesi. Il ransomware di Warlock non ha evidenze di essere un rebrand o riscrittura di famiglie esistenti. Il gruppo ha esaustivamente usato la vulnerabilita' ToolShell su circa 400 macchine (sia come attacchi a se stanti sia con campagne ransomware tramite Warlock) in poche settimane dalla pubblicazione della 0-day. Nonostante la natura attribuita a Warlock non sono state assegnate motivazioni differenti da quelle economiche tralasciando, per ora, motivazioni politiche o di spionaggio digitale.



ECONOMIA RaaS H1 2025

ANDAMENTO DEL FENOMENO ECONOMICO DEL RANSOMWARE

A cura di Edoardo Faccioli e Alessio Stefan

ECONOMIA RaaS H1 2025

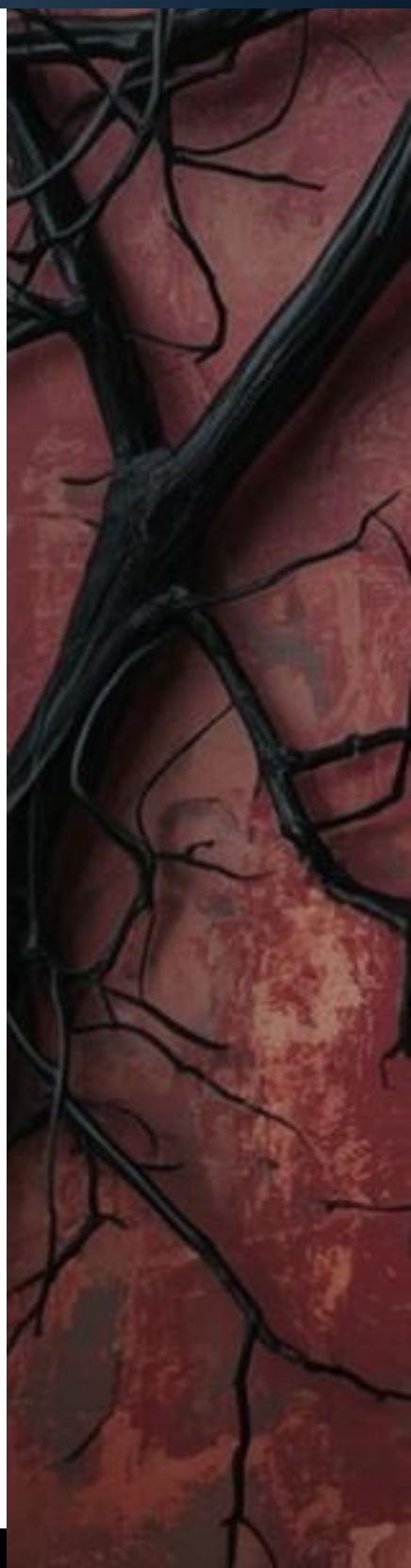
ANDAMENTO DEL FENOMENO ECONOMICO DEL RANSOMWARE

Il modello di attacco ransomware si sostiene principalmente attraverso i profitti derivanti dalle estorsioni successive agli attacchi. La motivazione primaria dei gruppi **RaaS** e dei loro affiliati è di natura **economica**: la maggior parte degli attori non persegue obiettivi ideologici, ma mira esclusivamente all'arricchimento personale e al miglioramento del proprio stile di vita.

Nel report **DarkMirror H2 2024** sono stati analizzati la struttura di **Evil Corp** e il gruppo **LockBit**, con particolare attenzione all'operazione Cronos e alle tecniche di riciclaggio impiegate per movimentare i flussi finanziari, al fine di reinserire i proventi illeciti nel circuito economico legittimo.

Per comprendere appieno l'andamento del fenomeno ransomware, oltre all'analisi della struttura delle gang, delle loro **TTP**, e della mentalità di amministratori e affiliati, è fondamentale valutare anche l'evoluzione del mercato e delle dinamiche estorsive.

Analizzando i dati sugli **attacchi rispetto agli anni precedenti** e considerando le operazioni di successo condotte dalle forze dell'ordine, sorge spontanea una domanda: il fenomeno è in costante declino oppure, nonostante i colpi inflitti dalle autorità e il miglioramento delle capacità difensive delle vittime, **il ransomware continua a rappresentare un'attività criminale redditizia e in grado di conseguire numerosi successi illeciti, inoltre gli attacchi stanno veramente aumentando**?



ECONOMIA RaaS H1 2025

ANDAMENTO DEL FENOMENO ECONOMICO DEL RANSOMWARE

Andamento del fenomeno Economico del Ransomware

I dati che emergono sui **Data Leak Site** (DLS) dei gruppi ransomware riguardano solo gli attacchi che hanno soddisfatto specifici requisiti stabiliti dagli attaccanti, tra cui:

Operazione completata con successo, con un impatto significativo sulla vittima

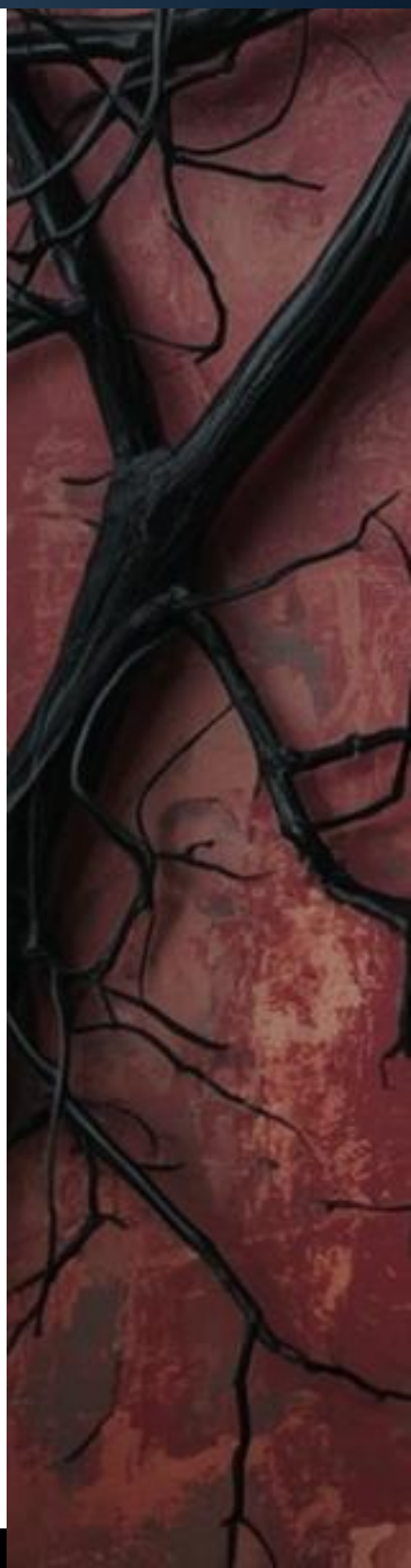
Avvio di una negoziazione da parte della vittima senza risposta da quest'ultima o fallimento nelle negoziazioni

Se una delle fasi critiche, come la crittografia, l'esfiltrazione dei dati o entrambe, fallisce, l'attaccante non ha possibilità di procedere con l'estorsione. Di conseguenza, solo gli attacchi che hanno raggiunto **almeno uno** di questi obiettivi vengono pubblicati sul DLS come "avvenuto attacco".

È importante sottolineare che non tutti gli attacchi vengono pubblicati sul network TOR. Inoltre, negli ultimi anni, molti gruppi ransomware e attori malevoli hanno adottato nuove modalità di monetizzazione dei dati rubati, abbandonando la pubblicazione sul proprio DLS (il cosiddetto "muro della vergogna") a favore di approcci alternativi, tra cui:

- Vendita tramite aste online
- Pubblicazione su forum pubblici o privati, con richieste di denaro in cambio dei dati esfiltrati
- Utilizzo per potenziali campagne

Questa evoluzione comporta una riduzione della visibilità complessiva: non tutti i post sono pubblici, facilmente accessibili o tracciabili, rendendo complessa la raccolta di una telemetria completa sulle vittime effettive.



ECONOMIA RaaS H1 2025

ANDAMENTO DEL FENOMENO ECONOMICO DEL RANSOMWARE

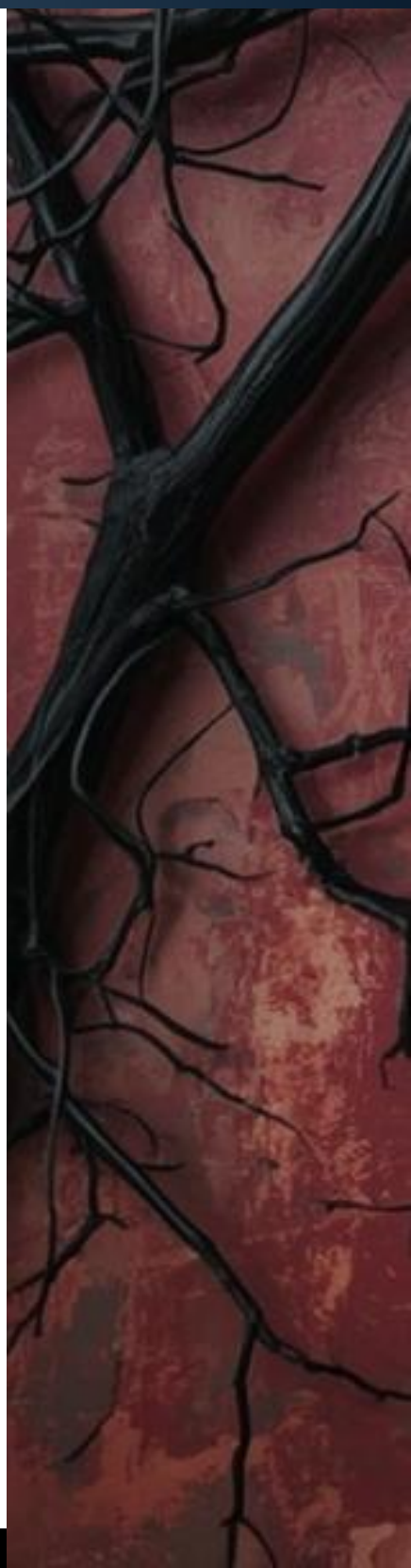
È importante evidenziare che le vittime vengono generalmente pubblicate sui DLS quando rifiutano di pagare il riscatto. Di conseguenza, un aumento del numero di vittime elencate su tali portali potrebbe indicare una diminuzione della percentuale di pagamento dei riscatti, suggerendo che sempre più organizzazioni scelgono di non cedere alle richieste estorsive.

Le attività di contrasto da parte delle forze dell'ordine hanno avuto un impatto significativo sul cybercrime, in particolare grazie all'Operazione Cronos, che ha dato il via a numerose azioni simili, con arresti e sanzioni mirate.

In questo contesto, lo scenario ransomware ha iniziato a modificarsi, portando a una frammentazione dei gruppi esistenti, alla nascita di nuove entità e alla chiusura di operatori storici. Questo continuo movimento rappresenta un chiaro indice di resilienza da parte degli attori criminali, che hanno mantenuto vivo l'ecosistema delle estorsioni informatiche nonostante i colpi inflitti dalle autorità. Nei primi tre mesi del 2025 sono stati rilevati un numero di attacchi superiori rispetto allo stesso periodo 2023 e 2024.

Analizzando la struttura e l'evoluzione del fenomeno, non possiamo affermare con certezza che il numero complessivo di attacchi stia realmente aumentando. L'andamento osservabile si basa esclusivamente sugli incidenti di cui siamo a conoscenza, ovvero quelli pubblicati sui DLS o rivendicati da attori malevoli.

I dati disponibili mostrano un incremento degli attacchi resi pubblici, ma questo deve essere interpretato in relazione a un altro fattore: la probabile diminuzione del numero di riscatti pagati. Come già evidenziato, la pubblicazione dell'attacco sul DLS rappresenta per l'attaccante l'ultima possibilità di ottenere un profitto dall'operazione, una volta fallita la negoziazione con la vittima.

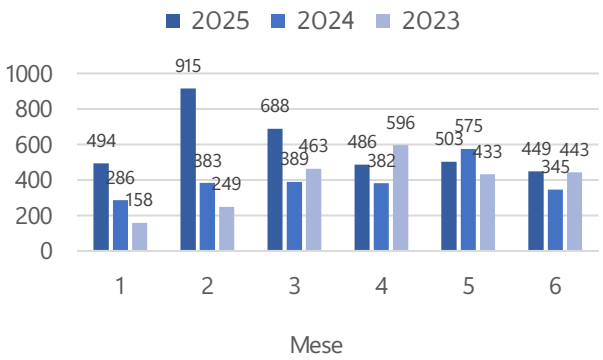


ECONOMIA RaaS H1 2025

ANDAMENTO DEL FENOMENO ECONOMICO DEL RANSOMWARE

Considerando che nei mesi invernali si registra tradizionalmente un incremento degli attacchi, possiamo analizzare l'andamento di quest'anno rispetto agli anni precedenti.

Nel 2023, la differenza rispetto al 2024 – sia nel primo semestre (H1) che sull'intero anno – è risultata minima, evidenziando una tendenza complessivamente stabile. In quel periodo, i pagamenti dei riscatti avevano un tasso di successo maggiore; di conseguenza, possiamo dedurre che il numero di vittime riportate sui DLS non riflette necessariamente il volume reale degli attacchi.



Attachi per mese	Anno		
Mese	2025	2024	2023
1	494	286	158
2	915	383	249
3	688	389	463
4	486	382	596
5	503	575	433
6	449	345	443
Totale generale	**3535**	**2360**	**2342**

Il vero cambio di tendenza si osserva tra il 2024 e il 2025, con un aumento del 49,79% (+1.175 attacchi) già nel solo H1. Ancora più significativo è il confronto tra il 2023 e il 2025, che mostra una crescita superiore al 50% nel primo semestre.

Mantenendo il focus su questi dati, analizziamo ora l'andamento dei pagamenti in criptovalute derivanti da estorsioni post-attacco ransomware. Secondo gli analisti di Chainalysis, negli ultimi anni i pagamenti sono diminuiti del 35%.

Questo solleva un interrogativo cruciale: ha ancora senso, per un attaccante, investire risorse in operazioni ransomware se le probabilità di ricevere il riscatto si stanno riducendo? La tendenza delle vittime a non pagare potrebbe, nel lungo periodo, condurre al declino – se non alla scomparsa – di questo modello criminale.

Tuttavia, è importante ricordare che i dati rubati mantengono un valore significativo nel mercato underground. Anche in assenza di pagamento, un attaccante che ha condotto con successo un'esfiltrazione può monetizzare i dati vendendoli o sfruttandoli per ulteriori attività criminali, oltre a tentare comunque un'estorsione.

ECONOMIA RaaS H1 2025

ANDAMENTO DEL FENOMENO ECONOMICO DEL RANSOMWARE

Influenza di assicurazioni e regolamentazione

La diffusione delle polizze assicurative cyber ha avuto un impatto diretto sul comportamento degli attori ransomware. In alcuni casi, la consapevolezza della copertura induce i criminali a modulare le richieste in base ai massimali assicurativi stimati; in altri, le compagnie scoraggiano il pagamento per ridurre il rischio di incentivare ulteriori attacchi.

Sul fronte normativo, provvedimenti come il GDPR in Europa o le regole SEC negli Stati Uniti impongono segnalazioni rapide degli incidenti, aumentando la trasparenza ma anche la pressione reputazionale sulle aziende colpite. Parallelamente, le sanzioni OFAC e analoghi regimi internazionali rendono rischioso, se non illegale, il pagamento verso gruppi collegati a stati ostili, incidendo sul tasso di riscatti saldati

In calo le estorsioni che ottengono un risultato positivo

Nel 2024 i gruppi ransomware hanno incassato circa 813,55 milioni di dollari in pagamenti da parte delle vittime, registrando una diminuzione del 35% rispetto al 2023.

Il 2024 si è distinto come un anno anomalo: nella prima metà (H1) si è osservato un picco nei pagamenti, con un incremento del 2,38% rispetto allo stesso periodo del 2023. Tuttavia, questa tendenza si è invertita nella seconda metà dell'anno (H2), che ha registrato un forte calo, portando il totale annuo a una riduzione complessiva del 34,9% rispetto all'anno precedente. L'H1 2024 ha visto anche alcuni pagamenti molto importanti, come il record da 75 milioni di dollari estorto da Dark Angels.

