RedHot Cyber

WWW.REDHOTCYBER.COM

La cybersecurity è condivisione. Riconosci il rischio, combattilo, condividi le tue esperienze ed incentiva gli altri a fare meglio di te.

# Dark Mirror Q1 - 2025 RHC Report Ransomware

DARKLAB
RHC INTELLIGENCE LABORATORY

DakLab è un laboratorio di Intelligence all'interno della vasta community di Red Hot Cyber, specializzato nel monitoraggio delle minacce informatiche. nasce con l'obiettivo di diffondere la conoscenza sulle cyber minacce, contribuendo a rafforzare la consapevolezza e le difese digitali del paese.

# 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 Q1 - 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.



# INTRODUZIONE

Nel panorama odierno della sicurezza informatica, il ransomware continua a rappresentare una delle minacce più pervasive, sofisticate e in rapida evoluzione. Il primo trimestre del 2025 segna un punto di svolta per l'Italia, che con 42 attacchi confermati si posiziona ai vertici della scena europea per volume e frequenza di incidenti, registrando il valore più alto mai rilevato sul territorio nazionale. Questo incremento, in netta crescita rispetto ai 33 attacchi del Q4 2024 e ai 28 del Q1 2024, evidenzia un trend preoccupante che riflette un'escalation senza precedenti della pressione ransomware sul tessuto produttivo e istituzionale del Paese. L'analisi storica dei Q1 dal 2022 al 2025 conferma questa traiettoria: da 37 attacchi nel Q1 2022, si era osservato un calo significativo nel 2023 (24), seguito da una progressiva risalita nel 2024 (33) fino al nuovo massimo attuale. Questo andamento conferma una volatilità strutturale del fenomeno, ma con una tendenza complessiva alla crescita, dovuta in parte alla frammentazione dell'ecosistema ransomware e alla comparsa di nuovi gruppi emergenti meno tracciabili ma altamente aggressivi.Gruppi come Cactus, Ransomhub, Kraken, e i più recenti Sarcoma e Fog, stanno sostituendo progressivamente attori storici come LockBit, la cui presenza in Italia appare in calo, probabilmente a seguito della pressione internazionale e di una riconfigurazione interna del gruppo.

A preoccupare ulteriormente è la massiva esfiltrazione di dati osservata in più casi recenti, con volumi superiori ai 400 GB, segno che le gang criminali stanno puntando più sulla minaccia di esposizione che sulla mera crittografia dei dati.In questo contesto, Dark Mirror – Q1 2025 propone un'analisi dettagliata e multidimensionale dell'evoluzione della minaccia ransomware in Italia e nel mondo. Attraverso dati empirici, studio delle tecniche, tattiche e procedure (TTPs), tracciamento dei wallet legati a campagne di estorsione e interviste esclusive ai threat actor, il report mira a fornire una visione strutturata delle dinamiche attuali del ransomware-as-a-service (RaaS), dei settori maggiormente colpiti e delle vulnerabilità più sfruttate.Il contributo della community Dark Lab di Red Hot Cyber, composta da esperti CTI, analisti e ricercatori, è centrale nella redazione di questo lavoro. Il report nasce infatti da un'attività continua di monitoraggio delle fonti underground, dall'analisi degli indicatori di compromissione (IoC) e da un confronto diretto con le realtà operative del cybercrime.Il nostro obiettivo è duplice: rafforzare la postura difensiva delle organizzazioni italiane e internazionali, e promuovere una cultura della sicurezza basata sulla conoscenza, sulla previsione e sulla risposta efficace. Il primo trimestre del 2025 ci ha mostrato che il ransomware è tutt'altro che in declino: è in metamorfosi, e come tale richiede approcci adattivi, intelligence dinamica e una capacità di lettura strategica del rischio cibernetico.

Pietro Melillo
Direttore del gruppo
Dark Lab Red Hot Cyber

# 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.

**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.

**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.

**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.

L'analisi presentata si basa su un framework comparativo multi-livello, progettato per monitorare l'evoluzione dell'attività ransomware a livello globale. I dati derivano da fonti OSINT, in particolare dalle dichiarazioni pubblicate nei Data Leak Sites (DLS) delle principali gang criminali. L'obiettivo è fornire una rappresentazione coerente e strutturata delle dinamiche operative, tattiche e geografiche osservate nel primo trimestre 2025.

1. Criteri di Selezione e Inclusione

▪ **Gang e TTPs** È stato adottato un criterio di Top 15 per i gruppi ransomware e di Top 20 per le TTPs, riferito al ranking trimestrale. È stato effettuato cross-checking temporale per analizzare la continuità delle entità attive tra i trimestri. Tutti i confronti YoY (Year-over-Year) e QoQ (Quarter-over-Quarter) sono stati limitati alle entità presenti nel ranking del Q1-2025, assunto come baseline analitico

.▪ **Paesi e Settori** Per l'analisi geografica e settoriale è stata utilizzata una soglia minima di TOP 10 Paesi colpiti e per i settori una soglia minima di 40 attacchi dichiarati nel Q1-2025 come criterio di inclusione. In questi ambiti non è stato effettuato cross-checking inter-trimestrale: il trimestre Q1-2025 rappresenta il punto di partenza per tutti i confronti longitudinali.

2. **Preprocessing e Normalizzazione**

Per garantire uniformità e leggibilità nei dati settoriali, prima dell'analisi è stato applicato uno script di ricategorizzazione automatica, che ha: Normalizzato le denominazioni dei settori secondo criteri omogenei; Raggruppato le vittime in macro-settori economici, sulla base di classificazioni funzionali (es. Servizi, Industria, Pubblica Amministrazione, etc.).

Questo passaggio è stato fondamentale per ridurre la frammentazione semantica e ottimizzare la lettura dei flussi nei grafici e nelle serie comparative.

3. **Periodo di Riferimento** Il trimestre Q1-2025 è stato adottato come riferimento unico per tutta l'analisi. Due prospettive temporali sono state utilizzate:
Quarter-over-Quarter (QoQ): confronto con Q4-2024
Year-over-Year (YoY): confronto con Q1-2024.

Metriche Calcolate
**Δ Assoluto**: variazione nel numero di vittime tra due trimestri.
**Δ Percentuale**, secondo la formula:

$$\Delta\% = \left(\frac{Vt - Vt-1}{Vt-1}\right) \times 100$$

dove Vt è il numero di vittime nel Q1-2025 e Vt−1 quello del trimestre di confronto (Q4-2024 o Q1-2024).
Entrambe le metriche sono state applicate a gang, TTPs, settori e Paesi, con attenzione alla distorsione dovuta a basi numeriche ridotte.

4. **Limiti Analitici**

L'analisi riflette esclusivamente gli attacchi rivendicati pubblicamente e pertanto non include incidenti non documentati nei DLS. Per i settori e Paesi non è stata applicata una logica di continuità temporale, ma solo un filtro basato sulla soglia del Q1-2025.

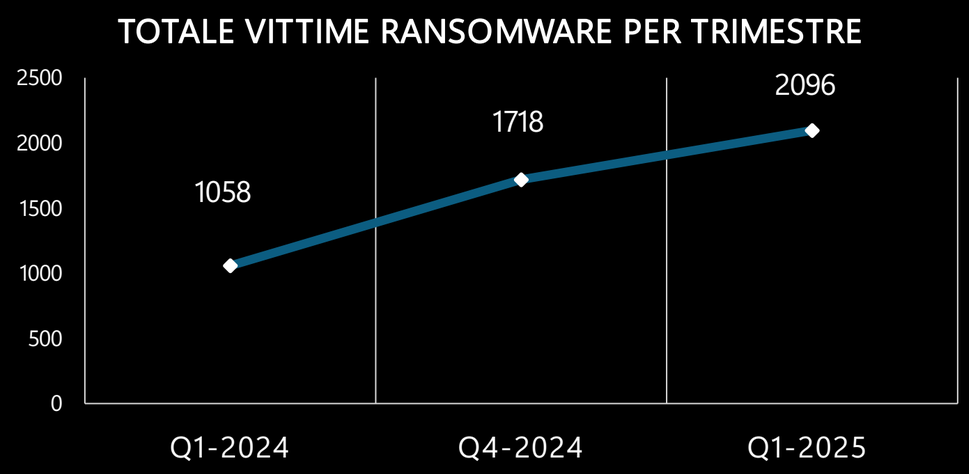
# ANALISI E TENDENZE GLOBALI

**A cura di Inva Malaj**

# TENDENZE

Nel **Q1 2025** il ransomware conferma il proprio status di minaccia sistemica globale. Le vittime complessive nel mondo sono salite a **2.096,** in netta crescita rispetto al trimestre precedente (**+22%**) e quasi raddoppiate rispetto allo stesso periodo dell'anno scorso (**+98,1%**). La curva evidenzia un'accelerazione persistente e allarmante, in linea con la diffusione del modello ransomware-as-a-service (RaaS), la proliferazione delle gang e la crescente superficie d'attacco in ambito entreprise e pubblico.

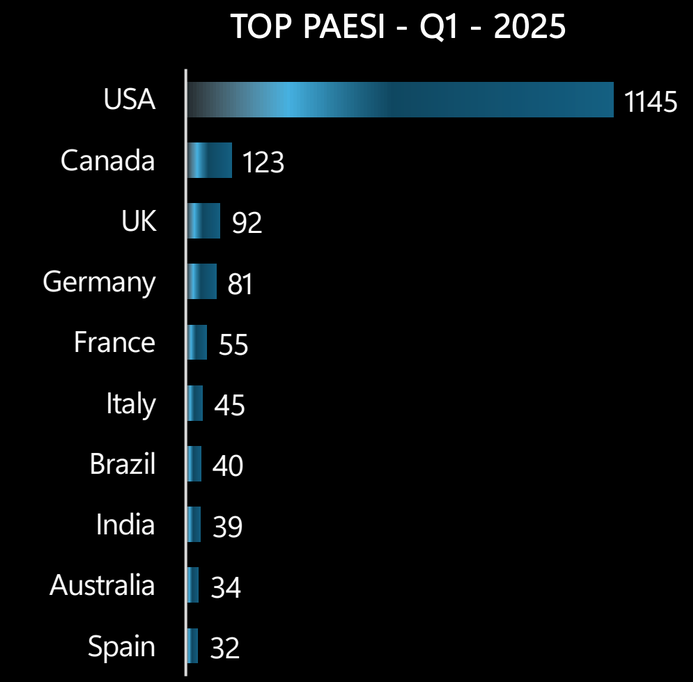
| QoQ<br>Q1-2025 VS Q4-2024 | YoY<br>Q1-2025 VS Q1-2024 |
|---|---|
| 22,0% | 98,1% |




# PAESI PIU'COLPITI

L'analisi mostra i paesi maggiormente colpiti da attacchi ransomware nel Q1-2025, secondo i dati pubblicati dalle gang criminali sui loro Data Leak Sites (DLS). Gli Stati Uniti si confermano nettamente al primo posto, seguiti da Canada, Regno Unito e Germania. Il confronto con i trimestri precedenti evidenzia un'estensione geografica crescente, con un incremento marcato anche in paesi dell'Unione Europea e Sud America.

| Paese | Q1 - 2025 | Paese | Q4 - 2024 | Paese | Q1 - 2024 |
|---|---|---|---|---|---|
| USA | 1145 | USA | 940 | USA | 547 |
| Canada | 123 | Canada | 82 | UK | 64 |
| UK | 92 | UK | 61 | Canada | 62 |
| Germany | 81 | India | 53 | Germany | 39 |
| France | 55 | Germany | 48 | France | 32 |
| Italy | 45 | Brazil | 41 | Italy | 28 |
| Brazil | 40 | France | 41 | Spain | 20 |
| India | 39 | Italy | 41 | Australia | 18 |
| Australia | 34 | Australia | 35 | Sweden | 15 |
| Spain | 32 | Spain | 23 | Brazil | 15 |



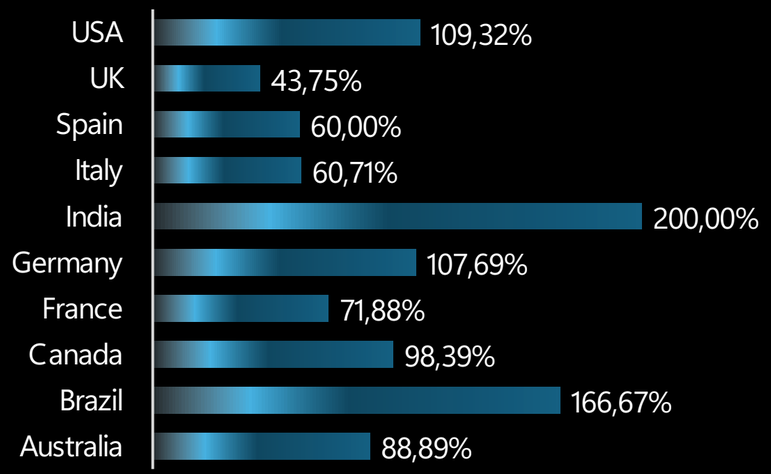
## Analisi Year-over-Year (Q1 2025 vs Q1 2024)

A livello annuale, il ransomware ha mostrato un'espansione significativa in quasi tutte le aree geografiche monitorate. I picchi più estremi si registrano in India (+200%), Brasile (+167%), Australia (+89%) e Canada (+98%), tutti con una più che duplicazione degli attacchi rispetto al Q1 2024. Anche USA (+109%) e Germania (+108%) confermano una crescita sostenuta. Incrementi importanti ma più contenuti emergono in Francia (+72%), Italia (+61%), Spagna (+60%) e Regno Unito (+44%), segno che il ransomware sta espandendo il suo raggio d'azione pur mantenendo un'alta incidenza nei paesi occidentali.

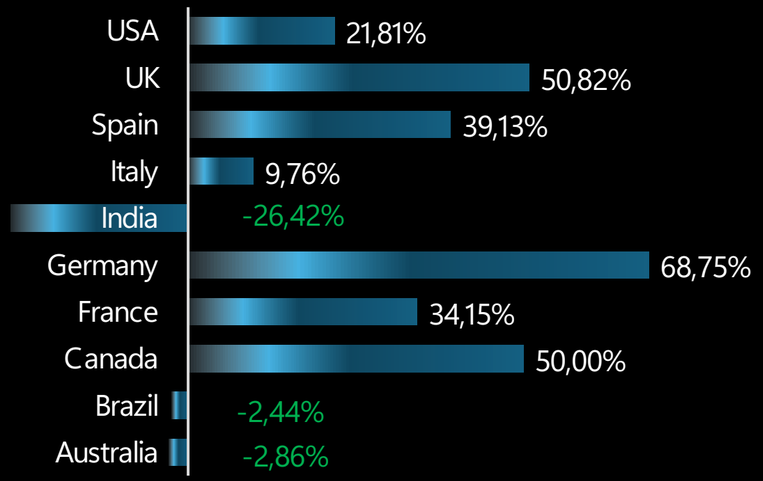
## Analisi Q-over-Q (Q1 2025 vs Q4 2024)

Nel confronto con il trimestre precedente, si registra un'accelerazione sensibile in Germania (+69%), Regno Unito (+51%), Canada (+50%) e Spagna (+39%), seguite da Francia (+34%) e USA (+22%), che segnalano una continuità nell'espansione nei paesi industrializzati. Italia (+10%) mostra invece una crescita marginale. Al contrario, alcuni paesi evidenziano una contrazione: India (-26%), Brasile (-2%) e Australia (-3%), tutti evidenziati in verde, suggerendo una temporanea riduzione dell'attività criminale o una rilocazione delle priorità operative da parte delle gang.

### YOY Δ % Q1-2025 VS Q1-2024



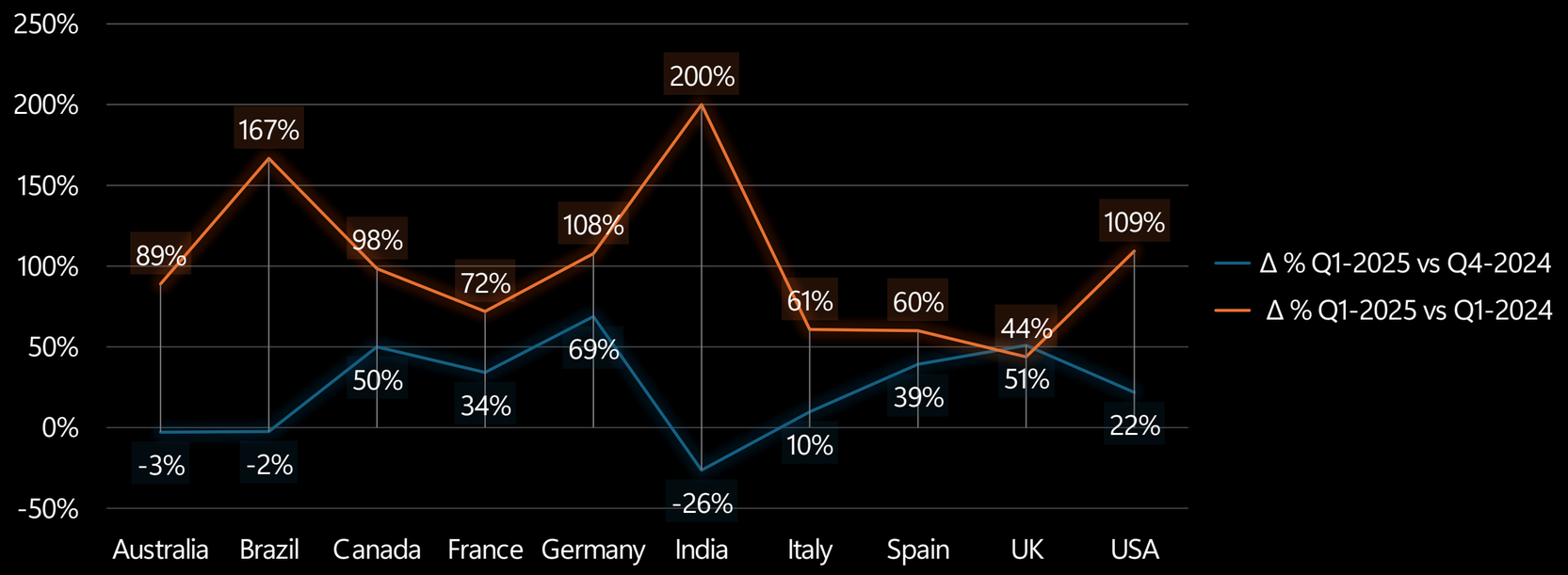

### QOQ Δ % Q1-2025 VS Q4-2024




La geografia del ransomware nel Q1 2025 evidenzia un'espansione importante. Il rischio è divenuto sistemico e non più limitato a singoli paesi.

**Raccomandazioni chiave**: Condivisione di intelligence: Potenziare le reti di scambio informativo tra governi, aziende e fornitori di sicurezza, così da anticipare minacce e target emergenti. **Readiness nazionale e aziendale:** Rafforzare piani di risposta rapida e simulazioni di crisi, specialmente nei paesi con alto tasso di crescita degli attacchi.

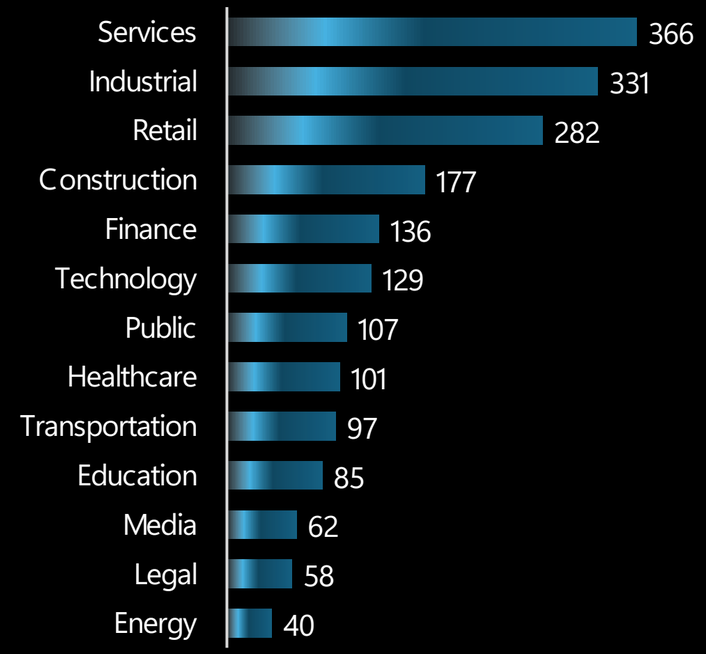
**Formazione e consapevolezza:** Innalzare il livello di competenza delle figure operative in ogni comparto economico, promuovendo programmi strutturati di cyber hygiene. L'approccio deve essere globale e multilivello. Solo la sinergia tra enti pubblici, settore privato e community di cybersecurity potrà ridurre l'esposizione delle aree più a rischio e stabilizzare una minaccia che, se trascurata, rischia di consolidarsi in modo irreversibile.




# SETTORI PIU' COLPITI

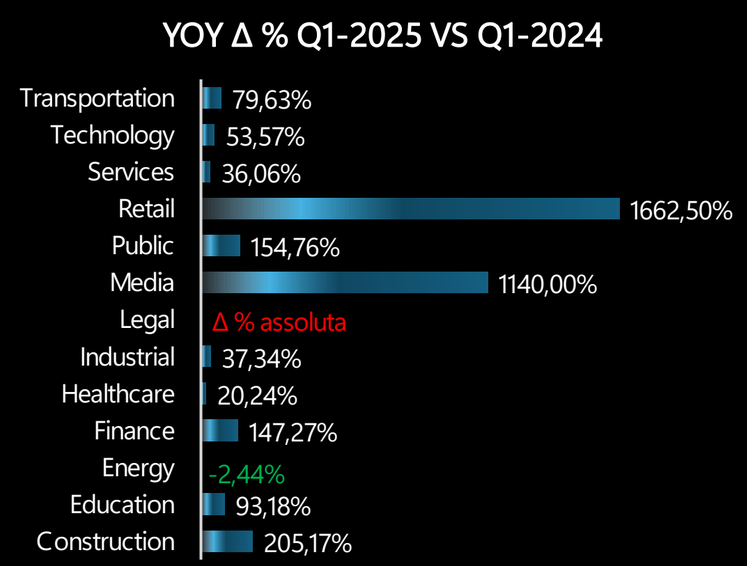
In questa sezione si analizzano i settori economici più colpiti da attacchi ransomware nel **Q1-2025**, sulla base delle segnalazioni pubblicate dai gruppi criminali nei Data Leak Sites (DLS). L'analisi si concentra sui comparti che, nel trimestre di riferimento, hanno registrato almeno **40 attacchi** documentati, selezionati come soglia minima per garantire significatività statistica. A partire da questo sottoinsieme, sono stati confrontati i dati year-over-year (YoY) e quarter-over-quarter (QoQ), per rilevare variazioni strutturali e dinamiche nel targeting delle gang. I risultati evidenziano una pressione crescente su settori come servizi, manifatturiero e retail, confermando una strategia di attacco orientata verso infrastrutture digitali critiche e catene operative ad alta esposizione.

| Settore | Q1 - 2025 | Settore | Q4 - 2024 | Settore | Q1 - 2024 |
|---|---|---|---|---|---|
| Services | 366 | Services | 295 | Services | 269 |
| Industrial | 331 | Industrial | 284 | Industrial | 241 |
| Retail | 282 | Retail | 153 | Retail | 16 |
| Construction | 177 | Construction | 201 | Construction | 58 |
| Finance | 136 | Finance | 112 | Finance | 55 |
| Technology | 129 | Technology | 88 | Technology | 84 |
| Public | 107 | Public | 131 | Public | 42 |
| Healthcare | 101 | Healthcare | 106 | Healthcare | 84 |
| Transportation | 97 | Transportation | 44 | Transportation | 54 |
| Education | 85 | Education | 81 | Education | 44 |
| Media | 62 | Media | 12 | Media | 5 |
| Legal | 58 | Legal | 8 | Legal | 0 |
| Energy | 40 | Energy | 44 | Energy | 41 |



## Analisi Year-over-Year (Q1 2025 vs Q1 2024)

•Nel confronto annuale, si osserva un'escalation estrema degli attacchi nel Retail (+1663%) e nei Media (+1140%), con il settore Pubblico (+155%) che conferma un'elevata vulnerabilità strutturale. Anche Construction (+205%), Finance (+147%) e Legal (valore assoluto rosso critico) mostrano picchi anomali, indicando un'evoluzione delle campagne ransomware verso infrastrutture civili e ambiti istituzionali. Il settore Education (+93%) e quello Transportation (+80%) risultano anch'essi in forte crescita. Più stabili i comparti Technology (+53%), Industrial (+37%) e Services (+36%), che pur con percentuali inferiori restano tra i target principali. Healthcare, nonostante storicamente esposto, cresce solo del +20%. Il settore Energy è l'unico in calo (-2%), segnale potenziale di resilienza o spostamento del focus da parte degli attori malevoli.