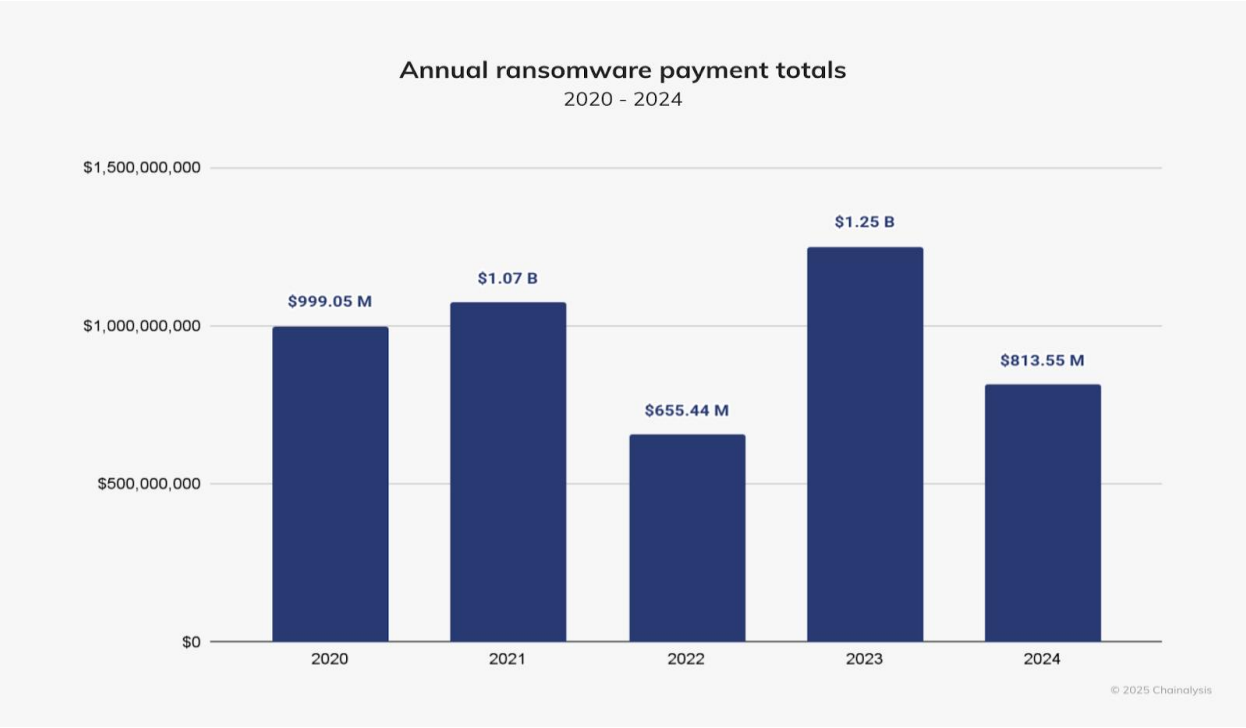
Fonte:

- https://www.chainalysis.com/blog/crypto-crime-ransomware-victim-extortion-2025/
- https://www.redhotcyber.com/post/75-milioni-di-dollari-e-il-riscatto-per-il-ransomware-finito-nelle-tasche-di-dark-angeles/

ECONOMIA RaaS H1 2025

ANDAMENTO DEL FENOMENO ECONOMICO DEL RANSOMWARE

Come evidenziato in precedenza, il numero di vittime è aumentato già nel 2024, ma i pagamenti registrati hanno continuato a diminuire, una tendenza che si sta confermando anche nel 2025.

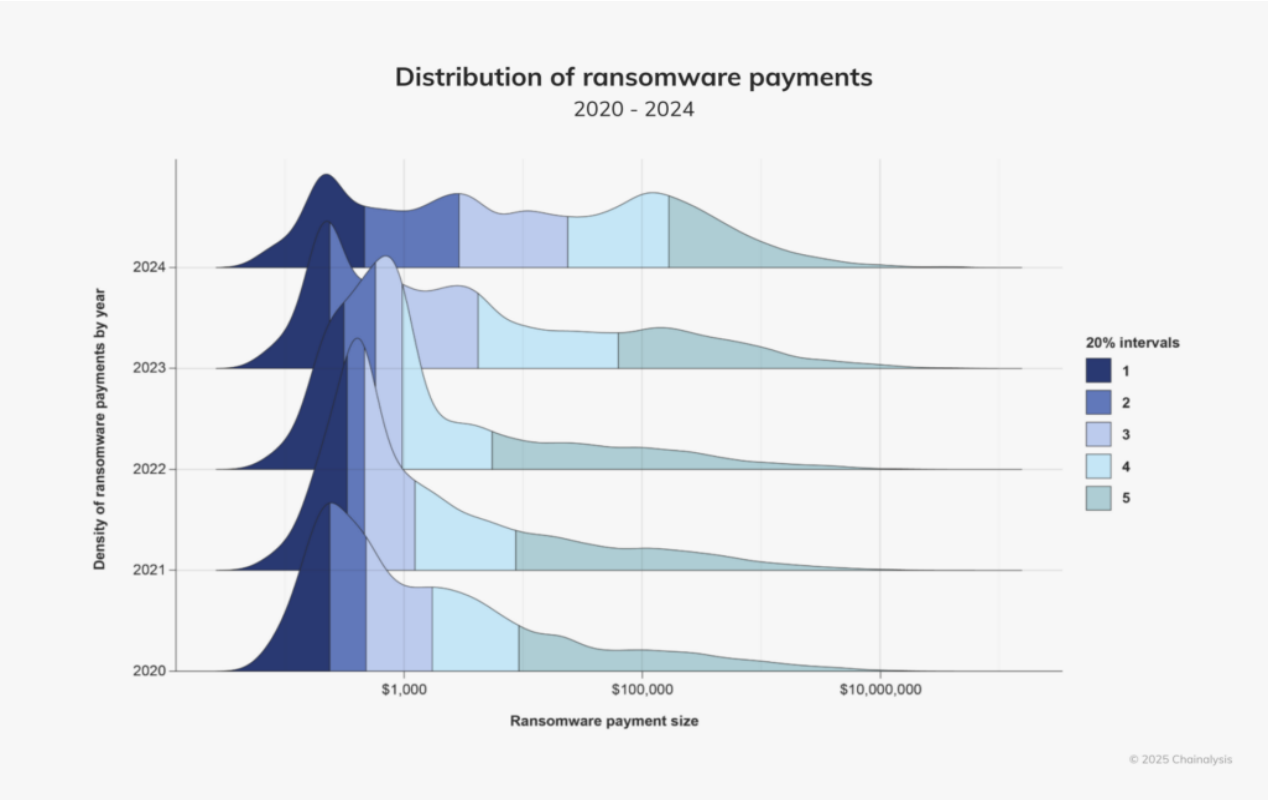


Secondo Dan Saunders, intervistato da Chainalysis, solo circa il 30% delle trattative porta effettivamente a un pagamento da parte delle vittime. Le decisioni di pagare o meno dipendono principalmente dal valore percepito dei dati compromessi. Inoltre, Saunders sottolinea che, grazie a una migliore igiene informatica e a una maggiore resilienza complessiva, le vittime sono oggi più in grado di resistere alle richieste di riscatto e valutare alternative per riprendersi da un attacco senza cedere al pagamento.

ECONOMIA RaaS H1 2025

ANDAMENTO DEL FENOMENO ECONOMICO DEL RANSOMWARE

Un'analisi aggiuntiva ha evidenziato come gli importi richiesti a titolo di riscatto siano aumentati nel tempo, superando in molteplici casi la soglia delle 7 e 8 cifre. Gli attaccanti modulano la cifra richiesta in base al tipo di vittima e alla qualità e rilevanza dei dati rubati.



La redditività del ransomware è legata anche a fattori macroeconomici: il valore delle criptovalute, la stabilità dei mercati, e la pressione economica sulle aziende influenzano la propensione a pagare. La volatilità delle crypto può ridurre il ROI atteso dagli attaccanti, portandoli a diversificare le fonti di guadagno.
Sul piano tecnologico, è probabile che i modelli RaaS e MaaS si integrino con strumenti di automazione e intelligenza artificiale, aumentando l'efficienza e la scalabilità degli attacchi, ma anche abbassando la soglia tecnica d'ingresso per criminali meno esperti. Già oggi servizi come DragonForce offrono soluzioni chiavi in mano per attori poco organizzati.

Conclusione

Dalle analisi condotte e dai dati raccolti sembrerebbe emergere un quadro dove non si registra un aumento nel numero di attacchi ransomware, ma piuttosto una diminuzione dell'efficacia nelle estorsioni. Il calo nei pagamenti è evidente.

Le operazioni delle forze dell'ordine hanno portato, come già detto, alla scomparsa di alcuni grandi "hub" o attori principali come LockBit, ALPHV/BlackCat e RansomHUB. Fanno eccezione solo Hunters e ClOP, che mantengono ancora un netto vantaggio. Si sta assistendo a una vera e propria "democratizzazione" delle vittime, con una distribuzione più equilibrata del numero di affiliati tra i vari gruppi. Questa frammentazione spiega perché le richieste più alte siano spesso casi isolati, eccezioni e non una tendenza generale.

Nonostante la diminuzione del tasso di pagamento, l'importo totale richiesto varia molto da vittima a vittima, permettendo ai criminali di ottenere somme molto elevate in casi specifici. Non è necessario aumentare il numero complessivo di attacchi reali, perché questo aumenterebbe il rischio di essere scoperti e arrestati. Pertanto, non vi sono evidenze sufficienti per considerare significativo un incremento degli attacchi ransomware; la sfida principale rimane il mantenimento e il potenziamento delle capacità di contrasto e di interruzione efficace di tali operazioni.

Con il calo della soglia tecnica necessaria per lanciare attacchi ransomware, sono nati nuovi servizi rivolti a soggetti meno esperti, interessati a ridurre i costi e semplificare le operazioni, come DragonForce o i modelli MaaS (Malware-as-a-Service). Questi servizi rappresentano una porta d'ingresso per attori meno qualificati o poco organizzati.
Nel breve termine, la sfida principale per le difese sarà doppia: mantenere alta la capacità di contrasto operativo e prevenire la proliferazione di modelli di attacco a basso costo e bassa competenza, che potrebbero ampliare la platea di attori coinvolti.

Law Enforcement H1 2025

IL RUOLO DELLE FORZE DELL'ORDINE NELLA LOTTA CONTRO IL RANSOMWARE

A cura di Raffaela Crisci e Alessio Stefan

Law Enforcement H1 2025

IL RUOLO DELLE FORZE DELL'ORDINE NELLA LOTTA CONTRO IL RANSOMWARE

Il primo semestre del 2025 ha confermato un quadro complesso e dinamico nel panorama della cybersecurity globale, con una crescita significativa delle attività ransomware e una risposta sempre più coordinata da parte delle autorità internazionali.

L'evoluzione tecnica delle minacce, l'espansione dei modelli di business criminale e l'innovazione nelle tattiche hanno reso necessario un approccio multilivello, combinando interventi operativi, azioni legali e collaborazione tra settore pubblico e privato. Questo report analizza le principali operazioni internazionali, i gruppi coinvolti e gli impatti registrati, delineando i trend emergenti e suggerendo raccomandazioni per la mitigazione.

1. Operazione Cronos & LockBit 4.0

LockBit è stato, per gran parte degli ultimi anni, il gruppo ransomware più attivo e strutturato al mondo, con una rete di affiliati globale e un modello di business maturo basato su ransomware-as-a-service. La sua capacità di rinnovarsi rapidamente e adattare le tecniche di attacco lo aveva reso una minaccia costante per aziende e istituzioni. L'Operazione Cronos, ha rappresentato una delle più incisive azioni internazionali contro un'infrastruttura criminale di questo tipo, con l'obiettivo di scomporre il cuore operativo di LockBit e minare la fiducia nel suo network di affiliati.

Nel febbraio 2024, l'Operazione **Cronos** – coordinata da FBI, Europol, NCA (UK) e CISA – ha colpito in profondità l'ecosistema LockBit 3.0, smantellando parte delle infrastrutture di comando e controllo (C2) e sequestrando diversi mirror Tor utilizzati per negoziare riscatti e pubblicare dati rubati.
Questo ha rappresentato uno dei colpi più incisivi mai inflitti al gruppo, con impatti operativi immediati ma non permanenti.

Riepilogo fase 2024

Infiltrazione della rete affiliati con acquisizione di credenziali interne e chat riservate con l'operatore "LBSupp". Sequestro di 10 server C2 e delle relative hidden services Tor. Rilascio di decryptor aggiornati tramite NoMoreRansom, consentendo la restituzione di dati a centinaia di vittime. Arresti: due affiliati in Ucraina e uno in Polonia. Pubblicazione di un tool di decryption open-source (GitHub) sviluppato in collaborazione con Kaspersky. Recupero di quasi 7.000 chiavi di decrittazione, impattando retroattivamente numerosi incidenti. LockBit è rimasto offline per circa due settimane, con calo visibile di campagne e blocco temporaneo del programma di affiliazione. Sono emersi collegamenti con ex-attori REvil, portando il gruppo a introdurre una selezione più stringente per nuovi affiliati.

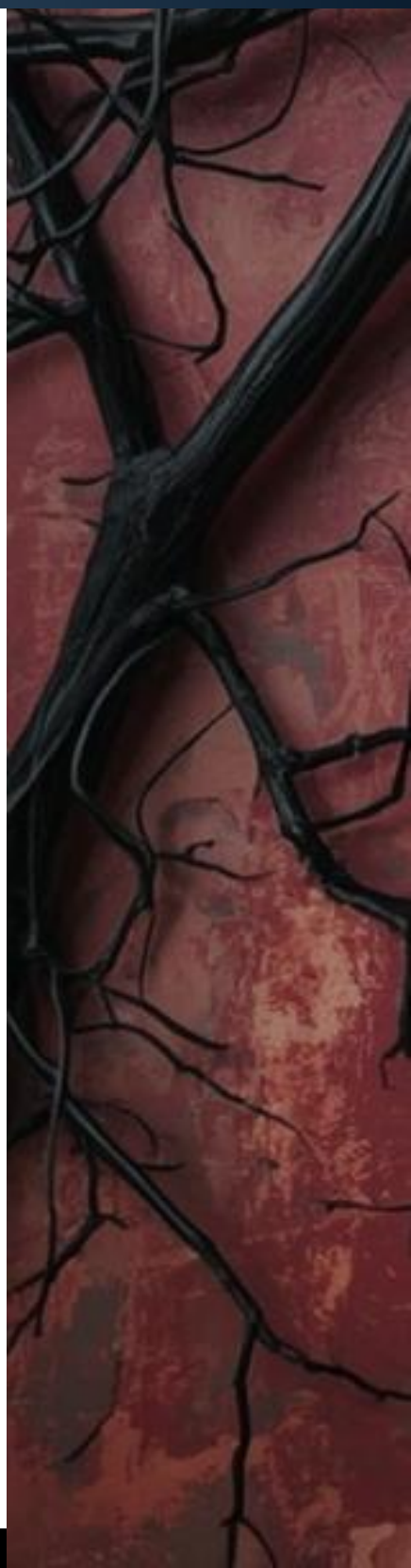
Law Enforcement H1 2025

Il Ruolo delle Forze dell'Ordine nella Lotta contro il RANSOMWARE

Riepilogo fase 2024

- **Infiltrazione della rete affiliati** con acquisizione di credenziali interne e chat riservate con l'operatore "**LBSupp**".
- **Sequestro di 10 server C2** e delle relative hidden services Tor.
- Rilascio di **decryptor aggiornati** tramite **NoMoreRansom**, consentendo la restituzione di dati a centinaia di vittime.
- **Arresti**: due affiliati in Ucraina e uno in Polonia.
- Pubblicazione di un tool di decryption open-source (GitHub) sviluppato in collaborazione con Kaspersky.
- **Recupero di quasi 7.000 chiavi di decrittazione**, impattando retroattivamente numerosi incidenti.

LockBit è rimasto offline per circa due settimane, con calo visibile di campagne e blocco temporaneo del programma di affiliazione.
Sono emersi collegamenti con ex-attori REvil, portando il gruppo a introdurre una selezione più stringente per nuovi affiliati.



Law Enforcement H1 2025

IL RUOLO DELLE FORZE DELL'ORDINE NELLA LOTTA CONTRO IL RANSOMWARE

LockBit 4.0

Il **3 febbraio 2025** il gruppo ha annunciato la nuova versione **LockBit 4.0**, completamente riscritta in Rust linguaggio moderno che offre vantaggi significativi in termini di portabilità e resistenza al reverse engineering rispetto a C++ o Python usati in precedenza e dotata di:

- Crittografia ibrida AES-256 + RSA-4096 (https://lockbitdecryptor.com/lockbit-4-0-ransomware-a-new-threat-emerges/)
- Esecuzione in Safe Mode per bypassare processi difensivi
- Shadow copy deletion per ostacolare il recovery
- Tecniche avanzate di self-protection:
    - modalità quiet (no modifica date/estensioni file)
    - caricamento DLL via proxy
    - rimozione VEH debug handler
    - packer UPX non protetto per velocizzare la distribuzione
    - estensioni criptate con hash random di 12 caratteri

LockBit 4.0 ha rafforzato il modello double extortion:
Criptaggio selettivo veloce
Esfiltrazione dati sensibili
Minaccia di pubblicazione su leak site
Il leak site rimane attivo ma con reclutamento affiliati più discreto, evitando forum pubblici e privilegiando canali chiusi e referral. **Microsoft** e **CISA** stimano che entro giugno 2025 **LockBit 4.0 è stato responsabile di oltre il 22 % di tutti gli attacchi ransomware globali**. Malgrado il colpo subito da Cronos (quasi 7.000 chiavi decrittazione recuperate), **LockBit mantenne una posizione dominante** nella prima metà del 2025, fino all'affermazione di gruppi emergenti come **RansomHub.**

Law Enforcement H1 2025

IL RUOLO DELLE FORZE DELL'ORDINE NELLA LOTTA CONTRO IL RANSOMWARE

Eventi rilevanti post-Cronos

Marzo 2025 – *Estradizione di **Rostislav Panev** negli USA*, sviluppatore chiave di **LockBit**. Le prove sequestrate includevano credenziali interne, conversazioni con "LBSupp" e codice sorgente di versioni inedite del ransomware.