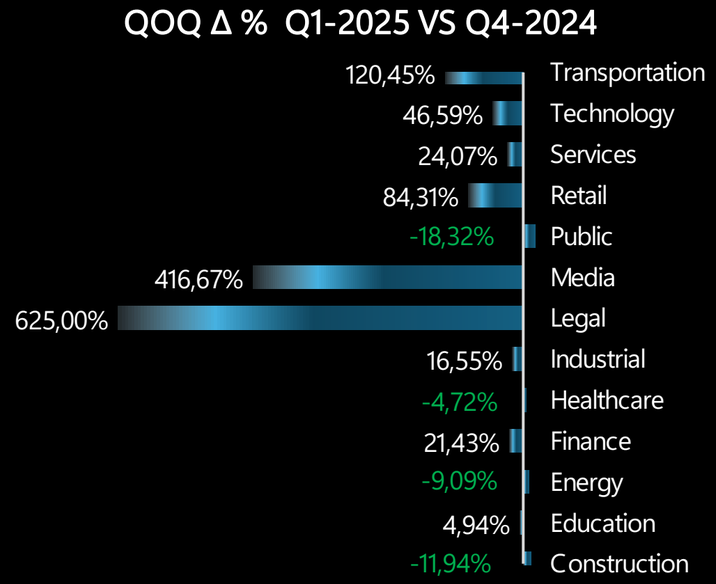


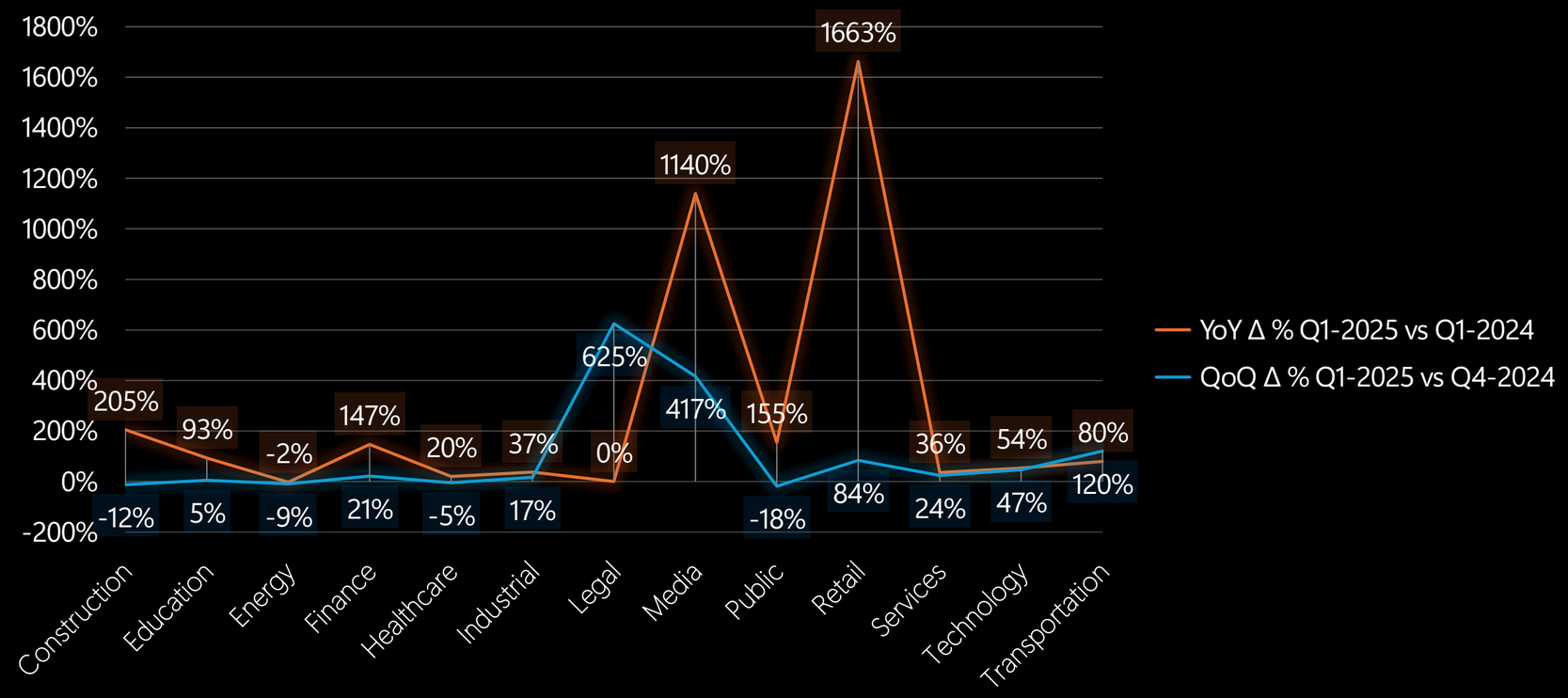

## Analisi Q-over-Q (Q1 2025 vs Q4 2024)

•Nel confronto su base trimestrale, la pressione ransomware si è intensificata nel Legal (+625%), Media (+417%), Transportation (+121%) e Retail (+84%), segno di un'azione offensiva focalizzata e non occasionale. Anche Technology (+46,6%), Services (+24%) e Finance (+21%) mostrano crescite solide.

•All'opposto, alcuni settori registrano una flessione nel numero di attacchi:

Public (-18%), Healthcare (-5%), Energy (-9%) e Construction (-12%). Queste diminuzioni (evidenziate in verde nei grafici) possono riflettere una momentanea ridistribuzione delle priorità operative da parte degli attaccanti, piuttosto che un reale rafforzamento difensivo.




Il Q1 2025 conferma che il ransomware si sta verticalizzando: le gang colpiscono in modo selettivo settori ad alto impatto operativo o economico. Retail, Technology, Finance e Healthcare risultano i più esposti, mentre l'aumento in Construction e Transportation segnala un ampliamento dei target. Le organizzazioni devono adottare un approccio settoriale e proattivo, basato su: Difese contestuali e threat modeling specifico per ogni settore; Gestione del rischio terze parti e verifica supply chain; Simulazioni regolari di crisi e recovery; CTI focalizzata su TTPs settoriali e indicatori precoci. Il ransomware non colpisce a caso: segue logiche di profitto e opportunità. La difesa deve rispondere con intelligenza operativa, rapidità e adattamento.

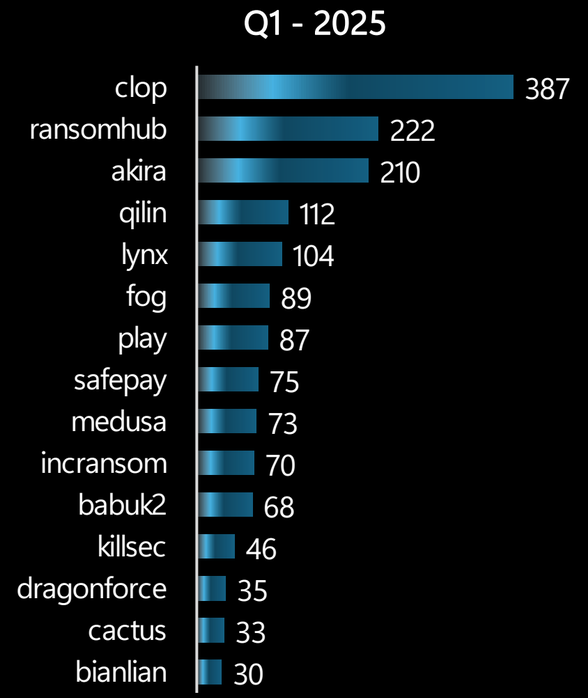
# THREAT ACTORS PIU' ATTIVI

Nel primo trimestre del 2025, l'attività ransomware globale ha mostrato una forte concentrazione attorno a un numero ristretto di gruppi estremamente attivi. I dati riportati si basano esclusivamente sulle dichiarazioni di attacco pubblicate dalle gang ransomware sulle Data Leak Sites (DLS), offrendo così una panoramica trasparente e verificabile delle campagne note. Confrontiamo i gruppi più prolifici del Q1-2025 con i trimestri precedenti, evidenziando l'evoluzione delle principali minacce a livello globale.

| Gang Ransomware | Q1 - 2025 |
|---|---|
| clop | 387 |
| ransomhub | 222 |
| akira | 210 |
| qilin | 112 |
| lynx | 104 |
| fog | 89 |
| play | 87 |
| safepay | 75 |
| medusa | 73 |
| incransom | 70 |
| babuk2 | 68 |
| killsec | 46 |
| dragonforce | 35 |
| cactus | 33 |
| bianlian | 30 |

| Gang Ransomware | Q4 - 2024 |
|---|---|
| ransomhub | 240 |
| akira | 149 |
| killsec | 95 |
| play | 95 |
| clop | 73 |
| fog | 65 |
| hunters | 61 |
| qilin | 57 |
| sarcoma | 56 |
| funksec | 53 |
| apt73/bashe | 49 |
| medusa | 47 |
| blackbasta | 47 |
| safepay | 46 |
| lynx | 44 |

| Gang Ransomware | Q1 - 2024 |
|---|---|
| lockbit3 | 214 |
| play | 76 |
| blackbasta | 75 |
| 8base | 68 |
| hunters | 63 |
| akira | 59 |
| bianlian | 58 |
| alphv/blackcat | 55 |
| medusa | 52 |
| qilin | 32 |
| cactus | 24 |
| ransomhub | 22 |
| ransom | 21 |
| trigona | 19 |
| blacksuit | 19 |



| Gang | Δ QoQ Q1-25 vs Q4-24 | Δ YoY Q1-25 vs Q1-24 | Insight |
|---|---|---|---|
| clop | +430% | +4200% | Escalation massiva, supply chain exploit, picco di 387 vittime in Q1-25. |
| ransomhub | –7.5% | +909% | Leggero calo trimestrale, crescita annuale significativa, 222 vittime Q1-25. |
| akira | +41% | +256% | Consolidamento verticale, TTP in espansione, forte presenza (210 vittime). |
| qilin | +96% | +250% | Alta persistenza operativa, incremento costante. |
| lynx | +136% | Δ assoluta | Emersa in Q4-24, crescita rapida, vettori da investigare. |
| fog | +37% | Δ assoluta | Nuova comparsa, trend di espansione. |
| play | –8% | +14% | Leggero calo trimestrale, crescita annua moderata. |
| safepay | +63% | Δ assoluta | Gang emergente, da 46 a 75 vittime, da monitorare. |
| medusa | +55% | +40% | Crescita graduale, attività costante. |
| incansom | +89% | +1650% | Escalation drastica (4 → 70 vittime), probabile RaaS underground. |
| babuk2 | Δ assoluta | Δ assoluta | Apparizione in Q1-25 (68 vittime). |
| killsec | –52% | +820% | Crollo trimestrale, crescita annuale esplosiva. |
| dragonforce | +106% | +192% | Attacchi raddoppiati, tendenza offensiva in crescita. |
| cactus | +120% | +38% | Picco trimestrale, evoluzione TTP possibile. |
| bianlian | –12% | –48% | Segnali di contrazione, calo progressivo. |
| lockbit3 | –62% | –90% | Riorganizzazione interna o perdita di asset. Continuità operativa compromessa |
| blackbasta | –83% | –89% | Rilevante ridimensionamento o chiusura. |
| 8base | +17% | –59% | Crescita modesta, declino annuo. |
| hunters | –62% | –63% | Forte calo operativo, possibile sospensione attività. |
| alphv/blackcat | –100% | –100% | Sparizione completa dopo Q1-24. |
| ransom | –100% | –100% | Inattività totale riscontrata. |
| trigona | –100% | –100% | Inattività totale riscontrata. |
| blacksuite | –95% | –89% | Calo drastico, possibile fase di cessazione. |
| apt73/bashe | –73% | Δ assoluta | Contrazione significativa, futuro incerto. |
| sarcoma | –59% | Δ assoluta | Contrazione lieve, monitoraggio consigliato. |
| funksec | –96% | Δ assoluta | Contrazione marcata, attività quasi cessata. |

# TECNICHE TATICHE E PROCEDURE

Nel Q1-2025, le tecniche MITRE ATT&CK più frequentemente associate agli attacchi ransomware evidenziano un'evoluzione verso operazioni più mirate e tecnicamente raffinate. Dominano T1486 (Data Encrypted for Impact), T1078 (Valid Accounts) e T1490 (Inhibit System Recovery), mentre emergono significativamente T1059.003 (Windows Command Shell) e T1570 (Lateral Tool Transfer), segnalando un affinamento tattico delle campagne.
**Nota metodologica**: Il grafico mostra le Top 20 TTPs per numero di vittime colpite da gang note per il loro utilizzo, secondo dati estratti da DLS pubblici e fonti OSINT (MITRE, SocRadar, Ransomfeed, Ransomware.live). L'associazione è basata sul profilo tecnico delle gang e non implica l'uso certo di ogni tecnica in ogni singolo attacco.

Di seguito sono presentate le principali tecniche, tattiche e procedure (TTPs) adottate dai principali Threat Actors, secondo il mapping al framework MITRE ATT&CK, riferito al periodo di osservazione considerato.

**T1486** - Data Encrypted for Impact: Ransomware o crittografia dati per scopo distruttivo.
**T1078** - Valid Accounts: Uso improprio di account legittimi per l'accesso.
**T1490** - Inhibit System Recovery: Ostacolo al recupero del sistema per garantire la persistenza.
**T1059.003** - Command and Scripting Interpreter: Windows Command Shell: Esecuzione di comandi attraverso CMD su Windows.
**T1082** - System Information Discovery: Raccolta di informazioni sul sistema target.
**T1570** - Lateral Tool Transfer: Trasferimento strumenti tra sistemi compromessi.
**TA0002** – Execution: Include tutte le tecniche relative all'esecuzione di codice malevolo.
**T1190** - Exploit Public-Facing Application: Sfruttamento di applicazioni rivolte al pubblico.
**TA0005** – Defense Evasion: Tecniche di evasione delle difese.
**TA0040** – Impact: Tecniche con impatto diretto sul sistema, ad esempio distruzione dati.
**T1562.001** - Impair Defenses: Disable or Modify Tools: Disattivazione o modifica di strumenti di sicurezza.
**TA0008** – Lateral Movement: Movimento laterale all'interno di una rete.
**T1059.001** - Command and Scripting Interpreter: PowerShell: Uso malevolo di PowerShell.
**T1083** - File and Directory Discovery: Scoperta di file e cartelle.
**T1018** - Remote System Discovery: Scoperta di sistemi remoti.
**TA0007** – Discovery: Attività di scoperta per identificare risorse da compromettere.
**T1057** - Process Discovery: Scoperta dei processi attivi sul sistema target.
**TA0003** - Persistence: Tecniche di persistenza nel sistema compromesso.
**T1566** - Phishing: Campagne di phishing per acquisire informazioni sensibili o accedere al sistema.
**T1003** - OS Credential Dumping: Dumping delle credenziali dai sistemi operativi.

# COMPARTO ITALIA

**A cura di Vincenzo Miccoli**

# TENDENZE

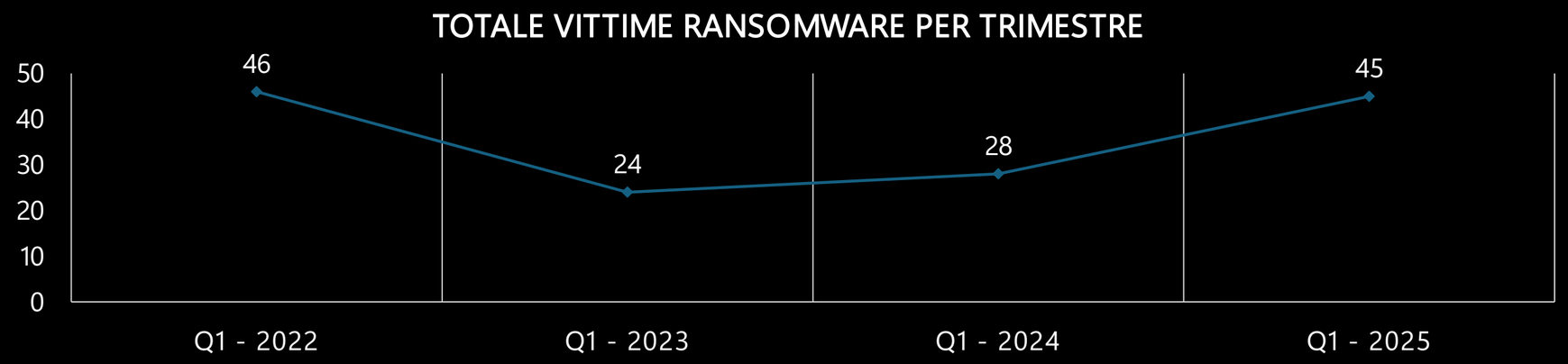
## Statistiche generali:

Numero totale di attacchi rilevati nel periodo.
(01/01/2025 - 31/03/2025 / 45 attacchi)
Confronto statistico con il trimestre precedente e con Q1 2024.
Nel primo trimestre 2025 ci sono stati 45 attacchi (Q1 2025), mentre nell'ultimo trimestre 2024 ci sono stati 41 attacchi. Nel Q1 2024 gli attacchi sono stati 28.

## Osservazioni principali

Si osserva un calo marcato tra Q1 2022 e Q1 2023 (da 46 a 24). Nel Q4 2024 si registra una ripresa con 41 attacchi. Il Q1 2025 conferma l'aumento, toccando 45 attacchi. Trend: Il trend evidenzia volatilità. Dopo il calo iniziale, si osserva una risalita e una stabilizzazione ai livelli del 2022. Il dato di Q1 2025 è allineato a quello di Q1 2022, indicando un rischio costante nel tempo.

**Confronto statistico Q1 2022-2023-2024-2025**




## Diversificazione dei gruppi ransomware attivi

I gruppi che colpiscono l'Italia stanno diventando più frammentati. Non c'è più un solo attore dominante come LockBit, ma una presenza distribuita tra gruppi emergenti come Cactus, Ransomhub e Kraken. Questa frammentazione potrebbe rendere più difficile il monitoraggio e la prevenzione degli attacchi.
Crescita dei gruppi meno noti
Alcuni nuovi gruppi ransomware, come Sarcoma e Fog, stanno prendendo piede in Italia. Questo suggerisce un ricambio tra attori consolidati e nuove minacce in espansione.

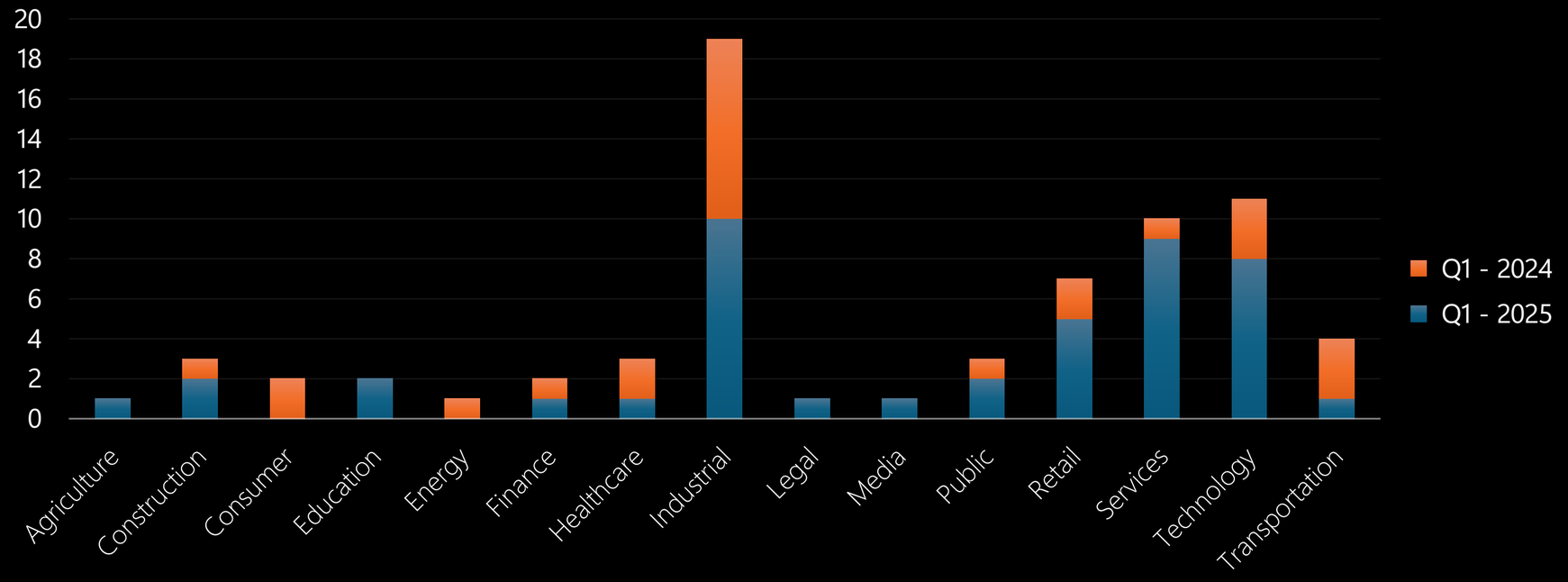
## Aumento delle esfiltrazioni di grandi volumi di dati

Alcuni attacchi recenti hanno portato alla pubblicazione di enormi quantità di dati rubati (es. Everel Group con 440GB e Calspa con 350GB). Questo indica che le gang ransomware stanno puntando sempre più su minacce di esposizione piuttosto che sulla semplice crittografia dei file.
Diminuzione del peso di LockBit 3.0 in Italia
LockBit, che in passato dominava la scena ransomware italiana, sembra aver perso rilevanza rispetto a nuovi gruppi più aggressivi. Questo potrebbe essere dovuto a una maggiore pressione delle forze dell'ordine o a un cambio di strategia del gruppo stesso.

# SETTORI PIU' COLPITI

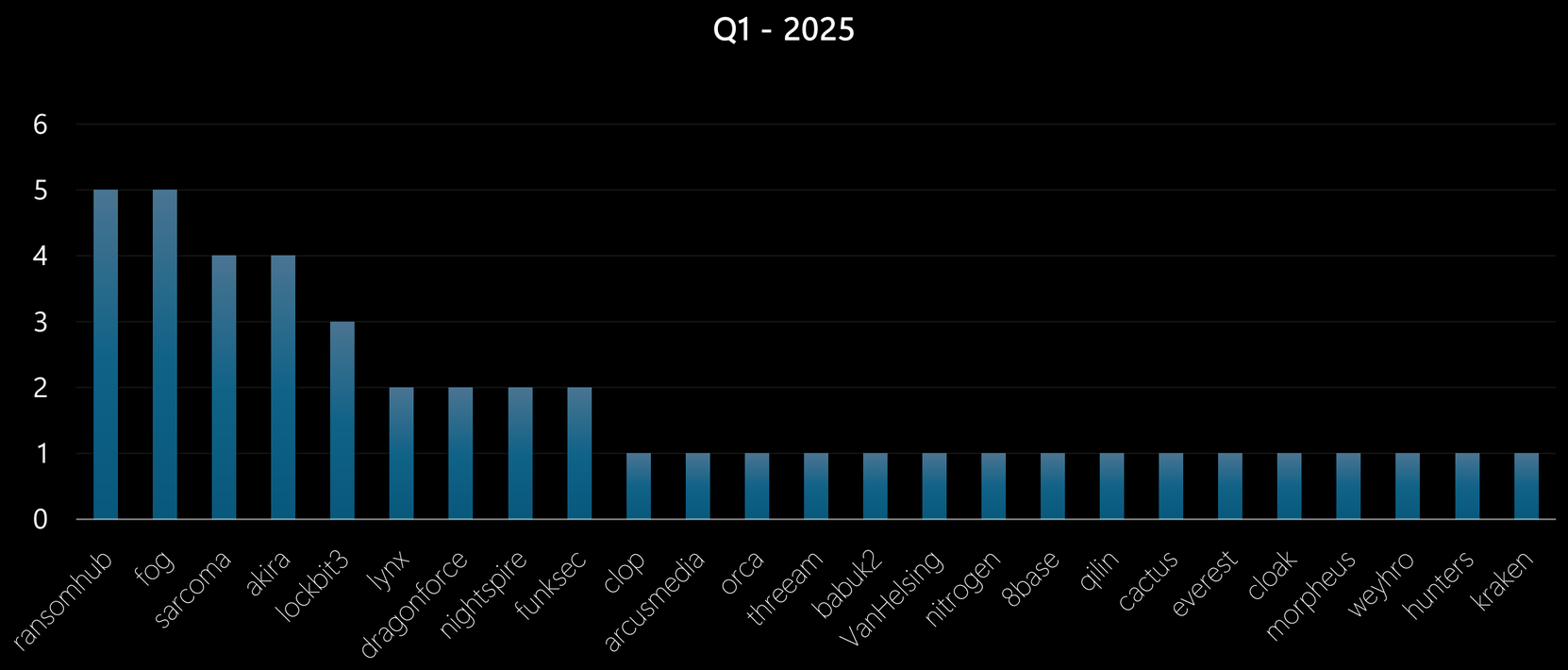
I principali settori più colpiti dai ransomware in Italia nel Q1 2025 sono Industrial, Services, Retail, Technology. Nel grafico viene mostrata la distribuzione degli attacchi ransomware per settore nei trimestri Q1 2024 e Q1 2025. Si osserva un aumento significativo degli attacchi nel settore Industrial, che passa da circa 7 a 18 attacchi. Anche i settori Retail e Services registrano un incremento rispetto all'anno precedente. Il settore Technology mostra invece una diminuzione degli attacchi nel Q1 2025 rispetto al Q1 2024. Altri settori, come Finance, Healthcare e Public, presentano valori contenuti, con variazioni minime tra i due periodi.

**Conclusioni**: Nel 2025 gli attacchi ransomware si concentrano soprattutto sull'industria e sui servizi. Il settore Transportation mostra un calo, segno di un cambiamento tattico degli aggressori. L'aumento verticale nel settore Industrial indica che le infrastrutture produttive italiane sono un bersaglio prioritario.




# THREAT ACTORS PIÙ ATTIVI

Tra gennaio e marzo 2025, l'Italia ha subito attacchi ransomware da 24 gruppi diversi. I più attivi sono stati Ransomhub, Fog, Sarcoma e Akira. Il trend mostra una forte pressione su PMI e settori critici come industria, servizi e tecnologia. La presenza di gruppi emergenti indica un ecosistema ransomware frammentato e competitivo. La varietà di vittime suggerisce che molti attaccanti scelgono obiettivi con difese informatiche deboli. L'Italia si conferma bersaglio costante, evidenziando la necessità urgente di rafforzare la sicurezza, soprattutto nelle realtà minori.




# TECNICHE TATTICHE E PROCEDURE

I principali gruppi di ransomware che hanno attaccato le aziende italiane nel Q1 2025 includono RansomHub, LockBit3, Sarcoma, VanHelsing, Dragonforce, Kraken e Akira. Questi gruppi hanno colpito una vasta gamma di settori e aziende, suggerendo una grande varietà nelle tattiche di attacco.
Nel Q1 2025, l'analisi delle principali TTPs adottate nei cyberattacchi ransomware mostra una prevalenza di metodi di impatto diretto sui sistemi, mirati a massimizzare il danno operativo e aumentare la pressione sulle vittime. Di seguito le cinque tecniche più osservate.

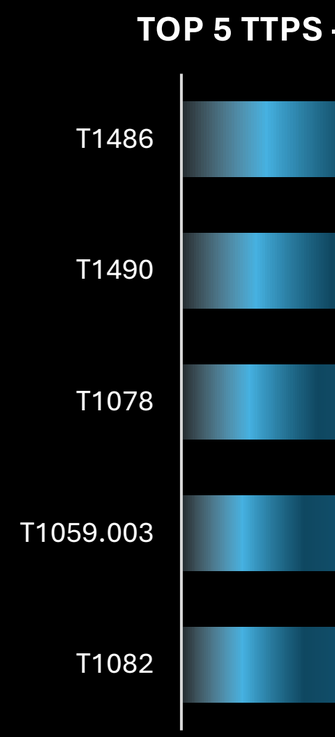
**•Data Encrypted for Impact (T1486) – Cifratura dei Dati a Scopo di Impatto**
Tecnica dominante nei gruppi ransomware e APT.
**Obiettivo:** rendere i dati indisponibili tramite cifratura a fini estorsivi.

**•Inhibit System Recovery (T1490) – Inibizione dei Sistemi di Ripristino**
Tecnica per impedire il ripristino dei sistemi compromessi.
**Obiettivo:** aumentare il danno operativo e forzare il pagamento del riscatto.

**•Valid Accounts (T1078) – Accesso con Account Legittimi**
Tecnica diffusa per abusare di credenziali valide e ottenere accesso furtivo ai sistemi.

**•Windows Command Shell (T1059.003) – Uso della Shell di Comando di Windows**
La cmd.exe viene sfruttata per eseguire comandi arbitrari o automatizzare attività post-compromissione.

**•System Information Discovery (T1082) – Ricognizione Informazioni di Sistema**
Tecnica di raccolta dati su OS e ambiente target per orientare le fasi successive dell'attacco.




# ANALISI DEL RANSOMWARE GLOBALE VS RANSOMWARE ITALIA

A cura di Edoardo Faccioli

# TREND DI ATTACCHI

Il team DarkLab di RHC ha condotto un'analisi dei trend di attacchi confrontando il primo trimestre del 2025 con il primo trimestre dell'anno precedente, il 2024, notando una netta crescita del numero totale di attacchi.