Maggio 2025 – *Data breach interno*: Il gruppo ha subito anche un data breach in maggio 2025: un dump SQL ha rivelato dettagli sull'affiliate program (80+ membri), password in chiaro, indirizzi Bitcoin (quasi 60.000) e conversazioni interne, sfruttando una vulnerabilità in PHP 8.1.2 RCE.
Impatto: temporanea chiusura di più nodi C2 e sospensione forzata delle attività di negoziazione

L'operazione Cronos, pur avendo ottenuto risultati immediati significativi, ha evidenziato la **resilienza e capacità di reingegnerizzazione rapida di LockBit**.

LockBit 4.0 rappresenta un'evoluzione tecnica e organizzativa che riflette la crescente professionalizzazione del cybercrime: minor visibilità pubblica, uso di linguaggi moderni e tecniche anti-analisi rendono più difficile il contrasto. Nonostante la pressione delle forze dell'ordine, LockBit mantiene una quota significativa del mercato ransomware, costringendo a innovare continuamente le strategie difensive.

Law Enforcement H1 2025

IL RUOLO DELLE FORZE DELL'ORDINE NELLA LOTTA CONTRO IL RANSOMWARE

2. Operazione Endgame

Negli ultimi anni, il ruolo dei malware broker specializzati nell' **Initial Access Brokers** (IAB) è diventato cruciale nell'economia del cybercrime. Questi attori forniscono a gruppi ransomware e altri criminali digitali l'accesso diretto a reti compromesse, facilitando la fase iniziale degli attacchi. L'**Operazione Endgame**, nella sua nuova fase di maggio 2025, ha ampliato il raggio d'azione oltre le tradizionali **botnet**, mirando direttamente a questo segmento chiave del **mercato criminale** e colpendo una serie di gruppi che agivano come fornitori di accesso-as-a-service.

Nel maggio 2025 le forze dell'ordine internazionali hanno portato a termine una nuova, decisiva fase **dell'Operazione Endgame**, estendendo l'obiettivo oltre le tradizionali botnet e puntando direttamente al cuore del mercato criminale dell'accesso iniziale. Per quattro giorni, tra il 19 e il 22 maggio, un'ampia coalizione guidata da **Europol** e **Eurojust**, con il supporto di Stati Uniti, Germania, Regno Unito e Canada, ha colpito i principali malware broker che forniscono ai **gruppi ransomware** le **credenziali e gli accessi compromessi** alle reti aziendali.

Nel mirino sono finite famiglie di malware particolarmente diffuse come **Qakbot**, **DanaBot**, **Trickbot**, **Latrodectus**, **Bumblebee**, **WarmCookie** e **HijackLoader**. Questi strumenti, spesso invisibili agli utenti comuni, rappresentano il primo anello della cosiddetta **ransomware kill chain**: infettano i sistemi, **aprono backdoor persistenti** e **rivendono l'accesso ad altri criminali**, che poi eseguono le fasi successive di **cifratura ed estorsione**.

Law Enforcement H1 2025

IL RUOLO DELLE FORZE DELL'ORDINE NELLA LOTTA CONTRO IL RANSOMWARE

Risultati operativi:

- Neutralizzazione di oltre 300 server e rimozione di circa 650 domini malevoli (https://thehackernews.com/2025/05/300-servers-and-35m-seized-as-europol.html)
- Sequestro di € 3,5 milioni in criptovalute, che si aggiungono ai € 17,7 milioni già confiscati nelle precedenti fasi (totale oltre € 21 milioni)
- Emissione di 20 mandati di arresto internazionali, con diversi sospettati inseriti nella lista europea dei più ricercati (https://www.reuters.com/technology/eu-us-authorities-take-down-malware-network-2025-05-23/)

Sul fronte giudiziario, il Dipartimento di Giustizia statunitense ha formalizzato accuse contro sedici individui legati a **DanaBot** e ha incriminato **Rustam Gallyamov**, ritenuto un leader chiave dell'ecosistema Qakbot. Negli stessi documenti è stato richiesto **il sequestro di oltre 24 milioni di dollari** in fondi, sia fiat che crypto. Le indagini hanno anche rivelato come alcune varianti di DanaBot fossero state adattate per colpire obiettivi governativi e diplomatici, confermando il crescente interesse dei broker di accesso per settori strategici.

Europol ha definito questa fase di **Endgame** una delle più efficaci mai realizzate, sottolineando come sia riuscita a "**rompere la kill chain del ransomware alla fonte**". Colpendo direttamente il mercato degli accessi compromessi, l'operazione ha reso più difficile e costoso per i gruppi criminali avviare nuove campagne, generando un impatto tangibile sulle attività di diversi operatori ransomware nelle settimane successive.

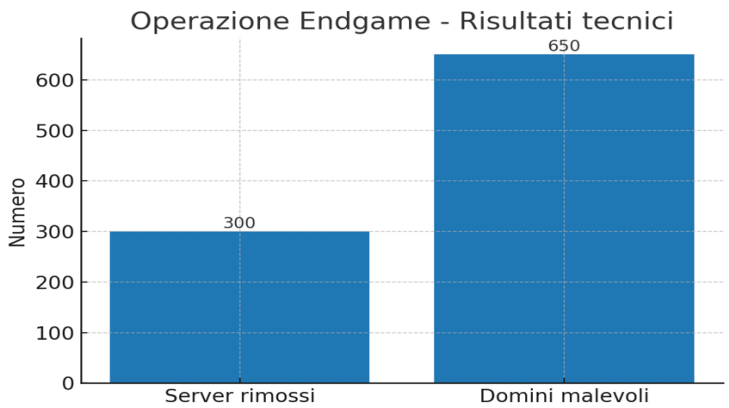
Law Enforcement H1 2025

IL RUOLO DELLE FORZE DELL'ORDINE NELLA LOTTA CONTRO IL RANSOMWARE

3. Operazione 8Base / Phobos

Nel panorama del cybercrime, il ransomware Phobos ha rappresentato negli ultimi anni una delle minacce più persistenti e adattive, specialmente contro le piccole e medie imprese meno preparate a sostenere attacchi sofisticati. La sua rete di affiliati, tra cui spiccava il gruppo 8Base, operava con metodiche collaudate di doppia estorsione e una notevole capacità di penetrazione in diversi settori industriali. L'azione congiunta di febbraio 2025 ha segnato un punto di svolta nella strategia di contrasto a questo ecosistema, colpendo al cuore una delle sue cellule più organizzate.

L'11 febbraio 2025, un'operazione internazionale coordinata tra agenzie europee, statunitensi, giapponesi e britanniche ha portato all'arresto di quattro leader del gruppo criminale 8Base, affiliato al ransomware Phobos, e al sequestro di 27 server utilizzati per la gestione delle campagne malevole.
Il gruppo Phobos, e in particolare la cellula 8Base, aveva preso di mira principalmente piccole e medie imprese dei settori manifatturiero, istruzione e trasporti, sfruttando un modello di doppia estorsione: criptazione dei dati seguita dalla minaccia di pubblicazione in caso di mancato pagamento.



L'operazione ha prodotto un impatto immediato: riduzione significativa degli attacchi distribuiti da 8Base, rallentamento del reclutamento di nuovi affiliati e apertura di indagini parallele su altri gruppi che utilizzavano i servizi di Phobos. Gli investigatori ritengono che l'azione abbia interrotto almeno temporaneamente una delle catene di distribuzione ransomware più attive dell'ultimo anno.

4. Operazione Eastwood - NoName057

Il gruppo **NoName057(16)** si è imposto come uno dei **principali attori dell'hacktivismo filorusso**, orchestrando campagne di attacchi **DDoS** contro obiettivi strategici in Europa. Forte di un vasto seguito online e di un approccio "**gamificato**" al reclutamento, il collettivo ha saputo sfruttare il fattore ideologico per alimentare la partecipazione di migliaia di volontari. L'Operazione Eastwood, avviata a luglio 2025, ha rappresentato una risposta senza precedenti alla loro capacità di coordinamento e alla resilienza della loro infrastruttura di attacco.

Il 15 luglio 2025, la cosiddetta **Operazione Eastwood** ha colpito duramente il gruppo **hacktivista pro-russo NoName057(16)**, responsabile di centinaia di attacchi DDoS contro infrastrutture critiche in Europa. L'intervento ha portato allo smantellamento della loro rete di attacco e alla compromissione della piattaforma di coordinamento usata per mobilitare volontari.

Law Enforcement H1 2025

IL RUOLO DELLE FORZE DELL'ORDINE NELLA LOTTA CONTRO IL RANSOMWARE

Risultati operativi principali:

- Disattivazione di **80 server** dedicati agli attacchi DDoS
- Arresto di 2 membri chiave (in Francia e Spagna)
- Esecuzione di **7 mandati di cattura internazionali**
- Effettuate **24 perquisizioni in sette paesi**, inclusi Italia e Germania
- Notifica di responsabilità penale a oltre 1.000 supporter e 17 amministratori di canali Telegram collegati

Il gruppo, che coinvolgeva circa 4.000 volontari tramite la piattaforma DDoSia, utilizzava un approccio gamificato al reclutamento, premiando gli attacchi riusciti con classifiche e riconoscimenti interni. L'operazione ha quasi azzerato il network DDoS del gruppo per diverse settimane, bloccando le campagne più recenti e rendendo estremamente difficile la riorganizzazione.

In Italia, **NoName057(16)** aveva condotto attacchi già a febbraio 2025 contro aeroporti (Linate, Malpensa), istituti bancari (Intesa San Paolo) e porti strategici (Taranto e Trieste), spesso in risposta a dichiarazioni politiche pro-Ucraina. A livello europeo, gli obiettivi principali hanno incluso istituzioni governative, enti finanziari, infrastrutture energetiche e sistemi di trasporto, con impatti significativi in Germania e Svezia.

5. Operazione Checkmate – BlackSuit

BlackSuit ha rappresentato l'evoluzione moderna di famiglie ransomware come Conti e Royal, si era affermato come uno dei gruppi ransomware più aggressivi e strutturati, imponendosi con modalità aggressive di **double extortion**, targeting multipiattaforma e richieste di riscatto da più milioni. Con un portafoglio di oltre 180 vittime note e richieste di riscatto che in alcuni casi hanno superato i 60 milioni di dollari. Alla fine di luglio 2025, l'**Operazione Checkmate** ha irrompe nei meccanismi operativi del gruppo, colpendo duramente la sua presenza sul **dark web**.

Il 24 luglio 2025, con l'**operazione Checkmate** le autorità hanno compromesso l'infrastruttura web del gruppo, oscurato il leak site e il portale di negoziazione di BlackSuit, sostituendoli con banner che ne annunciavano la confisca da parte delle autorità U.S. Homeland Security Investigations e partner internazionali.
Hanno partecipato all'azione: DoJ, FBI, US Secret Service, Europol, NCA (UK), agenzie di Germania, Francia, Olanda, Ucraina, Lituania, Canada, Irlanda e Bitdefender.
Impatto operativo:

BlackSuit, che tra 2022 e 2025 avrebbe compromesso oltre 450 entità negli USA e raccolto circa $370 milioni in riscatti, ha perso la sua infrastruttura nodale. Tuttavia, nessuna cattura è stata resa pubblica, e gli investigatori avvertono come gruppi con risorse elevate possano riorganizzarsi rapidamente.
Nel frattempo, emergono già i primi segni della sua trasformazione: il gruppo denominato Chaos ransomware, attivo da febbraio 2025 e probabilmente guidato da ex affiliati BlackSuit/Royal, continua la **strategia di attacco** via **double extortion** (Target: Windows, Linux, ESXi, NAS).

6. Operazione DuckHunt – Cl0p

Il gruppo Cl0p, già responsabile della massiccia campagna MOVEit del 2023, ha continuato nel 2025 a monetizzare dati esfiltrati tramite la propria piattaforma di leak. Con l'Operazione DuckHunt, a marzo 2025, le forze dell'ordine hanno mirato a interrompere le campagne di pubblicazione post-esfiltrazione, agendo sia a livello tecnico che legale. La CISA, l'FBI e le autorità indiane, in collaborazione con Cloudflare e CERT-In, hanno condotto un takedown coordinato dei server proxy che supportavano i mirror asiatici del leak site. Parallelamente, azioni legali contro operatori di hosting in Uzbekistan e Kazakistan hanno ridotto la resilienza dell'infrastruttura edge del gruppo.

Nonostante il ritorno online del leak site dopo 10 giorni su una nuova estensione .onion, l'operazione ha impedito la pubblicazione di dati sensibili appartenenti a oltre 12 enti governativi indiani, rappresentando una rara vittoria preventiva nella gestione di incidenti ransomware. Di seguito i risultati operativi:

- Takedown coordinato di server proxy per mirror asiatici del leak site
- Blocco infrastruttura edge con supporto Cloudflare
- Azioni legali in Uzbekistan e Kazakistan
- Protezione di oltre 12 enti governativi indiani da leak imminenti

Cl0p si è distinto come speciale attore ransomware focalizzato sull'estorsione tramite esfiltrazione dati, piuttosto che crittografia. Dopo una serie di attacchi, il gruppo è entrato nel mirino delle forze dell'ordine nella primavera 2025.

L'Operazione DuckHunt ha consentito di smantellare i server proxy usati per i mirror commerciali asiatici del leak site di Cl0p e avviare azioni legali contro hosting provider in Uzbekistan e Kazakistan. Il sito di leak è rimasto offline circa 10 giorni prima di riorganizzarsi su un nuovo dominio .onion. Tuttavia, si stima che almeno 12 enti governativi indiani siano stati protetti da esfiltrazioni imminenti, grazie a un intervento preventivo efficace.

7. Operazione Eclipse – Lazarus / APT38

Il collettivo **nordcoreano Lazarus**, e in particolare la sua componente **APT38** specializzata in **operazioni finanziarie**, rappresenta da anni una delle minacce più sofisticate nel panorama della **cyber-finanza**. Il gruppo ha adottato i **cyber-heist** come strumento strategico per finanziare **programmi militari**, combinando tecniche di intrusione avanzate con una **rete globale di riciclaggio**.

Nel primo semestre del 2025, **Lazarus** ha raggiunto un nuovo livello di attività con due attacchi significativi contro le piattaforme **crypto Bybit** (febbraio, $1,5 miliardi) e **BitoPro** (maggio, circa $11,5 milioni). In risposta, tra febbraio e maggio, è stata lanciata **l'Operazione Eclipse**, coordinata da **FBI**, **OFAC** (Treasury USA), **Europol** e supportata da **Chainalysis**, **Elliptic** e **TRM Labs**.

L'operazione ha segnato il primo impatto tangibile su una pipeline finanziaria nordcoreana, rallentando concretamente il riciclaggio dei fondi.

https://www.bleepingcomputer.com/news/security/fbi-confirms-lazarus-hackers-were-behind-15b-bybit-crypto-heist/

https://www.infosecurity-magazine.com/news/fbi-confirms-north-koreas-lazarus

Risultati operativi:

- Blacklisting di 51 indirizzi Ethereum collegati a Lazarus
- Congelamento di wallet su Binance, KuCoin e OKX
- Sequestro di circa $96 milioni in stablecoin
- Pressione diplomatica su Hong Kong per rafforzare i controlli AML e KYC

INITIAL ACCESS BROKERS

LA PORTA D'INGRESSO DEL CYBERCRIME

A cura di Pietro Melillo, Fulvio Fedi, Alberto Davanzo, Luca Palazzo, Flaviano Cardone, Daniele Fiungo, Irene La Bollita

INITIAL ACCESS BROKERS

LA PORTA D'INGRESSO DEL CYBERCRIME

"La tecnologia avanzata è l'arma più affilata dello Stato moderno. Se i paesi occidentali sono stati in grado di dominare il mondo in epoca moderna è anche perché detenevano il primato tecnologico" [Xi Jinping].

1. Executive Summary

Nello scenario globale dell'Information Technology e della Cybersecurity, un ruolo sempre più centrale, importante e spesso sottovalutato viene oggi ricoperto dagli Initial Access Broker (IAB). Spesso operanti nell'ombra, questi attori rappresentano la prima, cruciale, fase di molteplici attacchi informatici complessi, fungendo da veri e propri "facilitatori" per gruppi criminali più strutturati.