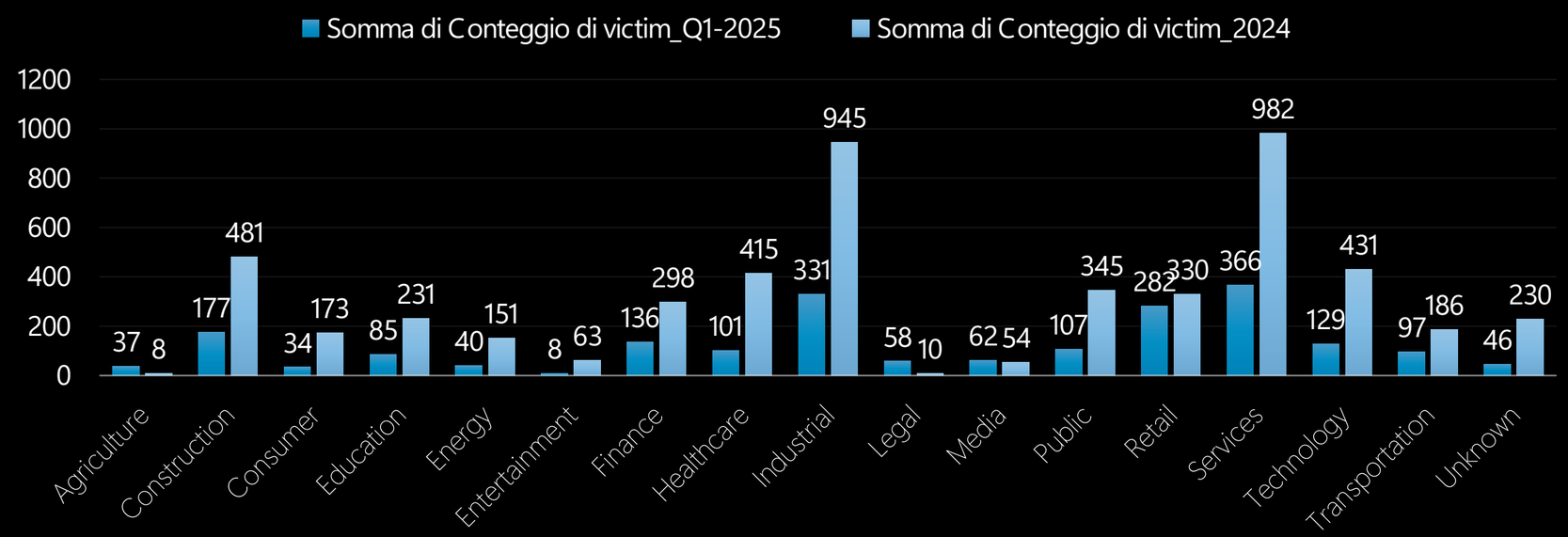
Il panorama ransomware in questo inizio anno si sta diffondendo molto rapidamente, con attacchi sempre più frequenti. Questo comportamento potrebbe inevitabilmente portare a gravi problematiche per tutti i settori lavorativi, indipendentemente dalle dimensioni. Inoltre, potrebbe indicare una capacità di attacco da parte di gruppi molto più sviluppata, che consente agli attori malevoli di ottenere risultati significativi nel breve periodo.

Dai grafici che proponiamo, possiamo notare che gli attacchi globali sono già iniziati nel mese di gennaio, con ben 495 attacchi rispetto ai 286 registrati nello stesso periodo dell'anno 2024. Questo numero è aumentato nel mese successivo, superando la soglia dei 900 attacchi, per poi tornare a 686 attacchi nel mese di marzo, ma comunque con una tendenza rialzista rispetto all'anno precedente. Questo trend conferma un aumento, mostrando un incremento degli attacchi nello stesso periodo in percentuale del +98.86%. Andando a fare un'analisi dettagliata sulle tendenze italiane, notiamo che anche per il nostro paese, come per le tendenze mondiali, gli attacchi sono in aumento. Nello stesso periodo, il numero degli attacchi ha raggiunto i 45 attacchi, rispetto ai 28 attacchi dello scorso anno, con un incremento di circa il +70%.

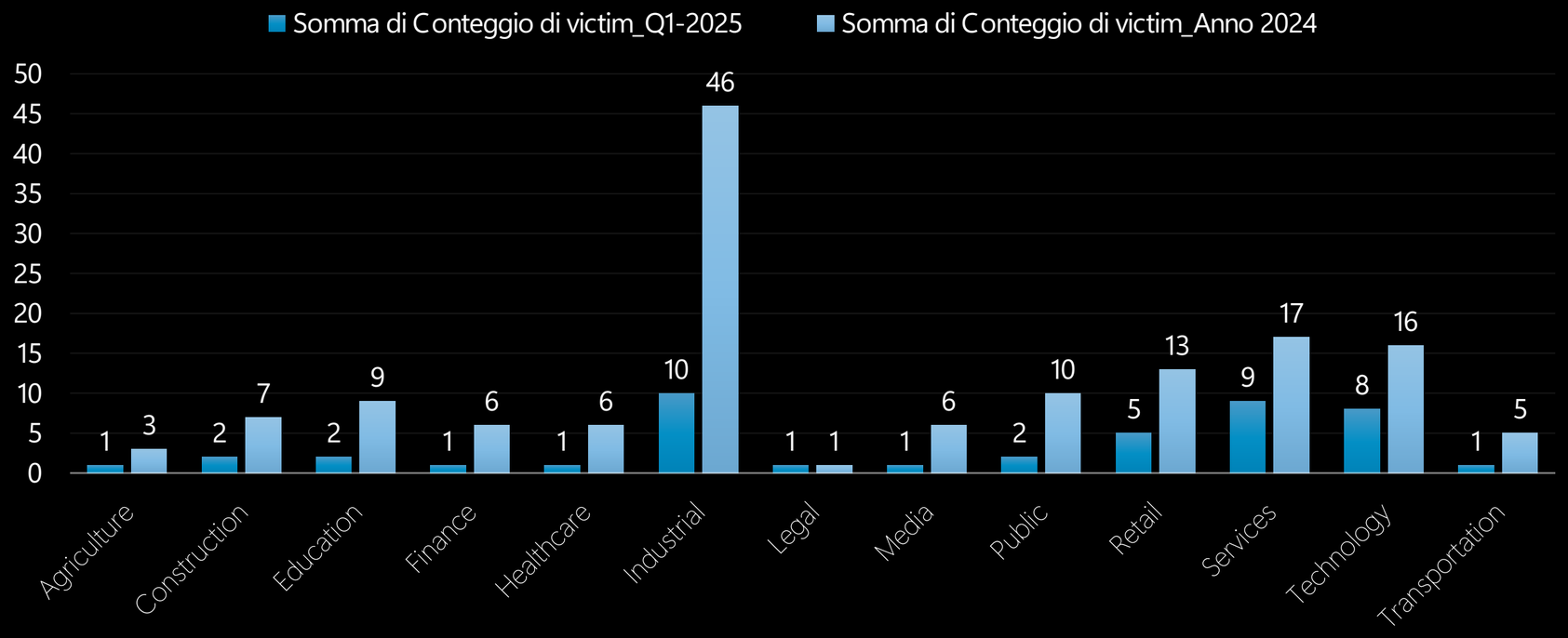


# ANALISI DEI SETTORI COINVOLTI NEL Q1 2025

Analizzando il primo trimestre dell'anno 2025 rispetto al 2024, si nota subito che anche per questa caratteristica gli attacchi sono in aumento, non solo per il numero di attacchi in un determinato settore, ma anche per la varietà dei settori colpiti. Si osserva che, se nel 2024 gli attacchi nel primo trimestre si concentrano principalmente sui settori più sviluppati, come quello industriale o dei trasporti, oggi gli attacchi si stanno espandendo a tutti i settori disponibili e potenzialmente profittevoli.




Queste due tendenze sono identiche sia a livello globale che per quanto riguarda l'Italia, dove i settori coinvolti nel 2025 mostrano già un'importante crescita.




# THREAT ACTORS: ANALISI, STUDI, INTERVISTE

A cura di Pietro Melillo, Alessio Stefan, Edoardo Faccioli e Inva Malaj

# THREAT ACTORS IN EVOLUZIONE / DECLINO

Gang in evoluzione che mostrano comportamenti strutturati e transizione verso modelli RaaS.

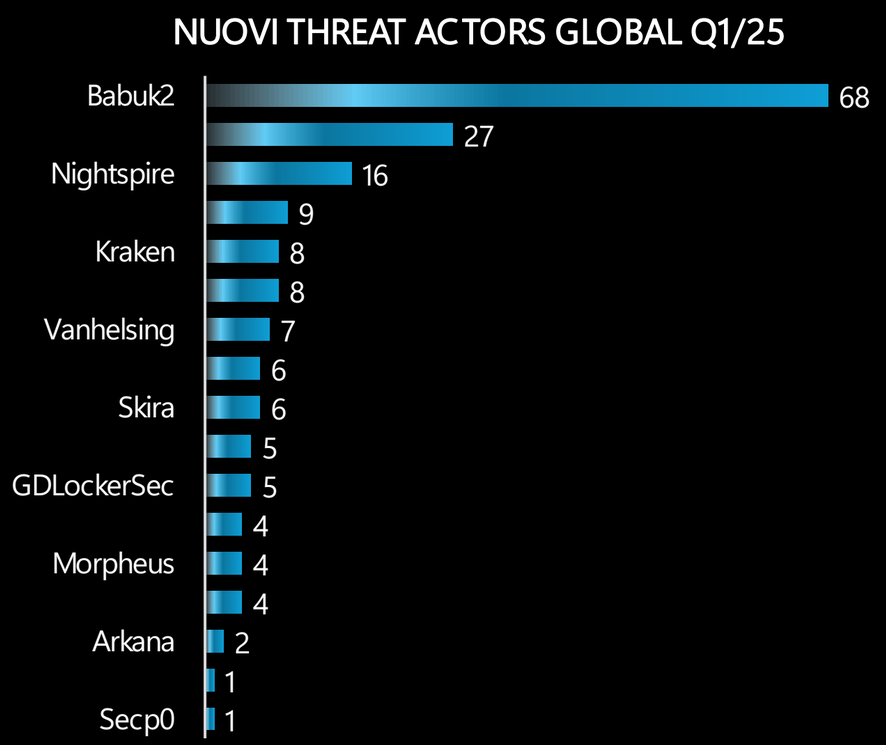
| Gang | Δ QoQ | Δ YoY | Insight |
|---|---|---|---|
| Clop | +430% | +4200% | Dominio assoluto, supply chain attack massivi. |
| Incransom | +89% | +1650% | Escalation rapida, probabile servizio RaaS emergente. |
| Akira | +41% | +256% | Crescita verticale, continuità e consolidamento. |
| Qilin | +96% | +250% | Alta persistenza operativa, espansione coordinata. |
| Cactus | +120% | +38% | Picco operativo, forte attività trimestrale. |
| Dragonforce | +106% | +192% | Incremento marcato, strategia offensiva crescente. |
| Safepay | +63% | Δ assoluta | Gang emergente in fase di strutturazione. |
| Lynx | +136% | Δ assoluta | Crescita esplosiva, nuova minaccia in osservazione. |

Gang in forte declino, alcuni potenzialmente dispersi o confluiti in nuovi cluster.

| Gang | Δ QoQ | Δ YoY | Insight |
|---|---|---|---|
| Killsec | −52% | +820% | Contrazione recente, persistenza YoY elevata. |
| Hunters | −62% | −63% | Declino marcato, calo strutturale stabile. |
| Bianlian | −12% | −48% | Contrazione progressiva, rischio declino. |
| Lockbit3 | −62% | −90% | Collasso operativo, sopravvive a livelli minimi. |
| Blackbasta | −83% | −89% | Ridimensionamento drastico, attività marginale. |
| Alphv/Blackcat | −100% | −100% | Scomparsa totale, cessazione o rebrand. |
| Ransom | −100% | −100% | Cessazione completa. |
| Trigona | −100% | −100% | Cessazione operativa. |
| Funksec | −96% | Δ assoluta | Residuo minimo di attività, possibile fusione. |
| Sarcoma | −59% | Δ assoluta | Forte contrazione trimestrale. |

# NUOVI THREAT ACTORS

Nel periodo analizzato, sono emerse diverse nuove ransomware gang rispetto all'anno precedente. Nel primo trimestre del 2024 ne sono nate 12, mentre nello stesso periodo del 2025 il numero è salito a 17. Questo dato evidenzia la continua crescita del fenomeno e il costante riequilibrio dei poteri criminali. All'interno del mondo underground, infatti, si formano fazioni in competizione tra loro, dando vita a un ambiente sempre più spietato e senza scrupoli.




# NUOVI THREAT ACTORS

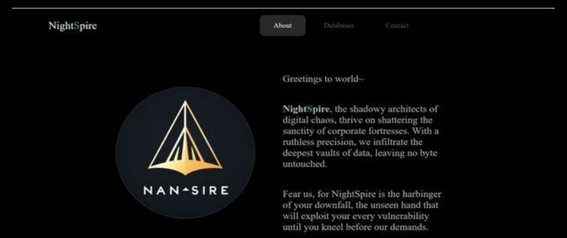
| Gang | Vittime Q1/25 | Insight Operativo |
|---|---|---|
| Anubis | 5 | Attività limitata; operazioni sporadiche che richiedono monitoraggio per eventuali evoluzioni. |
| Arkana | 2 | Presenza marginale; al momento nessuna evidenza di crescita o impatto significativo. |
| Babuk2 | 68 | **Evoluzione consolidata**: Riecheggia attacchi risalenti al 2021 con il nome "Babuk", ora ribrandizzata come Babuk2 – segno di un consolidamento operativo. |
| Chaos | 4 | Attacchi isolati; possibile test sperimentale senza evidenze di strategia continuativa, da rivalutare in futuri monitoraggi. |
| Crazyhunter | 9 | Iniziali attività non ancora strutturate; potenziale seme di crescita se si traduce in operazioni più continuative. |
| Frag | 27 | Notevole impatto per un nuovo player; il livello delle vittime suggerisce un'attività operativa non trascurabile, da monitorare attentamente per evoluzioni tattiche. |
| GDLockerSec | 5 | Attività contenuta; al momento non emergono trend evolutivi, ma monitorare per possibili incrementi o variazioni future. |
| Kraken | 8 | Presenza discreta; se il trend si conferma, potrebbe consolidarsi in un player di rilievo a medio termine. |
| Linkc | 1 | Evento isolato; impatto minimo, probabilmente un caso sporadico da verificare in ulteriori analisi. |
| Morpheus | 4 | Attività limitata; nessun segnale d'evoluzione al momento, ma da monitorare per sviluppi futuri. |
| Nightspire | 16 | Presenza consistente; attore interessante con impatto moderato che potrebbe evolversi in un player più strutturato. |
| Ralord | 6 | Impatto moderato; attivita' confinata con possibilità di crescita o cambiamenti operativi in base al contesto. |
| RunSomeWares | 4 | Attacchi isolati; senza evidenze di consolidamento, da rivalutare in successive analisi per eventuali sviluppi. |
| Secp0 | 1 | Caso sporadico; attività minima, probabilmente un'operazione isolata senza trend evolutivo al momento. |
| Skira | 6 | Presenza stabile; operativa a livello contenuto, da monitorare per eventuali variazioni future. |
| Vanhelsing | 7 | Attività moderata; mantenimento della stabilità operativa con potenziale per crescita se supportata da ulteriori campagne. |
| Weyhro | 8 | Impatto discreto; attuale presenza operativa moderata, da includere nel monitoraggio periodico per rilevare eventuali segnali di incremento. |

# NIGHTSPIRE: UN NUOVO PREDATORE NEL CYBERSPAZIO!

Nel marzo 2025, Red Hot Cyber ha segnalato NightSpire, un nuovo gruppo ransomware scoperto da DarkLab durante il monitoraggio di Data Leak Site nel dark web. Il portale del gruppo, già attivo ma poco conosciuto, rivela una comunicazione aggressiva e un'estetica curata, indice di un attore attento alle strategie dei grandi nomi del settore. La sezione "About" del sito di NightSpire contiene un messaggio intimidatorio, tipico dei gruppi ransomware che cercano di diffondere il terrore tra le aziende. Il linguaggio utilizzato richiama quello di attori ben noti come BlackCat, LockBit e Conti, sottolineando la loro intenzione di colpire organizzazioni vulnerabili e minacciarle per ottenere un riscatto. Ma dietro la retorica si cela una struttura tecnica solida. NightSpire adotta lo schema della doppia estorsione: sottrazione di dati seguita da minacce di pubblicazione. Il sito include una sezione "Databases" con informazioni sulle vittime e countdown per il rilascio dei dati. I canali di comunicazione sono multipiattaforma: email cifrate (ProtonMail, OnionMail), form online e un canale Telegram per trattative e aggiornamenti, in linea con il modus operandi dei gruppi RaaS moderni. L'origine del gruppo è ancora incerta, ma la presenza scenica, la scelta linguistica e la struttura tecnica suggeriscono un rebranding o la rinascita di un attore esperto. NightSpire mira alla destabilizzazione, non solo all'infezione, colpendo aziende distribuite su più territori. È probabile che stia ancora testando la propria infrastruttura o cercando esposizione.

Conclusione: NightSpire non innova, ma perfeziona. Un gruppo che comunica con intelligenza scenica e agisce con precisione operativa. Non va sottovalutato: l'approccio suggerisce un'evoluzione consapevole del modello ransomware-as-a-service.
Sintesi (8 righe max)NightSpire è un nuovo gruppo ransomware emerso nel 2025 con un portale aggressivo e tecnicamente maturo. Utilizza doppia estorsione, countdown e canali cifrati per aumentare la pressione sulle vittime. Il linguaggio scenografico e l'estetica curata suggeriscono influenze da RaaS affermati. Potrebbe trattarsi di un rebranding da parte di attori esperti. L'obiettivo è seminare caos, non solo infettare. Il gruppo appare ancora in fase di test, ma con un'identità già definita. Va monitorato con attenzione. Opinione NightSpire non è una minaccia di passaggio. L'equilibrio tra narrativa strategica e operatività concreta è tipico di chi ha già esperienza nel settore. L'assenza di storicità è solo apparente.

Per maggiori informazioni:
Fonte: Melillo, P. (2025, 13 marzo). Arriva NightSpire! Un nuovo attore nel panorama del ransomware. Red Hot Cyber.



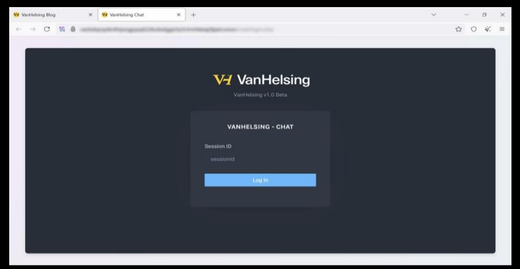

# VANHELSING RAAS: UNA NUOVA RAAS

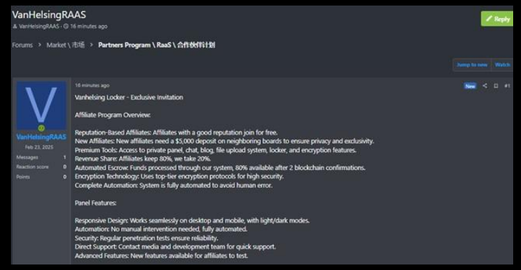
VanHelsing RaaS: silenzioso, strutturato, pronto a scalare
Nel marzo 2025, Red Hot Cyber ha documentato l'attività di VanHelsing RaaS, nuovo gruppo ransomware apparso il 23 febbraio su forum underground, con un primo attacco già pubblicato su un Data Leak Site. Il gruppo si presenta con un'infrastruttura professionale e un programma di affiliazione selettivo: ingresso gratuito per criminali affermati, 5.000 dollari per i novizi. La piattaforma offre pannello web, crittografia avanzata, tool di esfiltrazione, automazione completa e una chat riservata, escludendo Telegram. Il revenue sharing prevede l'80% all'affiliato e il 20% a VanHelsing, con pagamenti tramite escrow su blockchain per evitare frodi interne. La prima vittima è un ente pubblico, segno di un possibile focus su target istituzionali e civili, spesso vulnerabili. Sebbene il DLS riporti un solo attacco, la struttura suggerisce che il gruppo sia in fase di test operativo, con potenziale per un'espansione rapida, seguendo il modello LockBit. VanHelsing non cerca visibilità immediata, ma costruisce fiducia interna, automazione e controllo. L'approccio ibrido tra decentralizzazione e rigore operativo lo rende un gruppo con ambizioni chiare e capacità già in atto.

VanHelsing RaaS è un gruppo ransomware emerso nel 2025 con una struttura tecnica avanzata e un modello di affiliazione calibrato. Offre canali privati, escrow blockchain, e un'infrastruttura completamente automatizzata. La prima vittima è un ente pubblico, segno di possibili focus istituzionali. L'assenza di Telegram e l'uso di chat riservate indicano attenzione alla sicurezza interna. Il gruppo sembra in fase iniziale ma pronto a espandersi rapidamente.

Conclusioni: VanHelsing è l'archetipo del ransomware moderno: silenzioso, efficiente e centrato sull'automazione. La scelta di strumenti privati e il controllo dei flussi economici rivelano un'intelligenza operativa non comune. È un attore da tenere sotto stretta osservazione.

Per maggiori informazioni:
Fonte Melillo, P. (2025, 19 marzo). VanHelsing RaaS: Un nuovo modello di Ransomware-as-a-Service in espansione. Red Hot Cyber.




# L'INTERVISTA A HELLCAT

Nel Q1 2025, Red Hot Cyber ha pubblicato un'intervista esclusiva al collettivo HellCat,.
HellCat nasce come un piccolo collettivo di hacker senza grandi ambizioni, ma si evolve rapidamente in un'entità strutturata, con un focus preciso su obiettivi di alto profilo. La transizione a un modello Ransomware-as-a-Service non è stata pianificata, ma è stata accelerata dalla percezione mediatica definito come RaaS prima ancora di esserlo, il gruppo ha deciso di costruire attorno a questa etichetta una piattaforma reale, con un programma di affiliazione ristretto e selettivo. Gli affiliati accedono a un ransomware locker avanzato e multipiattaforma, con funzionalità moderne e un'interfaccia efficiente. Il target minimo è un'azienda con almeno 40 milioni di euro di fatturato annuo, e sono escluse categoricamente le vittime di basso profilo. Regole ferree e marketing mirato: HellCat non punta solo ai profitti, ma alla reputazione. Il programma di affiliazione è altamente controllato, e chi entra deve aderire a standard elevati sia tecnici che "etici". Il gruppo dichiara di offrire le commissioni di riscatto più competitive sul mercato, elemento che gioca un ruolo chiave nel reclutamento di affiliati. Interessante anche la scelta di posizionarsi pubblicamente come "marchio", registrando addirittura una società in Francia con il nome HELLCAT SOFTWARES RAAS.

L'ironia delle baguette e il messaggio nascosto: Quando RHC domanda del famigerato riscatto "in baguette", HellCat conferma che era una provocazione satirica rivolta alla Francia e alle sue multinazionali.

Nessun sistema di monetizzazione alternativo, solo un'azione mediatica per rafforzare il loro storytelling criminale. Una mossa studiata per far parlare di sé – e ci sono riusciti.. Secondo HellCat, la sicurezza media delle organizzazioni attaccate è "piuttosto bassa". L'unico consiglio che offrono suona beffardo ma concreto: investire nella formazione. La maggior parte delle violazioni, affermano, avviene per colpa del social engineering. Un'ammissione che suona come un avvertimento per chi ancora considera l'elemento umano un fattore secondario nella sicurezza informatica. Un gruppo, una visione, nessuna scadenza. Oggi HellCat conta un team ristretto, composto da pochi membri accuratamente selezionati, e ha in cantiere nuove funzionalità oltre al ransomware principale. Non c'è una roadmap a tempo: il gruppo intende operare a lungo termine, reinvestendo i guadagni nello sviluppo di nuovi strumenti, espandendo il proprio marchio e consolidando la propria reputazione.

**Conclusioni:**
HellCat rappresenta un'evoluzione netta del ransomware: non più solo codice, ma cultura, branding e selezione chirurgica. L'elemento inquietante è la loro lucidità: strategia, ironia e regole etiche formano un mix efficace e pericoloso. Un modello da non sottovalutare, perché non punta solo ai soldi, ma alla longevità operativa.

Per maggiori informazioni:
Fonte: Red Hot Cyber (2025, 31 marzo). Intervista a HellCat – La chiave è assicurarsi che tutti comprendano la cybersecurity.

# NIGHTSPIRE – LA NOSTRA INTERVISTA ESCLUSIVA

Dopo il nostro primo focus su NightSpire a marzo 2025, Red Hot Cyber è riuscita a contattare direttamente la gang tramite canali sicuri nel dark web. Il risultato è un'intervista esclusiva, la prima in assoluto. Su 15 domande inviate, il gruppo ha risposto solo a tre, ma quanto dichiarato basta a delinearne profilo, strumenti e ideologia. Estratti dell'intervista a NightSpire (marzo 2025)

**Domanda 5** – Avete in programma di ampliare i servizi offerti con il vostro RaaS? Se sì, quali?

Risposta: «*Stiamo per iniziare a vendere documenti aziendali riservati, schede sanitarie, cartelle cliniche… tutte informazioni utili e preziose per lo sviluppo di altri soggetti.*»

Questo indica un'evoluzione dal semplice riscatto alla monetizzazione dei dati come merce, all'interno dell'ecosistema black market dell'intelligence industriale.

**Domanda 6** – Parlateci del vostro ransomware: quali sono le sue caratteristiche? Quali OS supporta? Vi siete ispirati ad altri strumenti esistenti? Quanto tempo ha richiesto lo sviluppo?

**Risposta:** «*Il nostro ransomware è pronto per tutti i sistemi operativi: Windows, MacOS, Linux (Ubuntu, ESXi…), Android… Lo abbiamo sviluppato in modo mirato per ogni OS e lo usiamo in attacchi specifici.*

*Alcune aziende sostengono di poterlo decrittare, quindi abbiamo cambiato interamente il nostro algoritmo di cifratura. Ora è tutto nuovo e pronto a colpire.*»

NightSpire mostra capacità tecniche avanzate e reattività alle difese, segno di un ciclo evolutivo maturo.

**Domanda 9** – Al momento sembra che il vostro RaaS sia guidato solo da logiche economiche. Ci sono anche motivazioni politiche, sociali o ideologiche?

**Risposta:** «*Qualsiasi Paese o azienda che si limiti a seguire l'Occidente continuerà a essere un nostro bersaglio. Continueremo a danneggiarli.*»

Una svolta netta: emergono motivazioni ideologiche, che proiettano NightSpire oltre la criminalità economica, verso un profilo ibrido, potenzialmente geopolitico.

**Conclusioni** NightSpire dispone di ransomware multipiattaforma e aggiornati, ha un modello di business che include la vendita di dati sensibili e rivela motivazioni ideologiche ostili all'Occidente. È un attore giovane ma sofisticato, con tratti che sconfinano nella minaccia APT. Se le intenzioni dichiarate troveranno riscontro sul campo, potremmo assistere a una nuova forma di RaaS, ibrida e geopoliticamente schierata.