Essi rappresentano la fase iniziale e cruciale di innumerevoli attacchi informatici complessi, fungendo da veri e propri "abilitatori" per i gruppi criminali organizzati.
Comprendere a fondo la natura degli IAB, il loro modus operandi e le loro implicazioni, è oggi fondamentale e indispensabile per qualsiasi strategia di difesa, sia a livello aziendale che nazionale.
Gli IAB, sono in sostanza, l'anello iniziale attraverso cui molte offensive digitali prendono forma, abilitando l'accesso a sistemi, infrastrutture e dati strategici.

Capire a fondo chi sono gli IAB, come operano e quali implicazioni portano con sé non rappresenta solamente un vantaggio competitivo, ma una necessità imprescindibile per qualsiasi strategia di difesa, sia aziendale che nazionale."

INITIAL ACCESS BROKERS

LA PORTA D'INGRESSO DEL CYBERCRIME

2. Introduzione

Il panorama della cybersecurity ha subito una trasformazione radicale nell'ultimo decennio, evolvendo da un insieme di attacchi spesso opportunistici e ben organizzati, ad una industria criminale, efficiente, altamente organizzata e profondamente interconnessa.
Quello che un tempo erano attività per singoli hacker o piccoli threat actor (attori malevoli) è diventata oggi un'economia sotterranea/clandestina complessa, con ruoli ben definiti e una sorprendente divisione del lavoro.

INITIAL ACCESS BROKERS

LA PORTA D'INGRESSO DEL CYBERCRIME

La Nascita della Specializzazione Criminale: Un Mercato nero digitale

Il tratto distintivo del cybercrime moderno è senza dubbio la sua specializzazione. Questa ripartizione dei ruoli, delle competenze e campi di appartenenza, ha reso gli attacchi più resilienti, più difficili da tracciare e incredibilmente più efficaci. Sono emersi oggi gruppi di threat actor e cybercriminali specifici, ognuno con competenze e obiettivi precisi, che interagiscono tra loro in un vero e proprio "mercato" sotterraneo:

- **Ransomware-as-a-Service (RaaS)**: Modelli in cui gli sviluppatori di ransomware affittano la loro infrastruttura e il loro codice (il "servizio") ad "affiliati" che poi conducono gli attacchi veri e propri, dividendo i profitti. Questo ha abbassato drasticamente la barriera d'ingresso per chi vuole dedicarsi agli attacchi informatici, spesso senza avere nemmeno competenze tecniche elevate.
- **Initial Access Broker (IAB)**: Il fulcro della nostra analisi. Come già accennato, sono gli specialisti nell'ottenere e rivendere l'accesso iniziale a reti e sistemi compromessi. Sono i "fornitori di chiavi" che alimentano gran parte degli attacchi successivi.
- **Infostealer Developers**: Creatori e distributori di malware specifici (gli "infostealer") progettati per raccogliere credenziali, dati sensibili e altre informazioni direttamente dai dispositivi delle vittime. Questi dati possono poi essere venduti ad altri attori o utilizzati per campagne mirate.
- **Malware-as-a-Service (MaaS)**: Simile al RaaS, offre strumenti malware complessi su abbonamento o a noleggio, rendendoli accessibili anche a criminali meno esperti.

INITIAL ACCESS BROKERS

LA PORTA D'INGRESSO DEL CYBERCRIME

Obiettivo del Documento: Decifrare il Ruolo degli Initial Access Broker

In questo contesto di specializzazione, il documento/articolo si propone di fare luce su uno degli attori più critici e spesso sottovalutati: gli Initial Access Broker (IAB). Esploreremo in dettaglio:

- **Il loro modus operandi**: Come ottengono gli accessi e quali sono le tecniche più diffuse.
- **Le loro interazioni**: Come si inseriscono nella catena di attacco, in particolare nel rapporto con altri gruppi ransomware.
- **Casi concreti:** Esempi di come la loro attività abbia contribuito a violazioni significative.
- **Le implicazioni di sicurezza:** L'impatto sulla sicurezza aziendale e nazionale.

Le strategie difensive: Misure proattive e reattive che le organizzazioni possono adottare per mitigare il rischio di essere compromesse tramite IAB, con un focus sull' importanza della Cyber Threat Intelligence

3. Chi sono gli IAB e Perché Sono Fondamentali?

L' **Initial Access Broker** è un professionista del cyber-crime che ottiene il primo punto di ingresso in una rete (VPN, RDP, account cloud, web-shell) e lo rivende a ransomware gang, APT o truffatori, senza toccare un bit di dati o cifrare nulla, monetizza solo l'accesso.

Questi attori si posizionano nella prima fase della kill chain , fornendo accessi a:

- **VPN** (Virtual Private Network)
- **RDP** (Remote Desktop Protocol)
- **Account Active Directory** (admin e non)
- **Sessioni cloud persistenti**

I tipi di accesso che gli IAB mettono in vendita possono variare ampiamente, includendo:

- Credenziali valide (compromesse tramite phishing, brute-forcing, o malware infostealer).
- Accesso a desktop remoti (RDP) o VPN.
- Exploit per vulnerabilità note in sistemi esposti.
- Backdoor installate su sistemi target.

Questi "pacchetti di accesso" sono solitamente quotati in base alla dimensione e alla criticità dell'organizzazione vittima, alla qualità e alla persistenza dell'accesso offerto, e alla presenza di privilegi elevati.
Una volta ottenuti, questi accessi vengono messi in vendita sul dark web, spesso in forma semi-anonima.

È importante notare che gli IAB non sono semplici hacker freelance. Molti di loro lavorano come fornitori esclusivi per gruppi ransomware affiliati (es. ALPHV, LockBit, BlackCat), con accordi di revenue sharing e contratti di abbonamento mensili.

In questo scenario, l'IAB assume un ruolo molto simile a quello di un subcontractor specializzato: non esegue direttamente l'attacco finale, ma fornisce un servizio chiave a chi intende colpire. La sua competenza sta nell'individuare e aprire accessi poco protetti, riducendo i tempi e i rischi per chi poi eseguirà la parte più visibile e devastante dell'operazione.

INITIAL ACCESS BROKERS

LA PORTA D'INGRESSO DEL CYBERCRIME

4. Tecniche di Compromissione

Gli **IAB** utilizzano un ventaglio di tecniche ben collaudate per ottenere **accesso iniziale** ai sistemi target. Secondo il **M-Trends 2025 Report** di Mandiant, i metodi di compromissione più utilizzati sono classificabili in quattro categorie principali, spesso combinate tra loro per aumentare l'efficacia e ridurre la probabilità di rilevamento.
Infostealer malware (Accesso tramite credenziali esfiltrare)
Malware come **Raccoon Stealer, Redline**, **Vidar** raccolgono credenziali da browser, client VPN e sessioni web.
Sono distribuiti tramite siti infetti, SEO poisoning, canali Telegram, malvertising e phishing kit.
I pacchetti di log compromessi vengono venduti in bulk su forum o venduti singolarmente dagli IAB.
Esempi di Infostealer e hash SHA-256: campioni di RedLine
RedLine Stealer è ampiamente utilizzato da IAB per acquisire credenziali e informazioni utilizzabili per accessi successivi, **crescendo del 500%** nel 2024 (insieme a **Vidar**)
All'interno dei **repository Github** (eset e altri) è possibile reperire un elenco importante degli **hash** di alcuni fra i più diffusi **infostealer**:

Redline	SHA256:
07/02/2024 2037746883 XXLS.zip	20512fc2441838c1a97f92449f0aa38a57bl549b26507ac132194f392aa0f6a6
05/16/2024 rrocc99355wwqaas.exe	67298e2681779093f4e291fa281db921fb8aa1e0eb472fcaf8e7b5d53d8a2077
07/02/2024 Ziraat Bankasi Swift Mesaji pdf.cab	0691fbf6ff5538977804e8f45b1ddc1fa95a5cc1e90475c761ab329da45595d6
07/02/2024 rock99588577yetdr.exe	35a8fccac293ccfb9339f1e30da1a04f91da48e5e2a98fff0c566a888a6db79e
07/02/2024 rrkk9947hhyft54.exe	f1ad91290261a53086074108d6dfa55299f52e45225ae871618110460l1d045a
07/02/2024 rrrrrr0olkt.exe	1a6ba87b6caaf5622647fd113666a8d3da1c526d6a419f2879c015ff615245d9
07/02/2024 SİPARİŞ FORMU_26.01.2024.zip	3f9a150c3465c7a6a7c0e0e182e11c238189afae9d6bb2eae5d1b576037f5c93

Squidloader	SHA256:
07/18/2025 b5086bc2224f44d7331b98656c1a009b	a244bfcd82d4bc2de30fc1d58750875b638d8632adb11fe491de6289ff30d8e5
07/18/2025 d2a909dffe9f645d5da592a992126e63	bb0f370e11302ca2d7f01d64f0f45fbce4bac6fd5613d8d48df29a83d382d232
07/18/2025 ce0c76a5af284a57859b8904ed6f2a77	663d4a7f6224db2718b015dca7b739a0538ccf0c8176c1f84ed6030ac3e7e2d0
07/18/2025 2ae404dd8aab7bbb1c81b6d8c4aed5bd	08f78a98770666da78416b034559a99a325de6732400ab4e6d357f9748f1d4cb
07/18/2025 5c35a91243023fd9bde2ae1808a77c2f	2cd9936fbdd2b98d1abfe9396341501223d35aa43b88a8ca1337dca36f4553ed
07/18/2025 52913eb70fa4ccb4f1859ef15213db9e	41523349ade62c5d2e9a3274043970ea43ce7c7e5fb2153497979f4b4df1479b

WretchedCatStealer	SHA256:
02/12/2025 e0b0855a6a36b445b819039cb79d09f984eda179ab552d41462cfe2772016a43	e0b0855a6a36b445b819039cb79d09f984eda179ab552d41462cfe2772016a43
02/12/2025 a5e53b0e11289e90df10c2ea326c7079	1c9a340d0711d3222fdc20572ebf0a7aefa832cdf8644ecd4713dc3eda569935
02/12/2025 ed6116430cb2888d73c0011f8526bb0e	72323309a56b0fc5f40e34ac5ea540139733c53a999a53f05e0db807b6aeaf8f
02/12/2025 93ecff0d15bb5edd43393ea415eb4cb7cf46f0dc6fcfc66846526d8335cff744	93ecff0d15bb5edd43393ea415eb4cb7cf46f0dc6fcfc66846526d8335cff744
02/12/2025 d61c36fc4f88157ce8fb16059e460d15b0b6adb46936d6759828156817954f79	d61c36fc4f88157ce8fb16059e460d15b0b6adb46936d6759828156817954f79

INITIAL ACCESS BROKERS

LA PORTA D'INGRESSO DEL CYBERCRIME

Accessi RDP/VPN deboli o esposti (Brute-force, credential stuffing)
Le configurazioni errate, credenziali deboli o mancanza di MFA continuano a essere vettori d'ingresso sfruttati con successo.

Mandiant segnala come nel 2024 siano aumentati gli attacchi mirati a MSP (Managed Service Provider), ovvero fornitori di servizi IT gestiti che operano in outsourcing per più aziende, sfruttando RDP/VPN condivisi per ottenere accesso indiretto alle reti dei loro clienti.

Exploiting vulnerabilità note (N-day) e 0-day
CVE recenti come **PAN-OS GlobalProtect** (**Palo Alto Networks**) **CVE-2024-3400**, **Connect Secure VPN** (**Ivanti**) e **CVE-2023-46805**, Policy Secure (Ivanti) CVE-2024-21887 sono tra i vettori più frequentemente sfruttati dagli IAB nel 2024.
Gli IAB più sofisticati mantengono accessi privilegiati a exploit privati e tool customizzati.

Tecniche avanzate di phishing e bypass MFA
Secondo **M-Trends**, si osserva un incremento delle tecniche di phishing avanzato, in particolare l'abuso di **token OAuth**, che consente di mantenere l'accesso continuo a servizi cloud senza richiedere una nuova autenticazione; la manipolazione delle sessioni browser tramite **proxy interattivi**, capaci di intercettare in tempo reale le credenziali inserite dall'utente; e le tecniche di **MFA fatigue**, che consistono nell'invio ripetuto di richieste di autenticazione nella speranza che l'utente, esausto o distratto, le approvi. Queste tecniche rappresentano oggi una parte significativa dei metodi di compromissione osservati nel panorama delle minacce.

5. Modello Economico e Vendita

All'interno di una delle chat di un noto gruppo di threat actor, si viene accolti con una frase emblematica: **"Il tempo è denaro, ma solo il denaro è denaro"**.

Questa citazione coglie con precisione l'essenza del modello operativo degli **Initial Access Broker** (IAB) e, più in generale, dell'intera economia del cybercrime: ogni accesso, ogni compromissione, ogni movimento è orientato a generare profitto. È questo principio economico a guidare le logiche del mercato sotterraneo in cui gli IAB prosperano, trasformando il crimine informatico in un'attività imprenditoriale strutturata.

Valutazione Economica del Target

Nel mercato illecito della rivendita degli accessi, la capacità economica dell'organizzazione target rappresenta uno dei fattori di maggiore interesse su cui gli IAB si concentrano.

Il fatturato di un'azienda viene spesso interpretato come un ottimo indicatore indiretto della sua posizione competitiva e della sua esposizione sul mercato, rendendola potenzialmente più appetibile per chi ha come scopo quello di massimizzare i profitti derivanti dalla rivendita o dall'utilizzo di accessi ad essi collegato.

Le imprese con maggiore peso economico tendono infatti a offrire un potenziale di monetizzazione più elevato, sia per l'estensione delle infrastrutture digitali, sia per la maggiore probabilità di ottenere ritorni più consistenti da attività successive. Tuttavia, si registra una crescente attenzione anche verso realtà aziendali di taglia inferiore. Questo spostamento di interesse suggerisce una razionalizzazione delle strategie adottate: l'obiettivo non è più solo il valore assoluto, ma un bilanciamento tra facilità di compromissione, valore potenziale e rapidità dell'operazione.

INITIAL ACCESS BROKERS

LA PORTA D'INGRESSO DEL CYBERCRIME

Il risultato è un modello di vendita più fluido, in cui il parametro economico rimane centrale ma non più esclusivo, e in cui anche le aziende con profili di fatturato più contenuti entrano a far parte del panorama commerciale degli accessi illeciti

Forum Underground Frequentati da IAB

Forum	Stato attuale	Tipo di contenuti	Accesso	Lingua	Rilevanza per IAB
Exploit[.]in	Attivo	Annunci di accessi, info su malware, TTPs	Registrazione	Russo	Molto elevata – noto per vendite RDP/VPN
XSS[.]is	Attivo	Discussioni tecniche, compravendita	Solo invito	Russo	Alta – canale di networking per IAB e affiliati
BreachForums	Chiuso (mirror attivi)	Dati leakati, credenziali, accessi	Mirror pubblici	Inglese	Storica – usato per drop iniziali
RaidForums	Chiuso (sequel RF2)	Dumps di credenziali, leak aziendali	Mirror/archivi	Inglese	Storico – importante per dataset accessibili
RAMP	Attivo (limitato)	Marketplace ibrido ransomware + IAB	Privato	Russo	Elevata – frequentato da affiliati ransomware
TOX Channels	Attivo (decentralizzato)	Comunicazione diretta P2P	TOX ID richiesto	Vari	Media – per trattative più riservate

Market Underground per la Vendita di Accessi

Marketplace	Stato	Categoria vendite	Modalità di pagamento	Tipo di accessi offerti	Particolarità
Genesis Market	Smantellato (Apr 2023, FBI)	Identità digitali, browser fingerprints	BTC, XMR	Credenziali, cookies sessioni	Basato su device fingerprint e botnet
Russian Market	Attivo	Credenziali, accessi RDP/VPN	BTC	RDP, VPN, webmail	Ampio, ma qualità variabile
2easy[.]shop	Attivo	Logs stealer, RDP, web access	BTC	Accessi post-infezione	Automatizzato con pannello
Ultimate Anarchy	Attivo	Dati leakati, account premium	BTC/XMR	VPN, cloud, SAAS	Forum + market unificato
Cocaine Market	Attivo (tor)	Accessi aziendali, RDP	XMR, escrow interno	RDP, Citrix, domain admin	Si autodefinisce come "premium access"
DarkLeak	Attivo (forum/market)	RDP, email, citrix, dump	BTC	Accessi corporate	Usato da broker specializzati

Marketplace, Prezzi e Modalità di Vendita

Gli **IAB** operano prevalentemente su **forum clandestini** accessibili tramite la darknet o reti private (es. Tor, I2P) e, più recentemente, anche su piattaforme più agili come Telegram o Discord.
Forum come Exploit.in, XSS.is, RAMP (attivo fino al 2022) e i diversi fork di BreachForums (tornato da poco disponibile con l'intero contenuto prima che andasse offline) rappresentano i principali hub per l'incontro tra domanda e offerta. Le offerte più comuni includono:

- Accessi RDP/VPN a reti aziendali;
- Credenziali privilegiate di dominio Active Directory;
- Accesso a pannelli di controllo web (CMS, CRM, portali ERP);
- Shell persistenti o webshell su server compromessi;
- Exploit zero-day o credenziali ottenute tramite infostealer (RedLine, Racoon, etc.).

Meccanismi di Escrow e Protezione dalle Frodi
L'**escrow** rappresenta un ruolo cardine nella prevenzione della truffe (scam) nei mercati cybercriminali, dove l'identità degli operatori viene spesso offuscata. La diffidenza reciproca viene supplita da meccanismi di mediazione, per lo più messi a disposizione dai moderatori dei forum.

Caratteristiche tipiche dell'escrow:

- Il compratore trasferisce il pagamento al moderatore, che lo trattiene fino alla conferma della validità dell'accesso da parte dell'acquirente.
- Il venditore riceve il pagamento solo a transazione completata.
- Viene spesso trattenuta una commissione variabile (dal 5% al 15%).

Secondo un report di **Flashpoint** (2022), alcuni forum forniscono anche funzioni avanzate di **arbitraggio**, in caso di dispute tra le parti.

INITIAL ACCESS BROKERS

LA PORTA D'INGRESSO DEL CYBERCRIME

Reputazione: Il Vero Asset degli IAB

Altro punto importante la reputazione che costituisce un asset fondamentale per gli IAB e, più in generale, per tutti i venditori attivi in ambienti sommersi.

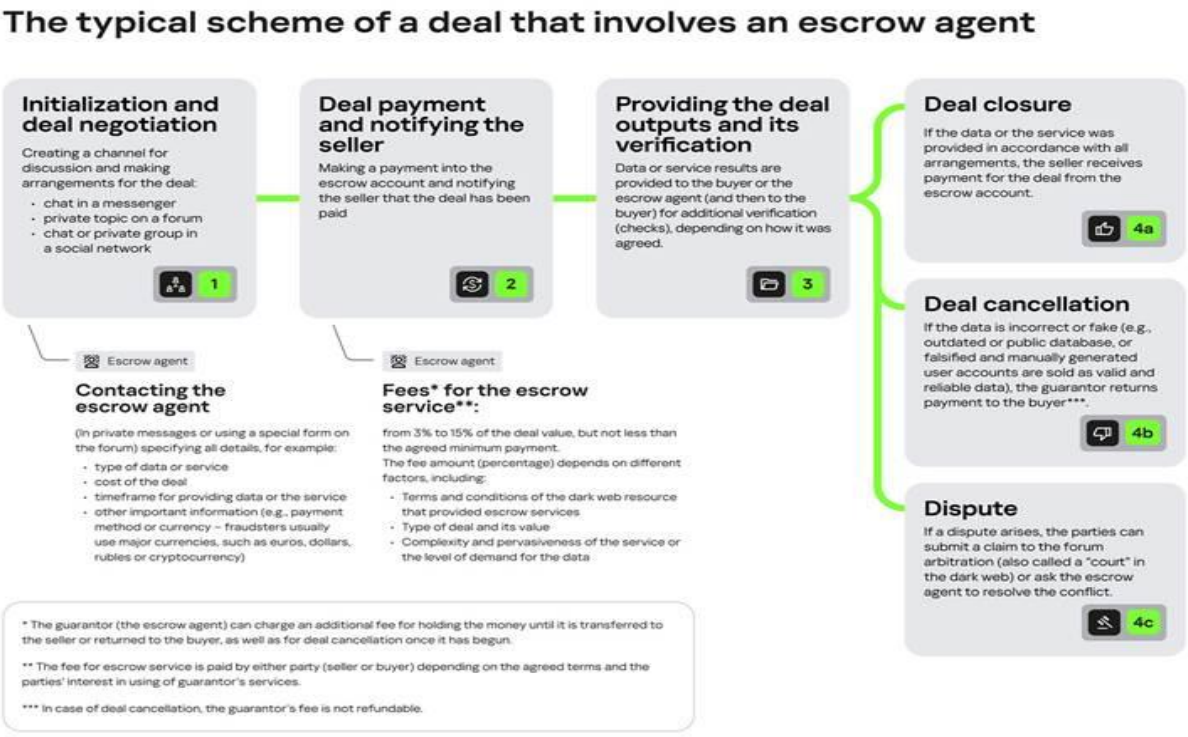
Essa si costruisce attraverso alcuni tipici comportamenti:

- Feedback pubblici da parte degli acquirenti (es. "+1", review positive/negative);
- Badge e status conferiti dai forum (es. "trusted vendor", "verified seller");
- Attività costante nel tempo (anzianità del profilo, numero di post);
- Partecipazione a community parallele (es. Telegram, altri forum).

Un caso emblematico è l'**IAB** noto come "**Fak3r**", attivo tra 2021 e 2023 su **Exploit** e **XSS**, il cui successo è stato largamente determinato dalla sua reputazione costruita su oltre 100 transazioni positive, molte delle quali con accessi a grandi **aziende IT europee** (Mandiant, 2023).

INITIAL ACCESS BROKERS

LA PORTA D'INGRESSO DEL CYBERCRIME



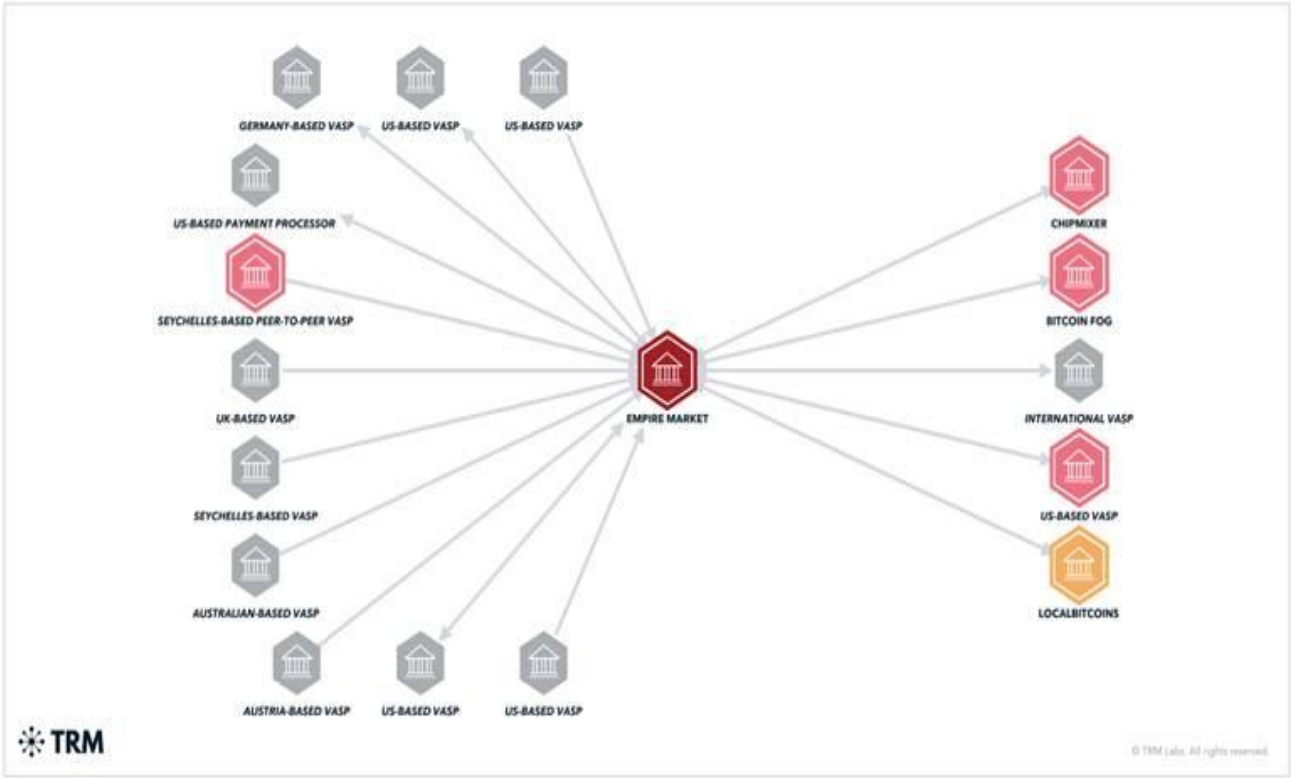
In assenza di identità reali, la fiducia viene costruita attraverso dinamiche di interazione ripetuta e trasparenza operativa. Tra i principali meccanismi osservati:

- Transazioni ricorrenti tra le stesse parti (acquirenti fidelizzati);
- Garanzie esplicite offerte dal venditore (es. sostituzione gratuita di accessi revocati);
- Utilizzo di middleman fidati, soprattutto in forum dove l'escrow è facoltativo;
- Condivisione di proof-of-access (screenshot, test VPN/RDP) per dimostrare l'autenticità del prodotto.

In alcuni casi, l'IAB può addirittura operare con un **pagamento posticipato**, elemento che denota un elevato livello di fiducia bilaterale (Group-IB, 2022).

INITIAL ACCESS BROKERS

LA PORTA D'INGRESSO DEL CYBERCRIME



Le dinamiche osservate confermano che l'ecosistema degli Initial Access Broker non è anarchico, ma regolato da norme informali e strutture sociali complesse. L'interazione tra escrow, reputazione e fiducia costituisce un sistema di garanzie efficiente, che sopperisce all'assenza di accordi "legali".

Comprendere tali meccanismi è cruciale per le attività di **cyber threat intelligence**, in quanto consente di profilare i venditori più pericolosi, prevedere dinamiche di collaborazione tra attori ostili e anticipare possibili compromissioni aziendali.

6. Collaborazione tra IAB e Ransomware Group

Nel panorama della criminalità informatica moderna, gli **Initial Access Broker** (IAB) svolgono un ruolo fondamentale.

Essi rappresentano l'anello di congiunzione tra la compromissione iniziale delle infrastrutture IT e le successive fasi di attacco, tra cui l'esecuzione di ransomware, la vendita di dati e altre forme di estorsione digitale.

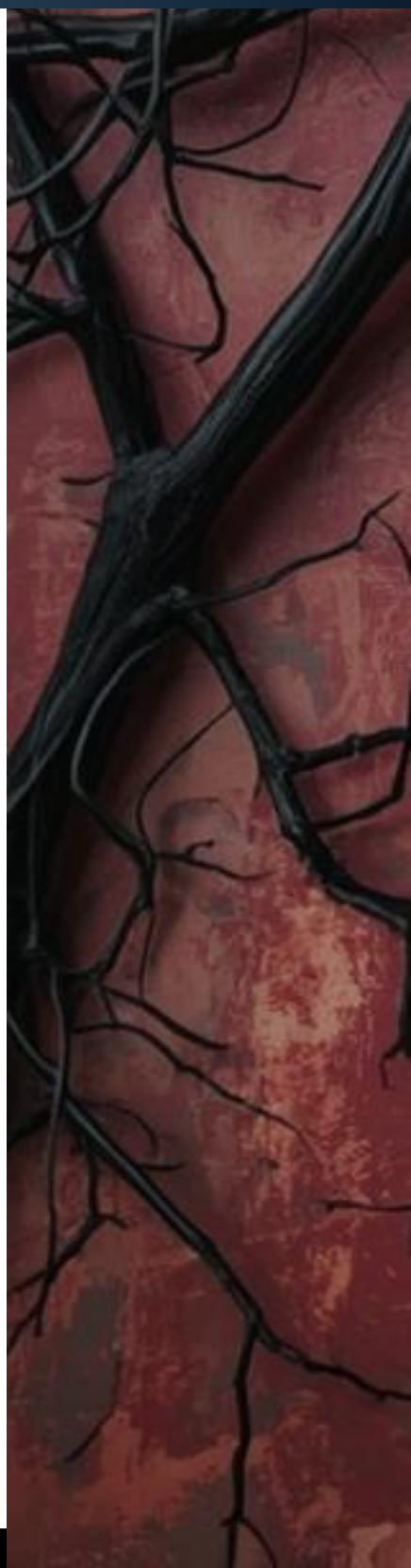
Meccanismi di Collaborazione IAB–Ransomware

I broker di accesso iniziale offrono punti di ingresso in infrastrutture compromesse ai gruppi ransomware-as-a-service (RaaS). Questo modello di business riduce drasticamente i tempi e i costi per l'esecuzione di attacchi su larga scala. Le modalità di collaborazione includono:

-Vendita pubblica su forum underground
-Offerte private e canali Telegram
-Partnership dirette e private
-Integrazione verticale tra infostealer e ransomware

Fonti:

- https://outpost24.com/blog/use-of-initial-access-brokers-by-ransomware-groups
- https://www.loginsoft.com/post/initial-access-brokers-the-hidden-architects-of-modern-cyberattacks
- https://www.proofpoint.com/us/blog/threat-insight/first-step-initial-access-leads-ransomware



INITIAL ACCESS BROKERS

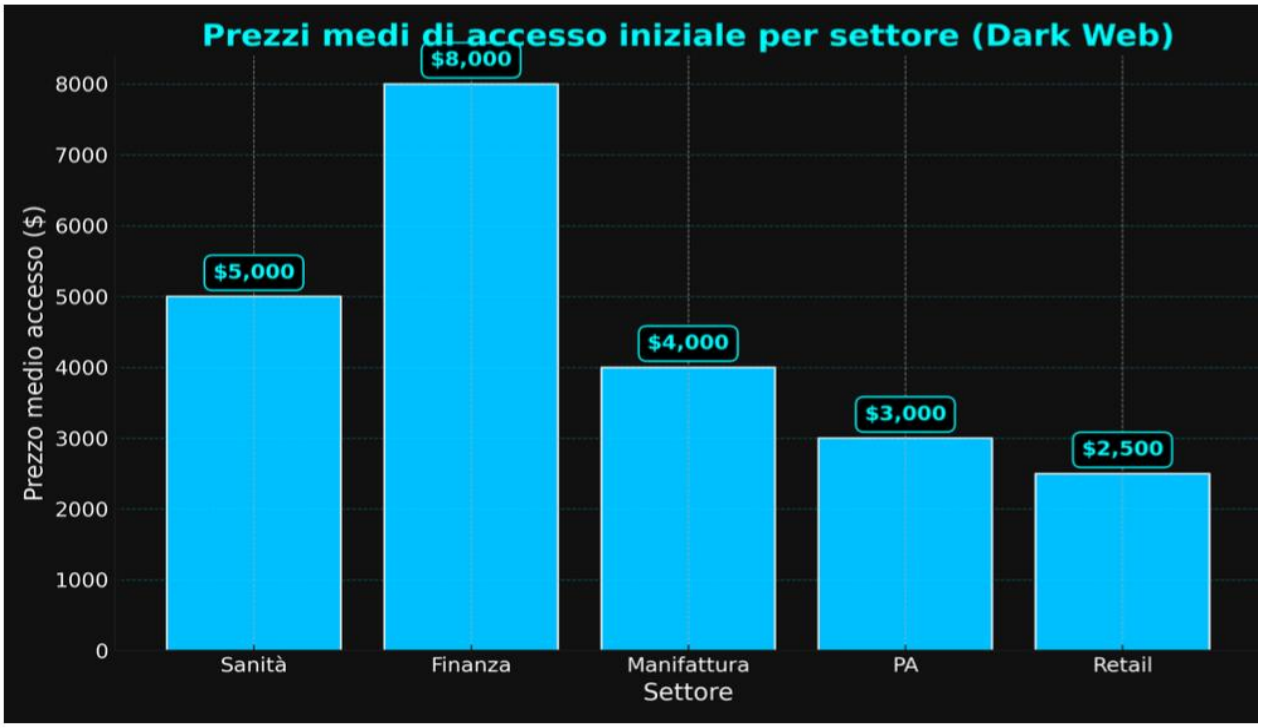
LA PORTA D'INGRESSO DEL CYBERCRIME

Timeline Tipica di Attacco

Un aspetto cruciale è la rapidità dell'attacco: grazie al supporto degli IAB, i gruppi ransomware possono compromettere un'organizzazione in meno di 72 ore.

Prezzi medi di accesso per settore

Il valore di un accesso iniziale dipende dalla dimensione e dal settore della vittima. Settori come sanità e finanza sono considerati premium.



INITIAL ACCESS BROKERS

LA PORTA D'INGRESSO DEL CYBERCRIME

Modalità Operative

Modalità di collaborazione	Caratteristiche
Vendita pubblica su forum underground	Transazioni trasparenti, rischio di tracciamento alto
Offerte private via Telegram/ICQ	Maggiore anonimato, selezione clienti affidabili
Partnership dirette con gruppi ransomware	Accessi forniti esclusivamente a gruppi affiliati
Brokeraggio tramite escrow	Pagamento sicuro con moderatore neutrale
Integrazione verticale (gruppo possiede infostealer e IAB)	Controllo completo su tutta la catena di attacco

7. Tecniche MITRE ATT&CK

T1078 – Valid Accounts

Gli attaccanti sfruttano credenziali legittime (rubate tramite infostealer o brute-force) per autenticarsi nei sistemi. Difficile da rilevare perché l'accesso avviene con account autorizzati.

T1133 – External Remote Services

Uso di servizi remoti esposti come RDP, VPN, VNC o Citrix per accedere all'ambiente della vittima. Espone la rete interna agli attori esterni.

T1566 – Phishing

Invio di email ingannevoli per convincere l'utente a cliccare su un link malevolo o aprire un allegato infetto. Tecnica di compromissione iniziale ampiamente usata.