# TECNICHE TATTICHE E PROCEDURE (TTPS) IN EVOLUZIONE / DECLINO

A cura di Inva Malaj

L'analisi comparativa delle TTPs adottate dalle gang ransomware tra Q1-2024, Q4-2024 e Q1-2025 evidenzia una crescente sofisticazione e standardizzazione degli attacchi. La tecnica **T1486 (Data Encrypted for Impact)** emerge come predominante, con un marcato incremento nell'ultimo trimestre analizzato. Tecniche come **T1078 (Valid Accounts)** e **T1490 (Inhibit System Recovery)** rimangono centrali, mentre emergono significativamente **T1059.003 (PowerShell)** e **T1570 (Lateral Tool Transfer)**. Questa evoluzione indica una chiara tendenza verso operazioni più mirate, aggressive e tecnicamente complesse, sottolineando la necessità di strategie difensive proattive basate su un'intelligence dettagliata delle minacce.

| Gang | TTPS | Nr. Attacchi Q1/25 | Gang | TTPS | Nr. Attacchi Q4/24 | Gang | TTPS | Nr. Attacchi Q1/24 |
|---|---|---|---|---|---|---|---|---|
| 31 | T1486 | 1583 | 31 | T1486 | 1231 | 33 | T1486 | 903 |
| 31 | T1078 | 1356 | 26 | T1078 | 989 | 18 | T1082 | 731 |
| 17 | T1490 | 1279 | 16 | T1082 | 855 | 21 | T1078 | 667 |
| 13 | T1059.003 | 1225 | 17 | T1490 | 840 | 20 | T1190 | 646 |
| 15 | T1082 | 1206 | 13 | T1059.003 | 799 | 16 | T1490 | 590 |
| 7 | T1570 | 1140 | 14 | T1083 | 730 | 12 | TA0002 | 587 |
| 9 | TA0002 | 1029 | 10 | TA0002 | 695 | 16 | T1562.001 | 527 |
| 17 | T1190 | 1020 | 7 | T1570 | 694 | 11 | T1133 | 512 |
| 10 | TA0005 | 1017 | 11 | TA0005 | 694 | 11 | T1027 | 484 |
| 9 | TA0040 | 1014 | 14 | T1562.001 | 663 | 19 | T1083 | 463 |
| 14 | T1562.001 | 994 | 18 | T1190 | 653 | 11 | T1566 | 434 |
| 7 | TA0008 | 985 | 9 | TA0040 | 653 | 6 | TA0004 | 413 |
| 10 | T1059.001 | 939 | 8 | TA0008 | 621 | 6 | T1567.002 | 410 |
| 13 | T1083 | 913 | 11 | T1057 | 583 | 6 | T1547 | 409 |
| 9 | T1018 | 893 | 10 | T1059.001 | 557 | 9 | T1070.004 | 407 |
| 9 | TA0007 | 879 | 11 | T1003 | 555 | 15 | T1059.001 | 403 |
| 10 | T1057 | 835 | 10 | TA0007 | 548 | 8 | T1485 | 397 |
| 7 | TA0003 | 762 | 5 | T1048 | 529 | 8 | TA0010 | 389 |
| 10 | T1566 | 742 | 10 | T1133 | 510 | 13 | TA0005 | 383 |
| 10 | T1003 | 738 | 15 | T1059 | 503 | 11 | TA0007 | 382 |

# TENDENZE STRATEGICHE

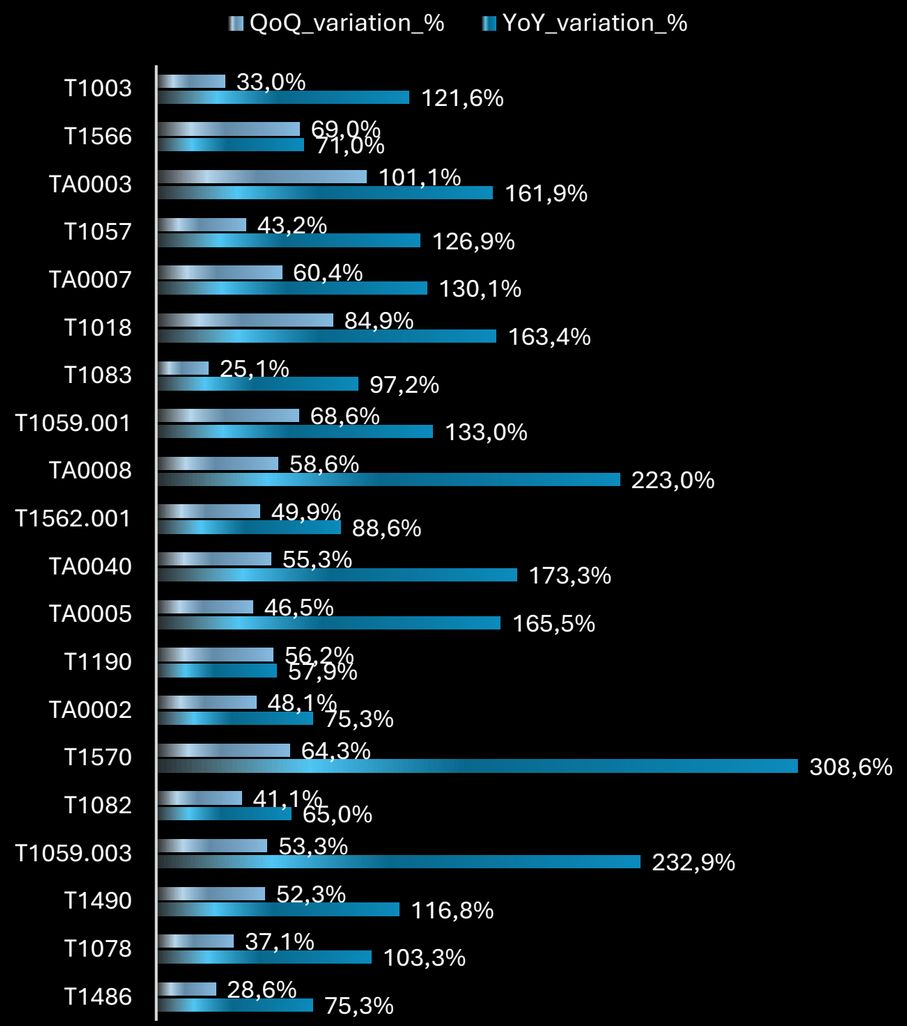
**Tendenze Annuali (Q1-2025 vs Q1-2024)**
Forte incremento tra le TTPs comuni alla top 20: **T1570** (+309%), **T1059.003** (+233%) e **TA0008** (+223%) si affermano tra le più dinamiche.
**T1486** si conferma stabile al vertice con +75% di crescita rispetto alla top 20 di Q1-2024.

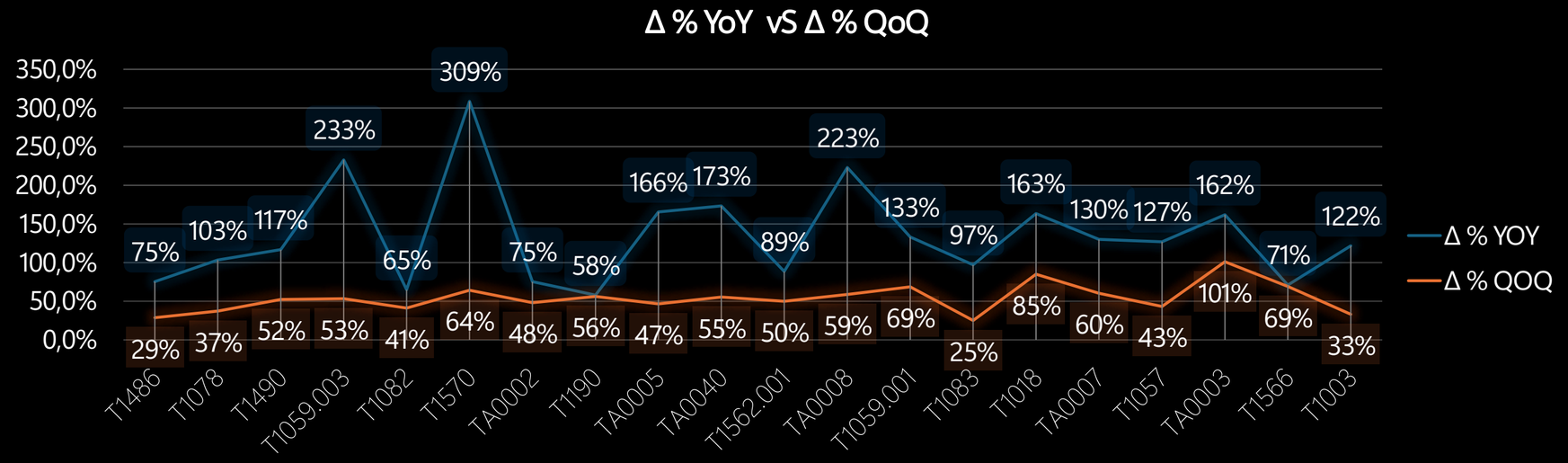
**Tendenze Trimestrali (Q1-2025 vs Q4-2024)**
**TA0003** (+101%), **T1018** (+85%) e **T1566** (+69%) mostrano le crescite relative più elevate tra le TTPs presenti in entrambe le top 20 trimestrali.
**T1059.001** e **T1570** registrano variazioni QoQ superiori al 60%, segnalando intensificazione delle fasi di persistenza e scoperta.

**Tecniche in Calo o Sostituite**

Le seguenti tecniche, presenti nella top 20 di **Q1-2024**, non compaiono nella top 20 di **Q1-2025**:
- **T1048** – Exfiltration Over Alternative Protocol
- **T1133** – External Remote Services
- **T1027** – Obfuscated Files or Information
- **T1567.002** – Exfiltration to Cloud Storage
- **T1547** – Boot or Logon Autostart Execution
- **T1485** – Data Destruction

Questo indica una transizione verso tecniche più selettive, invisibili o distribuite su nuove fasi della kill-chain.




## Implicazioni Operative

L'adattamento continuo delle gang ransomware richiede risposte difensive evolute e proattive:

- **Monitoraggio avanzato** basato su analisi comportamentale (Behavioral Analytics) per identificare tempestivamente l'uso di strumenti come PowerShell e tecniche di lateral movement.
- Implementazione di **controlli di sicurezza avanzati** e policy restrittive sulle tecnologie native del sistema operativo (LOLBin, Living-off-the-Land Binaries).
- Sviluppo di **threat intelligence proattiva** per identificare tempestivamente variazioni e trend emergenti nelle tecniche ransomware

## Conclusioni Strategiche

Le gang ransomware mostrano una capacità di rapido adattamento delle loro strategie offensive, puntando a tecniche sempre più integrate e meno facilmente individuabili. Una difesa efficace deve evolvere costantemente, adottando un approccio contestuale e proattivo, basato sull'intelligence continua delle TTPs emergenti e sulle capacità di risposta e mitigazione comportamentale.

La comprensione e l'anticipazione delle evoluzioni nelle TTPs ransomware rappresentano oggi un requisito essenziale per mantenere un adeguato livello di resilienza cyber.

# ANALISI TRIMESTRALE DELLE PRINCIPALI CVE DEL PERIODO

A cura di Luca Stivali

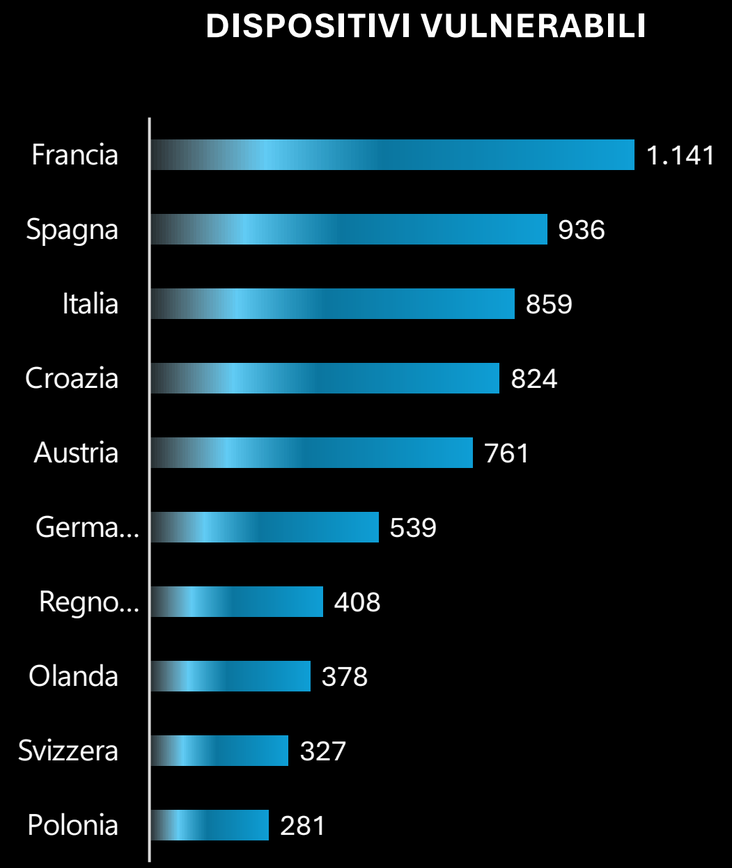
# INTRODUZIONE

Il presente report trimestrale ha l'obiettivo di monitorare l'esposizione dei dispositivi alle principali vulnerabilità (CVE - Common Vulnerabilities and Exposures) rilevate nel corso del trimestre in esame. L'analisi si concentra sul periodo compreso tra la data di pubblicazione di ciascuna CVE e la fine del trimestre, con l'intento di valutare il livello di risposta delle organizzazioni in termini di applicazione delle patch di sicurezza.

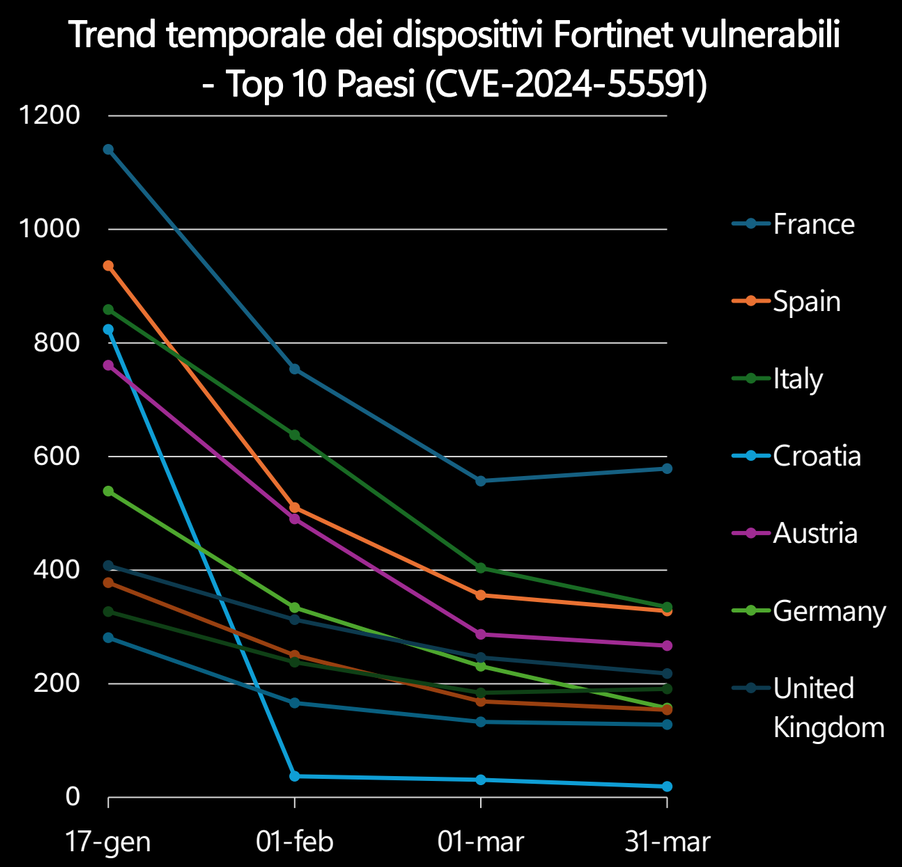
Attraverso il monitoraggio del trend di esposizione, idealmente decrescente, è possibile ottenere una visione chiara dell'efficacia delle strategie di gestione delle vulnerabilità adottate, evidenziare eventuali ritardi nell'attuazione delle contromisure correttive e identificare aree critiche su cui 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.