T1059 – Command and Scripting Interpreter

Utilizzo di strumenti di scripting (es. PowerShell, Bash, CMD) per eseguire comandi malevoli o automatizzare movimenti laterali. Estremamente versatile e spesso impiegato post-accesso.

T1203 – Exploitation for Client Execution

Sfruttamento di vulnerabilità software per eseguire codice malevolo su un endpoint client. Accesso immediato senza necessità di credenziali.

INITIAL ACCESS BROKERS

LA PORTA D'INGRESSO DEL CYBERCRIME

Mappatura framework MITRE > TTP VS Detection

TTP	Nome Tecnica	Uso da parte di IAB	Detection
T1078	Valid Accounts	Gli IAB utilizzano credenziali valide (raccolte da infostealer come Raccoon) per accedere a reti aziendali tramite RDP, VPN o SSH.	Monitorare accessi da utenti legittimi provenienti da IP anomali o in orari inconsueti; implementare MFA e alert su login geografici sospetti.
T1059.003	Command and Scripting Interpreter: Windows Command Shell	Spesso utilizzano script batch per automatizzare movimenti laterali o persistenti dopo l'accesso iniziale.	Analizzare esecuzioni di cmd.exe non firmate da utenti regolari; correlare attivitÃ con eventi di autenticazione recenti.
T1566.001	Phishing: Spearphishing Attachment	Campagne iniziali di Raccoon Stealer spesso veicolano loader tramite allegati e-mail (es. .doc, .exe mascherati).	Controllare allegati ricevuti via email con esecuzione immediata di processi sospetti o dropper in cartelle temporanee.
T1105	Ingress Tool Transfer	Dropper scaricano payload (infostealer o backdoor) da server controllati dagli attaccanti.	Monitorare download eseguibili da domini non autorizzati; ispezionare user-agent anomali o connessioni HTTP plain-text.
T1203	Exploitation for Client Execution	IAB sfruttano vulnerabilitÃ in software client (es. browser o PDF reader) per distribuire infostealer senza interazione.	Rilevare crash applicativi seguiti da esecuzioni sospette; usare sandbox per e-mail con allegati attivi.
T1055.001	Process Injection: Dynamic-link Library Injection	Infostealer come Raccoon usano DLL injection per eludere i controlli di sicurezza e rimanere in memoria.	Utilizzare Sysmon per tracciare injection tra processi; attivare regole EDR sulle API di injection (Es. VirtualAllocEx, WriteProcessMemory).

INITIAL ACCESS BROKERS

LA PORTA D'INGRESSO DEL CYBERCRIME

Casi Studio Estesi

EXOTIC LILY & FIN12

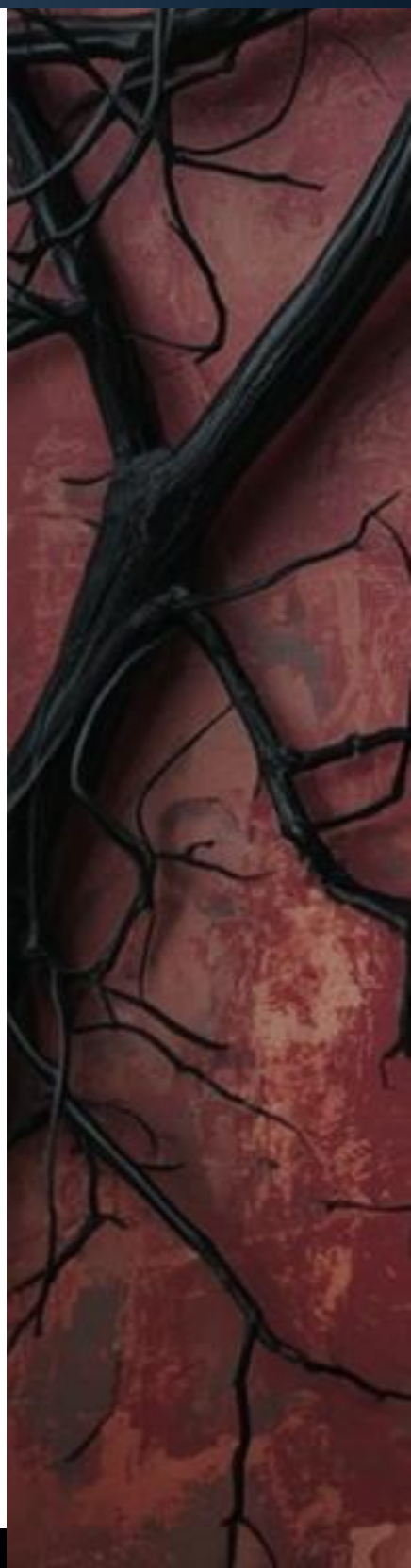
EXOTIC LILY è un noto **Initial Access Broker** documentato da Google TAG. Ha operato sfruttando vulnerabilità Microsoft (es. CVE-2021-40444) e fornendo accessi a gruppi come **FIN12**.

Metodo preferito: email phishing con allegati weaponizzati.
Fonte: https://blog.google/threat-analysis-group/exposing-initial-access-broker-ties-conti

FXMSP

FXMSP è stato uno dei **broker più attivi** fino al **2020**. Ha **venduto accessi RDP e VPN** ad alto privilegio su forum come XSS e Exploit.in, permettendo a gruppi come REvil e Hive di lanciare attacchi altamente distruttivi.

Fonte: https://www.kelacyber.com/blog/the-secret-life-of-an-initial-access-broker



8. Raccomandazioni Difensive

Threat hunting mirato su log RDP/VPN

È fondamentale analizzare regolarmente i log di accesso RDP e VPN per identificare pattern sospetti come login da geolocalizzazioni insolite, orari anomali o tentativi ripetuti di autenticazione fallita. L'utilizzo di strumenti SIEM e analisi comportamentali può migliorare la capacità di intercettare compromissioni iniziali avvenute tramite credenziali rubate o brute-force.

MFA hardware, ZTNA e segmentazione

Implementare l'autenticazione a più fattori basata su dispositivi hardware (es. YubiKey) riduce il rischio di compromissione delle credenziali. Il modello Zero Trust Network Access (ZTNA) nega l'accesso per default e verifica continuamente ogni richiesta. La segmentazione delle reti, inoltre, limita la possibilità di movimento laterale anche in caso di accesso iniziale ottenuto da attori malevoli.

Tecnologie XDR/EDR per anomaly detection

Le soluzioni di Extended Detection and Response (XDR) e Endpoint Detection and Response (EDR) permettono di identificare comportamenti anomali su host e reti aziendali. Sono essenziali per rilevare attacchi che utilizzano strumenti legittimi in modo malevolo, come l'abuso di PowerShell, o accessi autenticati ma inusuali. L'integrazione con UEBA migliora ulteriormente il rilevamento degli attacchi iniziali.

Monitoraggio di forum e canali Telegram

Il monitoraggio attivo delle fonti OSINT, forum underground e canali Telegram utilizzati dai broker, consente alle aziende e ai team CTI di anticipare le minacce. L'analisi delle vendite di accessi in tempo reale può permettere l'identificazione preventiva di compromissioni e mitigare rischi prima che l'attacco venga portato a termine. Strumenti di threat intelligence e crawling automatici sono consigliati.

8. Raccomandazioni Difensive

TTPs e IoC: Indicatori di compromissione e comportamenti avversari

Gli "indicatori di compromissione" (**IoC**) rappresentano evidenze tecniche che segnalano una possibile intrusione o infezione in corso. Possono includere hash di file malevoli, indirizzi IP di command and control, URL sospetti, domini utilizzati per phishing o nomi di processi anomali. Gli IoC hanno una natura puntuale e spesso temporanea, ma sono essenziali per rilevare attività avversarie in fase operativa.

Complementari agli IoC, le Tattiche, Tecniche e Procedure (**TTPs**) descrivono il "come" agiscono gli attaccanti, offrendo una visione comportamentale e strategica che resta più stabile nel tempo. Ad esempio, la tecnica di esfiltrazione tramite servizi cloud legittimi o l'uso di infostealer offuscati in archivi ZIP sono pattern osservabili anche in varianti diverse dello stesso malware.

Facendo nuovamente riferimento ad esempio di **RedLine Stealer**, tra le **TTPs** più ricorrenti rilevate nel 2024–2025 si osservano:

- **Tecniche di delivery**: diffusione tramite siti clonati con CAPTCHA fasulli (es. campagna ClickFix), file ZIP autoestraenti o loader offuscati via Lua bytecode;
- **Persistenza**: installazione come task di sistema o modifica di chiavi Run nel registro di Windows, nonché altre molteplici vie per ottenere un accesso remoto persistente su anche diversi OS
- **C2 communication**: comunicazione con server remoti su HTTP/S, spesso con IP dinamici o domini offuscati;
- **Data exfiltration**: furto di credenziali, wallet, cookie di sessione e file sensibili, poi inviati ai server C2.

Alcuni **IoC** di seguito sotto elencati includono **hash SHA-256** di sample **RedLine** attivi nel 2024/2025, **URL** usati per il **download del payload**, e **IP** noti associati ai server di comando. Anche se in continua evoluzione, questi indicatori forniscono un punto di partenza concreto per il rilevamento proattivo e l'arricchimento dei controlli di rete ed endpoint.

INITIAL ACCESS BROKERS

LA PORTA D'INGRESSO DEL CYBERCRIME

Dettagli quali SHA-256, descrizione e fonti

SHA-256 Hash	Descrizione	Fonte	URL
5e37b3289054d5e774c02a6ec4915a60156d715f3a02aaceb7256cc3ebdc6610	Archivio ZIP contenente un loader RedLine in Lua bytecode (aprile 2024)	McAfee Labs	LINK
9c6f132ef4142409bd7a1448d3dc52f774e9e33919031dac82f2afb27083945f	Campione attivo in diffusione su botnet (luglio 2024)	ThreatFox / Abuse.ch	LINK

IP/PORTA	Descrizione	Fonte	URL
http://185.222.57.67:55615/	C2 attivo con alta affidabilità associato a RedLine (luglio 2024)	ThreatFox	LINK

CAMPAGNA	Descrizione	Fonte	URL
ClickFix Campaign	Campagna basata su CAPTCHA fake che induce il download di RedLine (luglio 2025)	Okta – Threat Insight	LINK

9. Approfondimenti Strategici e Tattici

Perché gli IAB rappresentano un "game changer"
L'introduzione degli Initial Access Brokers ha modificato profondamente la struttura del cybercrime. Prima della loro diffusione, i gruppi ransomware erano costretti a svolgere autonomamente tutte le fasi dell'attacco: dalla compromissione iniziale alla persistenza, fino alla cifratura e all'estorsione. Con gli IAB, l'intera filiera è diventata più specializzata e scalabile, simile a una supply chain industriale. Questa specializzazione ha aumentato l'efficienza degli attacchi, permettendo a nuovi attori di entrare nel mercato grazie a barriere d'ingresso più basse. Il risultato è un incremento esponenziale degli incidenti e una maggiore difficoltà per le aziende nel rilevare e bloccare la compromissione nei primi stadi.

Dinamiche economiche e modelli di pricing nel mercato IAB
Il mercato underground degli accessi iniziali è altamente dinamico e regolato da logiche economiche sofisticate. I prezzi variano in base a fattori come:
- Tipologia di accesso (RDP, VPN, dominio admin, ecc.)
- Dimensione dell'azienda bersaglio (fatturato, numero dipendenti)
- Settore (sanità, finanza, pubblica amministrazione sono più redditizi)
- Presenza di software di sicurezza (EDR, firewall avanzati)

Gli accessi più completi possono superare i $20.000, mentre quelli minori si aggirano sui $500–$3.000. Alcuni broker offrono abbonamenti o bundle di accessi, specialmente su forum come Exploit.in, XSS e BreachForums.

Evoluzione recente: IAB-as-a-Service e automazione
Negli ultimi due anni si è osservata la crescita del modello IAB-as-a-Service (IABaaS), dove gruppi specializzati offrono pannelli web o API per accedere in tempo reale ad asset compromessi. Questi servizi automatizzano la raccolta e la vendita di credenziali, sfruttando infostealer come RedLine, Raccoon e Vidar. L'uso di botnet che aggiornano in tempo reale le liste di accessi disponibili rende il mercato estremamente veloce e competitivo. In alcuni casi, le offerte includono informazioni su endpoint vulnerabili, credenziali salvate nei browser, cookie di sessione validi e accessi MFA bypassati tramite session hijacking.

Caso Italia: Accessi Iniziali e Targeting Locale

Negli ultimi anni, l'Italia ha registrato un numero crescente di compromissioni iniziali condotte da broker di accesso (Initial Access Broker – IAB), che fungono da anello di congiunzione tra le fasi di intrusione e quelle di monetizzazione da parte di operatori ransomware o attori statali. Il contesto nazionale si distingue per una serie di vulnerabilità sistemiche, tecnologiche e culturali, che rendono il paese un bersaglio privilegiato per attacchi mirati.

Target preferenziali: PA, sanità e manifatturiero
Nel contesto italiano, gli attori delle minacce mostrano una spiccata preferenza per tre settori specifici: le Pubbliche Amministrazioni (PA), il comparto sanitario e le aziende manifatturiere. Questa predilezione è dovuta a diversi fattori: infrastrutture informatiche obsolete, ampie superfici di attacco esposte su internet, carenze nei processi di aggiornamento e una bassa consapevolezza del rischio cibernetico. Secondo il Rapporto Clusit 2024, oltre il 60% degli incidenti cyber noti in Italia ha riguardato questi tre settori. Le PA utilizzano sistemi legacy non supportati, spesso accessibili tramite RDP o VPN senza MFA. Il settore sanitario è esposto per l'eterogeneità dei sistemi (inclusi dispositivi medici IoT), mentre le PMI manifatturiere spesso non dispongono di un SOC o di processi strutturati di gestione della sicurezza e non investono nella formazione cyber dei propri dipendenti.

Evidenze OSINT: accessi in vendita e compromissioni pubbliche
Numerose evidenze OSINT dimostrano come accessi a sistemi italiani vengano regolarmente venduti su forum underground come XSS.is e tramite canali Telegram. Un esempio noto è un annuncio pubblicato nel 2023 su XSS, in cui veniva venduto un accesso VPN a un'ASL italiana al prezzo di $1000, con privilegi amministrativi. Tali dati sono stati archiviati e resi disponibili tramite il progetto open source deepdarkCTI. Inoltre, alcuni accessi venduti facevano riferimento a software verticali per la gestione documentale e contabile usati da comuni ed enti locali. In parallelo, il CSIRT Italia ha pubblicato nel 2024 almeno cinque bollettini su compromissioni della sanità pubblica, avvenute tramite accesso iniziale remoto.

INITIAL ACCESS BROKERS

LA PORTA D'INGRESSO DEL CYBERCRIME

Il ruolo degli infostealer nel contesto BYOD e PMI

In Italia, l'adozione di politiche BYOD (bring your own device) è spesso priva di regole di sicurezza minime. Dispositivi personali accedono a sistemi aziendali tramite connessioni poco sicure, con credenziali salvate nei browser. Infostealer come Redline, Raccoon e Aurora vengono diffusi tramite phishing, download da siti compromessi o allegati in email. Una volta infettato, il dispositivo esfiltra credenziali, cookie di sessione e informazioni di sistema che vengono poi vendute in blocco. Yarix e Swascan hanno documentato casi in cui il primo punto di infezione è stato un terminale personale non gestito usato per accedere a software ERP aziendali.

Canali Telegram e IAB: una nuova filiera criminale

La convergenza tra infostealer, IAB e ransomware-as-a-service (RaaS) passa oggi per canali Telegram semi-pubblici.

In lingua italiana, esistono gruppi e bot che offrono accessi a sistemi remoti, elenchi di credenziali esfiltrate, servizi di anonimizzazione e persino supporto. Molti attori agiscono in modalità anonima o pseudonima, ma utilizzano strumenti professionali. I contenuti sono archiviati e analizzati nel progetto github deepdarkCTI, che monitora anche le relazioni tra IAB e operatori ransomware (es. Nokoyawa, Black Basta) attivi in Italia.

Un' altro importante progetto che mostra la correlazione e l'evoluzione degli stessi è Ransomfeed disponbile al seguente link: https://ransomfeed.it/

Attribuzione difficile e silenzio mediatico

Un grave ostacolo alla resilienza cibernetica è rappresentato dalla mancanza di trasparenza. Molti incidenti in Italia non vengono resi pubblici, nemmeno in forma anonima o statistica. Questo impedisce la condivisione di TTP e IoC. Secondo CERT-AGID, solo una frazione degli incidenti subiti viene effettivamente riportata o segnalata. Le motivazioni sono diverse: paura di danni reputazionali, assenza di obblighi normativi chiari, mancanza di comunicazione tra IT e direzione. Di conseguenza, molti accessi iniziali restano invisibili fino all'esplosione dell'attacco (ransomware con esfiltrazione), riducendo il tempo utile per una risposta efficace.

Impatti economici e reputazionali in Italia

Le PMI italiane tendono a non esporsi pubblicamente quando subiscono attacchi informatici, per timore di ripercussioni legate alla reputazione e alla perdita di fiducia da parte di clienti e partner. Tuttavia, il danno diretto derivante da tali attacchi è spesso sottovalutato.
Le aziende si trovano a dover affrontare oltre ai costi per il ripristino tecnico anche perdite reputazionali e sanzioni legate al GDPR e interruzioni dell'attività produttiva.
Le spese più rilevanti riguardano la mitigazione delle vulnerabilità di sicurezza, colmare le lacune di sicurezza richiede non solo un investimento economico, ma anche uno sforzo significativo da parte del team IT di Sicurezza in termini di tempo, impegno e risorse.
Inoltre molte delle sfide relative alla sicurezza derivano da negligenza, errori o dalla scarsa consapevolezza dei dipendenti. Per questo motivo, un investimento strategico per le aziende consiste nella formazione del personale, al fine di ridurre il rischio umano e migliorare la resilienza complessiva.

Un trend in crescita riguarda la stipula, da parte delle aziende, di assicurazioni IT contro i rischi informatici (Il 62% secondo il Rapporto Clusit 2025), poiché i danni causati da un attacco possono avere conseguenze disastrose, fino a compromettere la sopravvivenza stessa dell'attività. Questo vale in particolare per le piccole e medie imprese, spesso il target privilegiato, insieme alla Pubblica Amministrazione, degli attaccanti in Italia.

Fonti consultate

- CSIRT Italia: https://www.csirt.gov.it
- CERT-AGID: https://cert-agid.gov.it
- deepdarkCTI(GitHub): https://github.com/fastfire/deepdarkCTI
- Ransomfeeds: https://ransomfeed.it
- Rapporto Clusit 2024: https://clusit.it/rapporto-clusit
- Swascan Threat Intelligence: https://www.swascan.com
- Yarix Cyber Threat Report 2024: https://yarix.com

INITIAL ACCESS BROKERS

LA PORTA D'INGRESSO DEL CYBERCRIME

Trend Futuri

Il panorama della cybercriminalità si sta trasformando rapidamente, segnando un'evoluzione che è tanto tecnica quanto strategica. I report più autorevoli del settore, come il Mandiant M-Trends 2024 e le analisi del team Google Threat Analysis Group (TAG), confermano sia l'accelerazione di alcuni trend chiave che le principali sfide per la cybersecurity nel futuro prossimo.

Crescita dell'automazione e Infostealer-as-a-Service (IaaS)
Gli **Initial Access Broker** (IAB) operano ormai secondo un modello industriale. Forniscono accessi iniziali chiavi in mano, sfruttando **malware infostealer** venduti come servizio (**IaaS**), spesso combinati con piattaforme che ne gestiscono infrastruttura, C2, e data broker. **Malware come Raccoon Stealer 2.0 o Vidar sono esempi emblematici.**
Secondo Mandiant (2024), questi strumenti sono responsabili di oltre il 30% delle compromissioni iniziali analizzate nel periodo 2023–2024. Il trend è verso la completa automazione delle fasi iniziali di raccolta credenziali, inclusi cookie di sessione, token e fingerprinting dei dispositivi.
Fonte: Mandiant M-Trends 2024; Red Hot Cyber, Lezione 3

Targeting delle PMI con bassa cyber hygiene
Le **Piccole** e **Medie Imprese** rappresentano oggi i **bersagli ideali**. La carenza di risorse, aggiornamenti tardivi e mancanza di formazione rendono queste realtà vulnerabili. Google TAG ha registrato **un incremento del 48% degli attacchi mirati a PMI** tra 2023 e 2024.

INITIAL ACCESS BROKERS

LA PORTA D'INGRESSO DEL CYBERCRIME

In molti casi le PMI fungono da punto di ingresso per supply chain più complesse, compromettendo software house o fornitori strategici, come dimostrato dall'attacco a CDK Global nel giugno 2024.

Fonte: Google TAG Threat Horizons Report 2024; Mandiant M-Trends 2024

Aumento del bypass MFA: MFA Fatigue, phishing proxy e session hijack

Anche l'autenticazione a più fattori non è più garanzia di sicurezza. Gli attaccanti adottano tecniche di MFA Fatigue (prompt bombing), proxy phishing (AiTM) e furto di cookie/sessione tramite infostealer.

Google TAG ha documentato campagne estese condotte tramite phishing-as-a-service in combinazione con reverse proxy come Evilginx. La compromissione delle sessioni consente accesso persistente, eludendo MFA anche in ambienti corporate protetti.

Fonte: Google TAG su AiTM; Mandiant Incident Response Insights

Gli IAB come risorsa per attori statali

In un contesto geopolitico instabile, gruppi come quelli affiliati a Iran (APT42) o Corea del Nord (Lazarus Group) ricorrono sempre più a broker di accesso per abbattere i tempi e i costi di intrusione.

Google TAG ha evidenziato come attacchi mirati sponsorizzati da stati si basino su asset già compromessi da attori criminali, poi acquistati o scambiati su forum del dark web. Questa convergenza tra minaccia statale e criminale è un tema chiave anche in MITRE ATT&CK e D3FEND.

Fonte: Google TAG 2024; MITRE D3FEND

Il ruolo dell'AI nella creazione di campagne avanzate

L'Intelligenza Artificiale Generativa sta trasformando la cyber offensive. Gli **IAB** possono sfruttarla per:

- Generare **email di phishing** altamente realistiche (deep phishing);
- Automatizzare scrittura di **exploit proof-of-concept** (PoC);
- Accelerare la **ricognizione su target** (OSINT automatizzato);
- Ottimizzare codice malware tramite AI-enhanced polymorphism.

Questi sviluppi rendono le campagne più scalabili, sofisticate e difficili da rilevare. Google e Microsoft hanno avviato task force per monitorare l'uso di LLM in contesti ostili.

In ambito difensivo, l'adozione dell'intelligenza artificiale sta potenziando le capacità di detection anticipata, migliorando i meccanismi di prevenzione e rendendo la gestione e risoluzione degli incidenti di sicurezza più rapida.

Fonte: Google DeepMind, Microsoft Security Copilot

Nuove superfici di attacco: supply chain, cloud, IoT e OT

Gli attaccanti puntano sempre più su ambienti cloud malconfigurati, sistemi IoT non gestiti e infrastrutture OT isolate. L'obiettivo è accedere a target che non sono adeguatamente monitorati dai SOC tradizionali.

L'attacco a CDK Global ha evidenziato la vulnerabilità delle supply chain digitali: un singolo fornitore può causare disservizi miliardari.

Fonte: Mandiant su CDK Global; MITRE D3FEND

Difese in evoluzione: MITRE D3FEND

Il framework **MITRE D3FEND** rappresenta la controparte difensiva di **ATT&CK**. Per contrastare i trend sopra descritti, **D3FEND** propone:

- **Credential Hardening** (es. token binding);
- **Session Isolation**;
- **Deception Infrastructure** (es. honeypot distribuiti);
- **MFA** Enforcement con detection anti-fatigue);
- **Behavioral Threat Hunting**.

L'adozione di D3FEND è in crescita tra SOC avanzati e framework NIST SP 800-207 (Zero Trust).

Fonte: MITRE D3FEND Knowledge Graph; NIST Zero Trust

Conclusioni

Il confine tra **criminalità informatica**, **interessi economici** e **tensioni geopolitiche** si sta rapidamente dissolvendo, dando vita a un ecosistema in cui le distinzioni tra attori criminali, statali e ibridi diventano sempre più sfumate. In questo scenario, l'accesso iniziale a infrastrutture strategiche, pubbliche e private, è ormai un asset commerciale, una merce nel dark web e nei canali underground, oggetto di una vera e propria economia parallela.

Attori statali come Iran, Corea del Nord o altri gruppi legati alla sfera russa sfruttano infrastrutture criminali esistenti, broker di accesso, **infostealer-as-a-service**, piattaforme di comando e controllo, per aggirare le barriere tecniche e legali che ostacolerebbero operazioni coperte.

Allo stesso tempo, strumenti di attacco sofisticati diventano disponibili in modalità as-a-service, abbassando drasticamente la soglia d'ingresso anche per attori con competenze limitate. L'accelerazione introdotta dall'**intelligenza artificiale generativa** riduce ulteriormente il divario tra esperti e principianti, permettendo la creazione automatica di malware, phishing iperrealistici e automazione delle fasi di intrusione.

Limitarsi a un approccio difensivo tradizionale, fatto di firewall e antivirus, equivale a ignorare il campo di battaglia. È necessario un cambio di paradigma: **un approccio proattivo** e **intelligence-driven**, fondato su **framework** strutturati come **MITRE ATT&CK** (per la comprensione delle TTP avversarie) e D3FEND (per la mappatura delle contromisure efficaci). Questo tipo di difesa, nota come Threat-Informed Defense, permette di allineare le capacità difensive agli scenari realistici, migliorando la detection, la risposta e la resilienza complessiva.

La cultura della sicurezza, dunque, deve diventare patrimonio diffuso, sostenuta da iniziative pubbliche, formazione continua e incentivi all'adozione di buone pratiche. Non basta proteggere i punti centrali della rete: bisogna rafforzare l'intera catena.

La **sicurezza informatica** non deve essere vista solo come una questione tecnica ma bensì come un pilastro strategico. E come ogni pilastro, se non viene rafforzato oggi, domani rischia di crollare sotto il peso del mondo che cambia.

CVE

ANALISI DELLE CVE DEL PRIMO SEMESTRE 2025

A cura di Luca Stivali

CVE

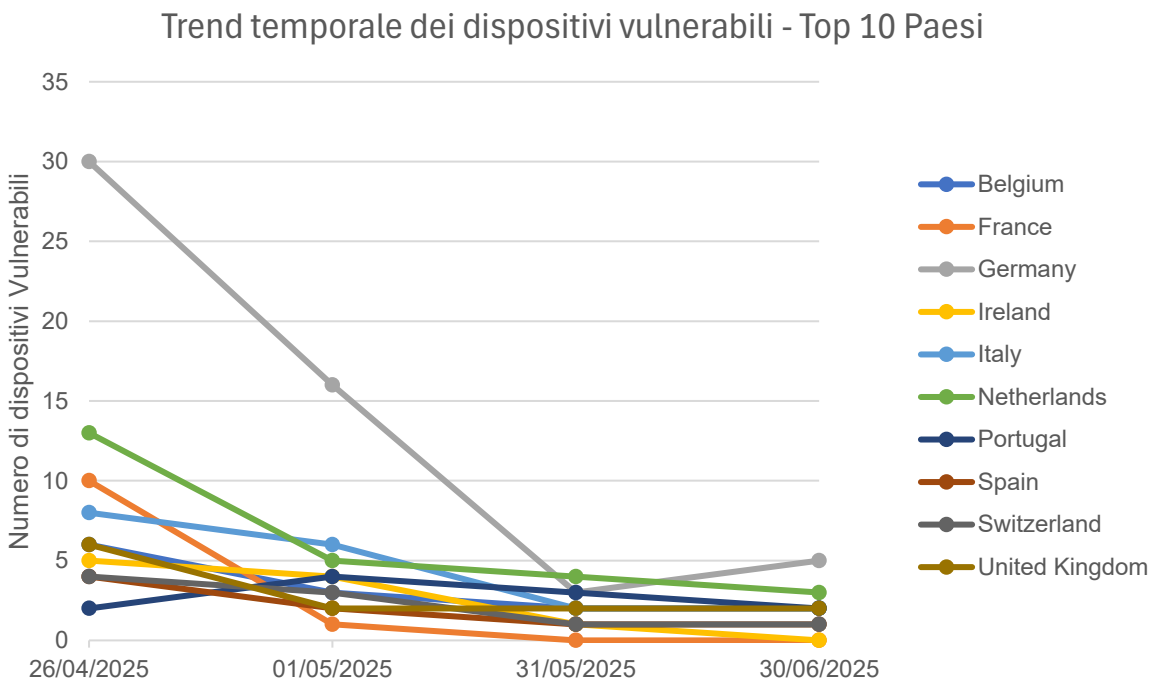
ANALISI DELLE CVE DEL PRIMO SEMESTRE 2025

Introduzione

Il presente report semestrale ha l'obiettivo di monitorare l'esposizione dei dispositivi alle principali vulnerabilità (CVE – Common Vulnerabilities and Exposures) rilevate nel corso del semestre in esame. L'analisi si concentra sul periodo compreso tra la data di pubblicazione di ciascuna CVE e la fine del semestre, con l'intento di valutare il livello di risposta delle organizzazioni in termini di applicazione delle patch di sicurezza. Attraverso il monitoraggio del trend di esposizione, idealmente decrescente, è possibile ottenere una visione chiara
dell'efficacia delle strategie di gestione delle vulnerabilità adottate, evidenziare eventuali ritardi nell'attuazione delle contromisure correttive e identificare aree critiche su cui intervenire per migliorare la postura di sicurezza complessiva.
Questo approccio permette inoltre di affinare i processi di patch management, promuovendo una cultura della sicurezza orientata alla tempestività e alla proattività.

SAP NetWeaver Visual Composer CVE-2025-31324

Il 24 aprile 2025, SAP ha rilasciato un bollettino di sicurezza per la vulnerabilità **CVE-2025-31324**, considerata critica con uno score di 10.0. I dati qui analizzati coprono il periodo dal 26 aprile 2025 al 30 giugno 2025 gennaio, su un campione di 10 paesi europei (*fonte Shadow Server*).



Osservazioni

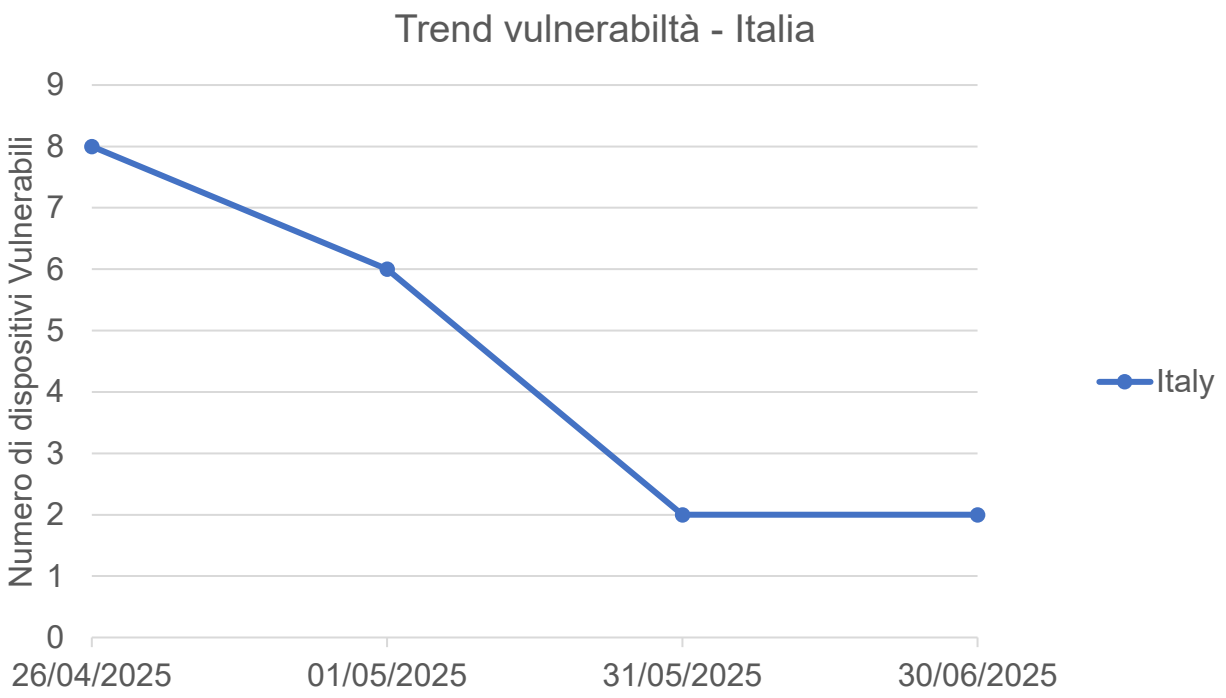
La Germania è di gran lunga il paese più colpito, con un picco iniziale di 30 istanze vulnerabili il 26 aprile, ridottisi drasticamente a 3 entro fine maggio, per poi risalire a 5 a giugno. Questo suggerisce un'efficace risposta iniziale ma forse una parziale ricaduta o nuove istanze esposte.
la Francia ha risposto in modo molto efficiente: da 10 esposizioni iniziali a zero già entro fine maggio. Si tratta della miglior performance tra tutti i paesi

CVE

ANALISI DELLE CVE DEL PRIMO SEMESTRE 2025

Focus sull'Italia

L'Italia ha ridotto rapidamente l'esposizione entro maggio, ma non è riuscita ad azzerarla. La stasi a 2 esposizioni tra maggio e giugno è indicativa di una zona grigia: potrebbe trattarsi di sistemi legacy difficili da aggiornare o non manutenuti. **In termini relativi, l'Italia è tra i paesi più virtuosi, con una riduzione del 75% complessivo**.