## Fortinet CVE-2024-55591

Il 15 gennaio 2025, **Fortinet** ha rilasciato un bollettino di sicurezza per la vulnerabilità **CVE-2024-55591**, considerata critica. I dati qui analizzati coprono il periodo dal 17 gennaio al 31 marzo 2025, su un campione di **47** paesi europei (fonte Shadow Server).




# TREND TEMPORALE – GENNAIO → MARZO 2025

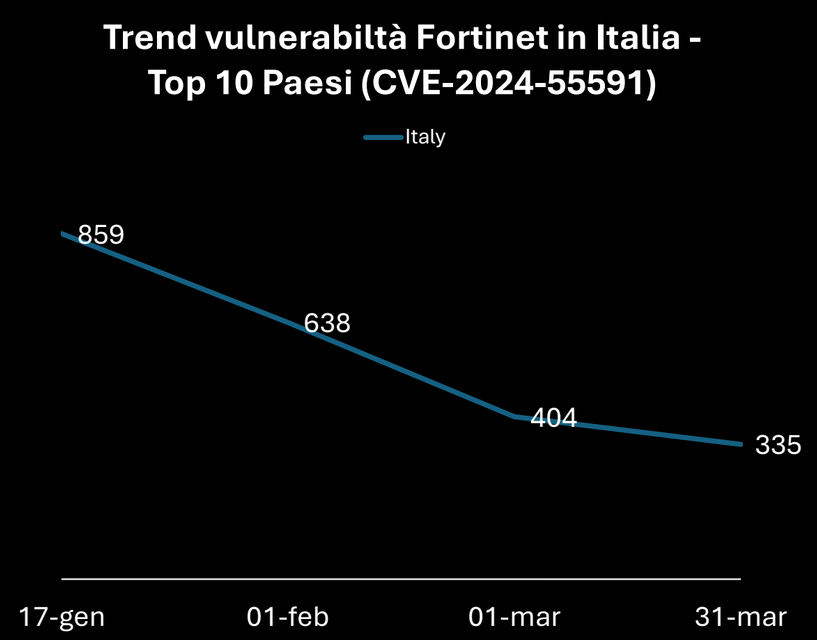



Tutti i paesi mostrano un calo sensibile nel numero di dispositivi vulnerabili:

- Francia: da 1.141 a 579 (riduzione del 49,26%)
- Spagna: da 936 a 328 (riduzione del 64,96%)
- **Italia: da 859 a 335 (riduzione del 61,0%)**
- Croazia: da 824 a 31 (riduzione del 97,69%)
- Austria: da 761 a 267 (riduzione del 64,91%)
- Germania: da 539 a 157 (riduzione del 70,87)
- Regno Unito: da 408 a 218 (riduzione del 46,57%)
- Olanda: da 378 a 154 (riduzione del 59,26%)
- Svizzera: da 327 a 191 (riduzione del 41,59%)
- Polonia: da 281 a 128 (riduzione del 54,45%)

# FOCUS SULL'ITALIA

L'Italia parte al terzo posto in Europa per esposizione, con **859** dispositivi vulnerabili il 17 gennaio. Si può osservare una riduzione complessiva del **61%** dei dispositivi vulnerabili.




## Osservazione

La curva italiana mostra un comportamento "a scalino", con una mitigazione più incisiva nelle prime due settimane e un rallentamento successivo. È verosimile che molti dispositivi residui siano ancora in ambienti dove l'applicazione delle patch è meno tempestiva (es. sedi remote, apparati obsoleti, o gestiti da terzi).

## Curiosità e Insight

Il paese con dispositivi più vulnerabili inizialmente è la Francia. Il paese più "virtuoso" con la riduzione più netta è la Croazia (da 824 a 19 dispositivi con una riduzione del 97,69%). La tendenza comune: calo in tutti i paesi, ma senza raggiungere l'azzeramento totale

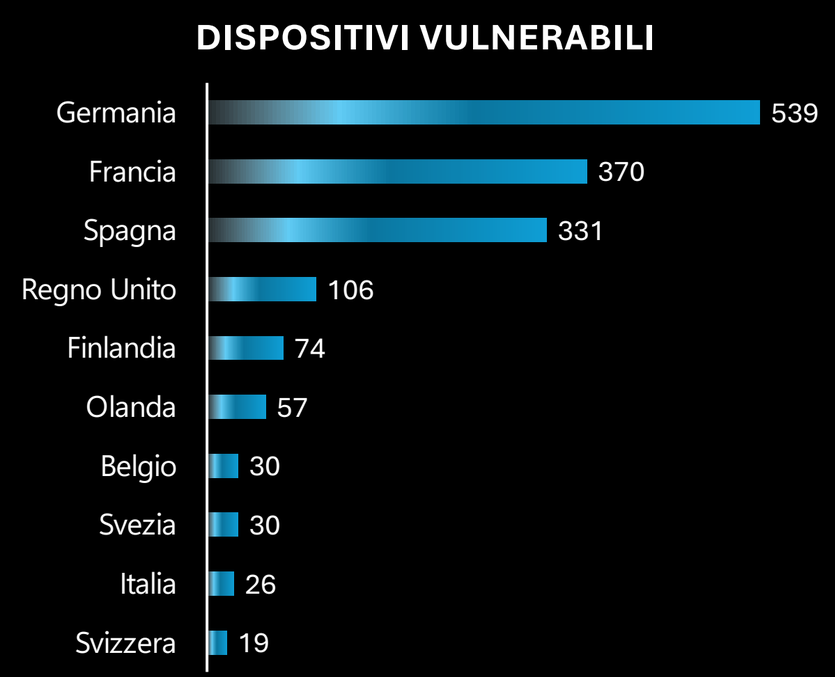
## Conclusione

I dati rivelano un'ampia esposizione iniziale in Europa alla CVE-2024-55591, mitigata progressivamente ma non ancora risolta completamente a fine trimestre. Serve una fase 2 di remediation più profonda. L'Italia, pur in calo costante, rimane tra i paesi con la maggiore superficie di attacco.

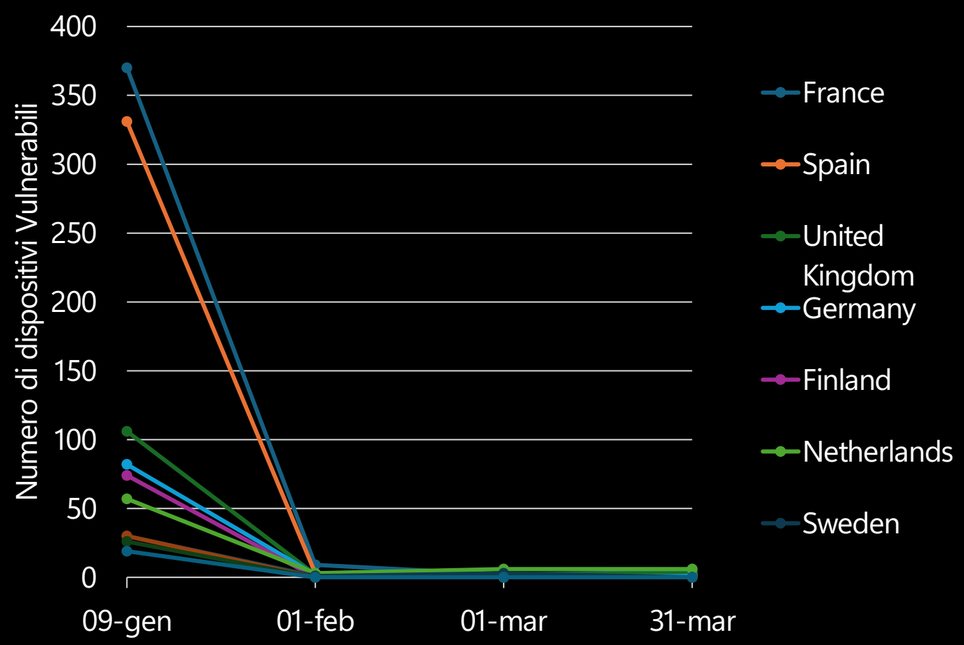
# IVANTI CVE-2025-0282

Il 9 gennaio 2025, è stata resa pubblica la vulnerabilità CVE-2025-0282 che ha interessato dispositivi Ivanti esposti in rete. Il presente report analizza i dati relativi a 24 paesi europei tra il 9 gennaio e il 31 marzo 2025 (fonte Shadow Server).

## Top 10 Paesi all'inizio del periodo (9 Gennaio 2025)




# TREND TEMPORALE – GENNAIO → MARZO 2025



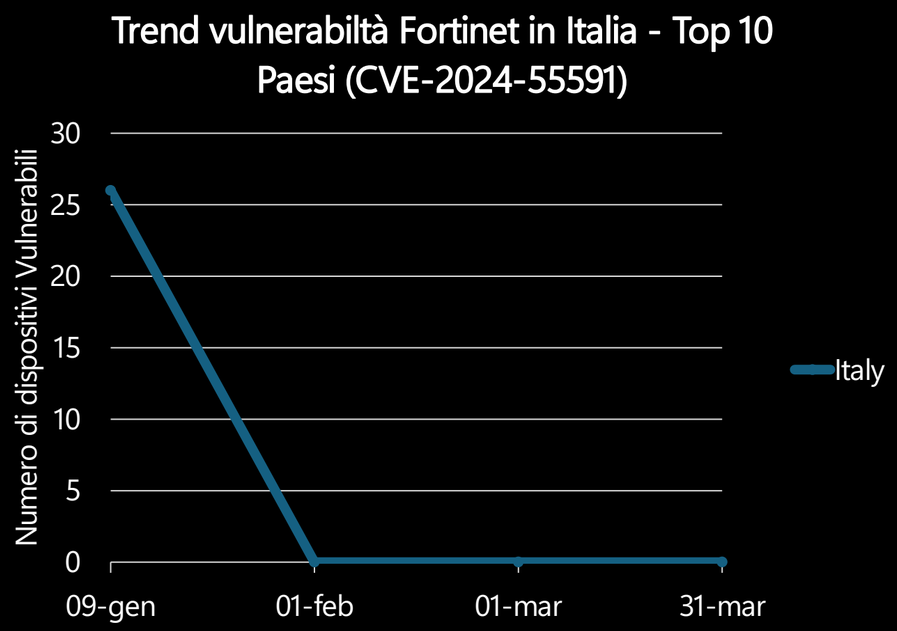

I paesi con il maggior numero iniziale di dispositivi vulnerabili (Francia, Spagna, Regno Unito) hanno mostrato un trend costantemente decrescente. In particolare:

- Francia: da 370 a 4 (riduzione del 98,2%)
- Spagna: da 331 a 2 (riduzione del 99,4%)
- Regno Unito: da 106 a 3 (riduzione del 97,17%)
- Germania: da 82 a 1 (riduzione del 98,78%)
- Finlandia: da 74 a 0 (riduzione del 100%)
- Olanda: da 57 a 6 (riduzione del 89,4%)
- Svezia: da 30 a 0 (riduzione del 100,00%)
- Belgio: da 30 a 0 (riduzione del 100%)
- **Italia: da 26 a 0 (riduzione del 100%)**
- Svizzera: da 19 a 0 (riduzione del 100%)

Questo suggerisce che le azioni correttive sono state implementate rapidamente nelle prime settimane.

# FOCUS SULL'ITALIA

L'Italia ha registrato 26 dispositivi vulnerabili alla data del 9 gennaio 2025. Non risultano ulteriori rilevazioni nei mesi successivi, il che potrebbe indicare una mitigazione immediata.




## Curiosità e Insight

- Paese con più dispositivi iniziali: Francia (370)
- Riduzione più rapida: Finlandia con l'azzeramento dei dispositivi vulnerabili nei giorni immediatamente successivi
- **Italia è risultata tra i paesi più veloci a rimuovere completamente l'esposizione**

## Conclusione

La CVE-2025-0282 ha avuto un impatto iniziale contenuto rispetto ad altre vulnerabilità critiche, ma ha coinvolto diversi paesi europei. Il monitoraggio mostra che la maggior parte dei dispositivi vulnerabili è stata progressivamente rimossa o messa in sicurezza nel giro di due mesi. Il caso italiano rappresenta un esempio di risposta rapida ed efficace alla minaccia.

# 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

**VINCENZO MICCOLI**
Cyber Security Analyst, costantemente motivato dalla volontà di approfondire le mie conoscenze e progredire costantemente.

**ALESSIO STEFAN**
Studente magistrale di AI & Cybersecurity e CTF player

EDOARDO FACCIOLI
Esperto di Cyber Threat Intelligence.

**INVA MALAJ**
Appassionata di Cyber Security e Cyber Threat Intelligence