Conclusione

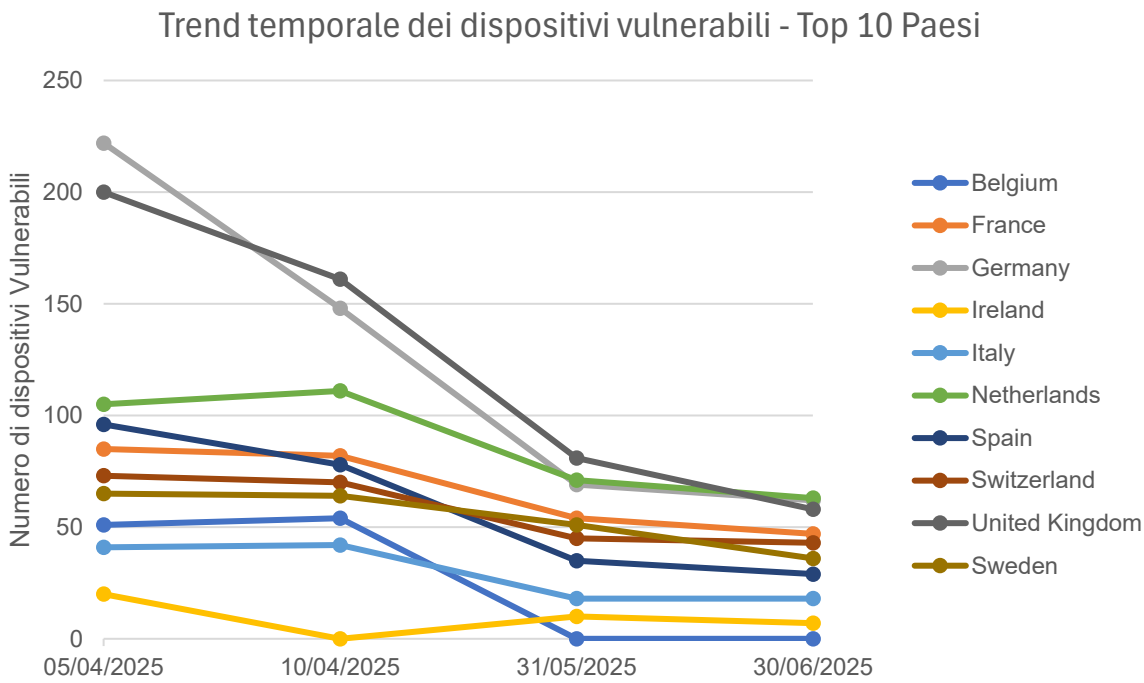
L'analisi mostra come la gestione della **CVE-2025-31324** sia stata in generale proattiva, ma non omogenea. L'Italia ha ridotto rapidamente l'esposizione, ma non è riuscita a completare la bonifica. Rimangono criticità in paesi con esposizioni persistenti (UK, Svizzera, Germania). Questi dati sono preziosi per valutare la maturità delle strategie di patch management a livello europeo.

CVE

ANALISI DELLE CVE DEL PRIMO SEMESTRE 2025

IVANTI Connect Secure VPN CVE-2025-22457

Il 4 aprile 2025, IVANTI ha rilasciato un bollettino di sicurezza per la vulnerabilità CVE-2025-22457, considerata critica con uno score di 9.8. I dati qui analizzati coprono il periodo dal 5 aprile 2025 al 30 giugno 2025 gennaio, su un campione di 10 paesi europei (fonte Shadow Server).



Osservazioni

L'andamento mostra una **tendenza decrescente** in tutti i paesi, ma con **tempi e intensità diverse**.

La Germania è di gran lunga il paese più colpito, con un picco iniziale di 222 istanze vulnerabili ad inizio periodo e con un residuo di 62 al 30 giugno. Il Belgio è il paese che è riuscito ad azzera le istanze vulnerabili.

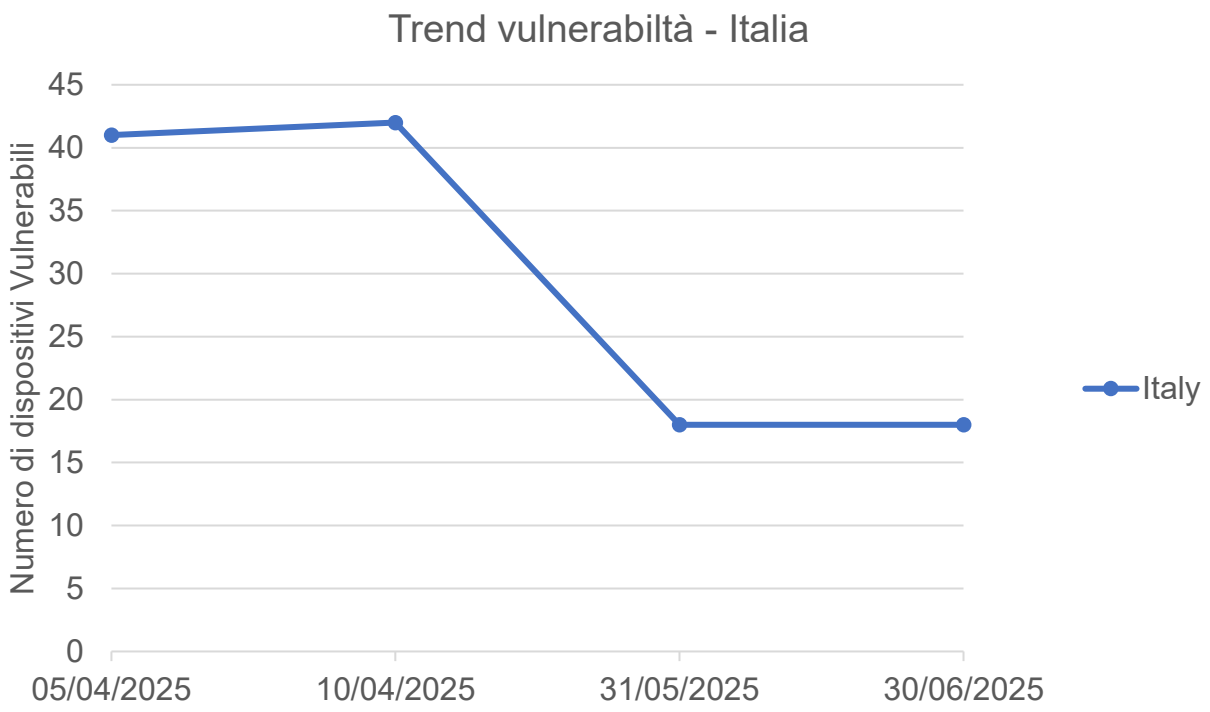
CVE

ANALISI DELLE CVE DEL PRIMO SEMESTRE 2025

Focus sull'Italia

Dopo un **piccolo incremento iniziale** il 10 aprile (da 41 a 42), l'Italia **ha ridotto bruscamente a maggio 18 esposizioni**. Tuttavia, tra maggio e giugno non si registrano miglioramenti: gli stessi **18 sistemi restano esposti**.

L'Italia si colloca a **metà classifica** per performance di mitigazione. Ha fatto meglio di Olanda, Svizzera e Francia in termini percentuali, ma **non ha completato la bonifica**.



Conclusione

Tutti i paesi hanno mostrato una tendenza al miglioramento, ma solo Belgio ha completato la bonifica. L'Italia ha avuto una buona reazione iniziale, ma non è riuscita ad eliminare del tutto l'esposizione. I dati suggeriscono che molti paesi (es. Olanda, Svizzera) abbiano margini di miglioramento nelle strategie di patching e gestione dei sistemi esposti a internet.

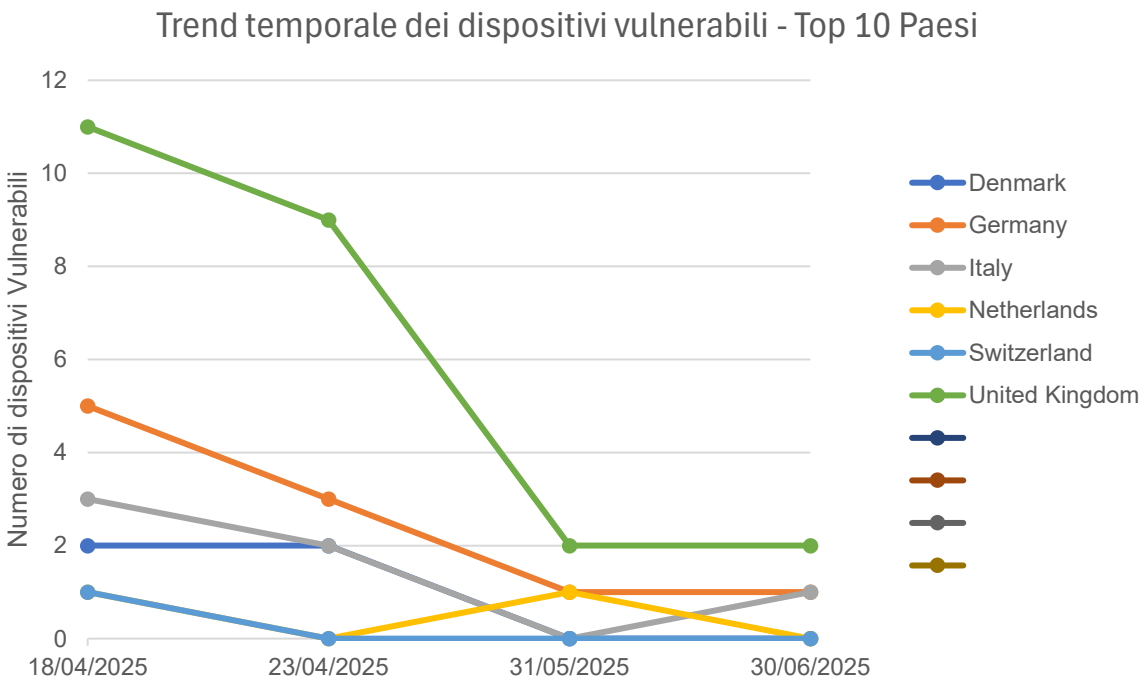
.

CVE

ANALISI DELLE CVE DEL PRIMO SEMESTRE 2025

RCE in Gladinet CentreStack CVE-2025-30406

Ad inizio aprile 2025, Gladinet ha rilasciato un bollettino di sicurezza per la vulnerabilità CVE-2025-30406, considerata critica con uno score di 9.8. I dati qui analizzati coprono il periodo dal 18 aprile 2025 al 30 giugno 2025 gennaio, su un campione di 10 paesi europei (fonte Shadow Server).

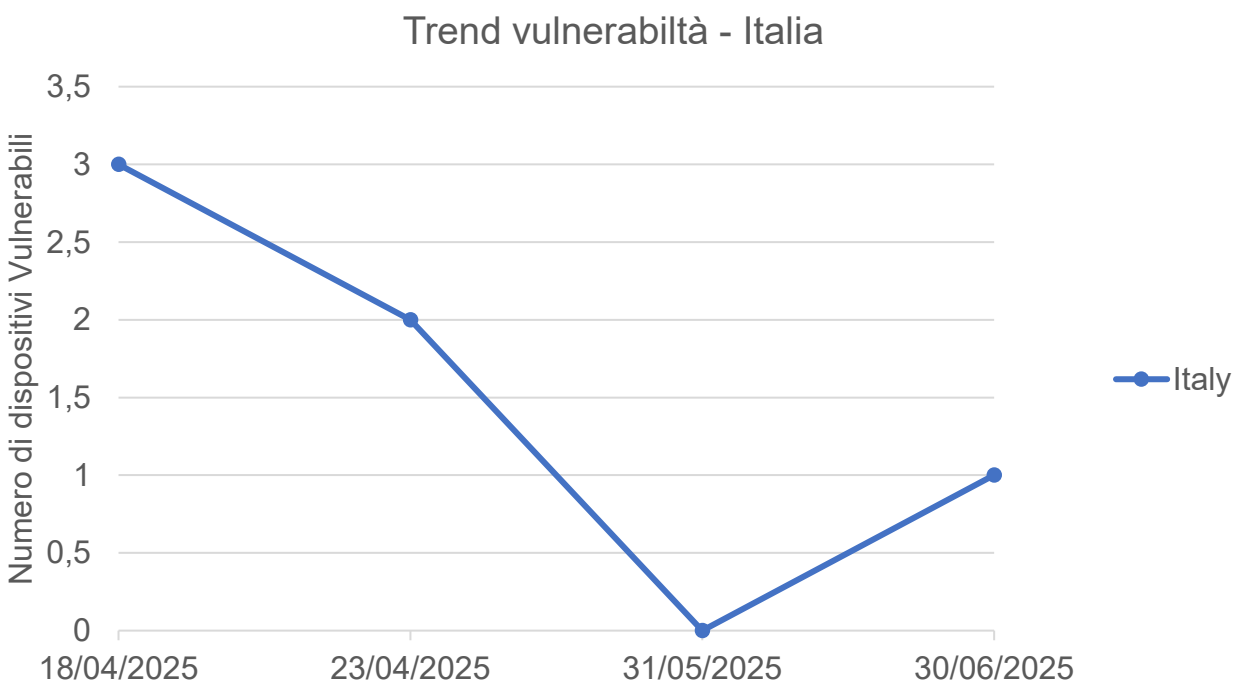


Osservazioni

Danimarca e Svizzera sono gli unici paesi che hanno azzerato completamente l'esposizione entro fine maggio. Ottimo esempio di mitigazione definitiva.
Il Regno Unito, con 11 istanze iniziali, è il più colpito, ma riesce a ridurre dell'82% in due mesi, stabilizzandosi a 2 istanze non risolte.
La Germania mantiene 1 istanza persistente a fine giugno, come il Regno Unito e l'Italia.
Il caso dell'Olanda è interessante: da 1 esposizione a 0, poi torna a 1 a maggio e di nuovo 0 a giugno. Si tratta di un andamento a "singhiozzo", compatibile con l'attivazione e disattivazione di sistemi vulnerabili in ambienti dinamici o cloud.
I numeri molto bassi rilevati rispetto agli altri dataset analizzati in questo report, suggerisce che la vulnerabilità **CVE-2025-30406** non ha avuto una diffusione massiva, ma è rimasta confinata a pochi casi mirati.

Focus sull'Italia

L'Italia sembrava aver **completamente bonificato** la vulnerabilità a fine maggio. Tuttavia, a fine giugno emerge **una nuova esposizione**. Ciò potrebbe indicare: il ripristino di un sistema da backup vulnerabile, la riapertura accidentale di un endpoint, un nuovo **deployment non aggiornato** (ma sono tutte ipotesi non confermabili).
Questo comportamento è rilevante perché suggerisce una **gestione non completamente strutturata** o **assenza di controllo continuo**.



Conclusione

L'esposizione a **CVE-2025-30406** è stata **limitata e gestita piuttosto bene** nella maggior parte dei paesi. L'**Italia** ha reagito rapidamente, ma la **riemersione di un caso a giugno** è un segnale di **residua vulnerabilità infrastrutturale**. In generale, si evidenzia l'importanza del **monitoraggio continuo anche dopo la bonifica iniziale**

DARKLAB COMMUNITY

La community di Dark Lab è il cuore pulsante dietro il report "Dark Mirror". Composta da esperti di Cyber Threat Intelligence (CTI), professionisti della sicurezza informatica e appassionati del settore, la nostra missione è quella di creare un'Italia più resiliente agli attacchi informatici attraverso la condivisione di conoscenze, risorse e competenze.
Dark Lab è una community eterogenea che unisce talenti da vari settori della cybersecurity. I nostri membri includono analisti di minacce, ricercatori, ethical hackers e consulenti di sicurezza, tutti uniti dalla passione per la difesa contro le minacce informatiche. Grazie alla nostra diversità di background e competenze, siamo in grado di affrontare le sfide della cybersecurity da molteplici prospettive.

Pietro Melillo
Esperto di Cyber Threat Intelligence e professore universitario, è il coordinatore del gruppo Dark Lab

LUCA STIVALI
Esperto di Cyber Threat Intelligence e Cyber Security

Reffaela Crisci
Esperta di Cyber Threat Intelligence, coordina un sotto gruppo di DarkLab

Edoardo Faccioli
Esperto di Cyber Threat Intelligence.

Alessio Stefan
Red Teamer e Membro di Dark Lab

Massimiliano Brolli
Esperto di sicurezza, di ricerca dei bug e del Red Team, è il fondatore di Red Hot Cyber

Inva Malaj
Appassionata di Cybersecurity, Intelligenza Artificiale e Analisi Dati

Dark Lab è un gruppo di appassionati di Cyber Threat Intelligence (CTI) e professionisti nel campo dell'intelligence delle minacce. Se sei interessato a partecipare e a contribuire attivamente alla redazione di articoli, a fornire informazioni di prima mano sulla sicurezza digitale e sei un esperto di Cyber Threat Intelligence (CTI), invia il tuo curriculum a redazione@redhotcyber.com per darci modo di valutare l'inserimento nel gruppo.