TRACKING RANSOMWARE : OCTOBER 2025

Published On : 2025-11-07

Share :

EXECUTIVE SUMMARY

In October 2025, ransomware activity surged globally, marking a significant resurgence after a period of mid-year stability. Victim counts climbed to 738, driven by renewed campaigns from leading operators and the emergence of several new groups. Qilin more than doubled its attacks to 181 victims, while Sinobi expanded sixfold, signaling aggressive growth among established actors. At the same time, new entrants such as Black Shrantac, Coinbase Cartel, and GENESIS intensified the threat landscape, collectively contributing to a rise in targeted data extortion campaigns. Attackers increasingly exploited kernel-level vulnerabilities, runtime environments, and trusted code-signing mechanisms, revealing a shift toward stealthier, hybrid attack models that evade traditional endpoint defenses. Industries most affected included Professional Services, Manufacturing, Information Technology, and Healthcare, with attackers focusing on sectors offering high disruption potential and ransom leverage. Geographically, the United States remained the epicenter of global ransomware activity, followed by Canada, France, and Germany, while expanding campaigns across Asia and the Middle East signaled a broader international reach. October also marked the rise of industrial extortion, exemplified by the Asahi Breweries incident, where ransomware caused direct operational disruption. Overall, October 2025 underscored a new phase of technical sophistication and industrial targeting, as ransomware evolved from data encryption to strategic business disruption, leveraging downtime, reputational damage, and financial pressure as its primary extortion tools.

Welcome to the October 2025 Ransomware Threat Report. This report delivers a detailed analysis of the ransomware landscape, highlighting the emergence of new ransomware groups, evolving attack techniques, and notable shifts in targeted industries. By examining key trends, tactics, and significant incidents, this report aims to support organizations and security teams in understanding the current threat environment. As ransomware campaigns continue to grow in complexity, this report serves as a vital resource for anticipating future threats and strengthening proactive cybersecurity strategies.

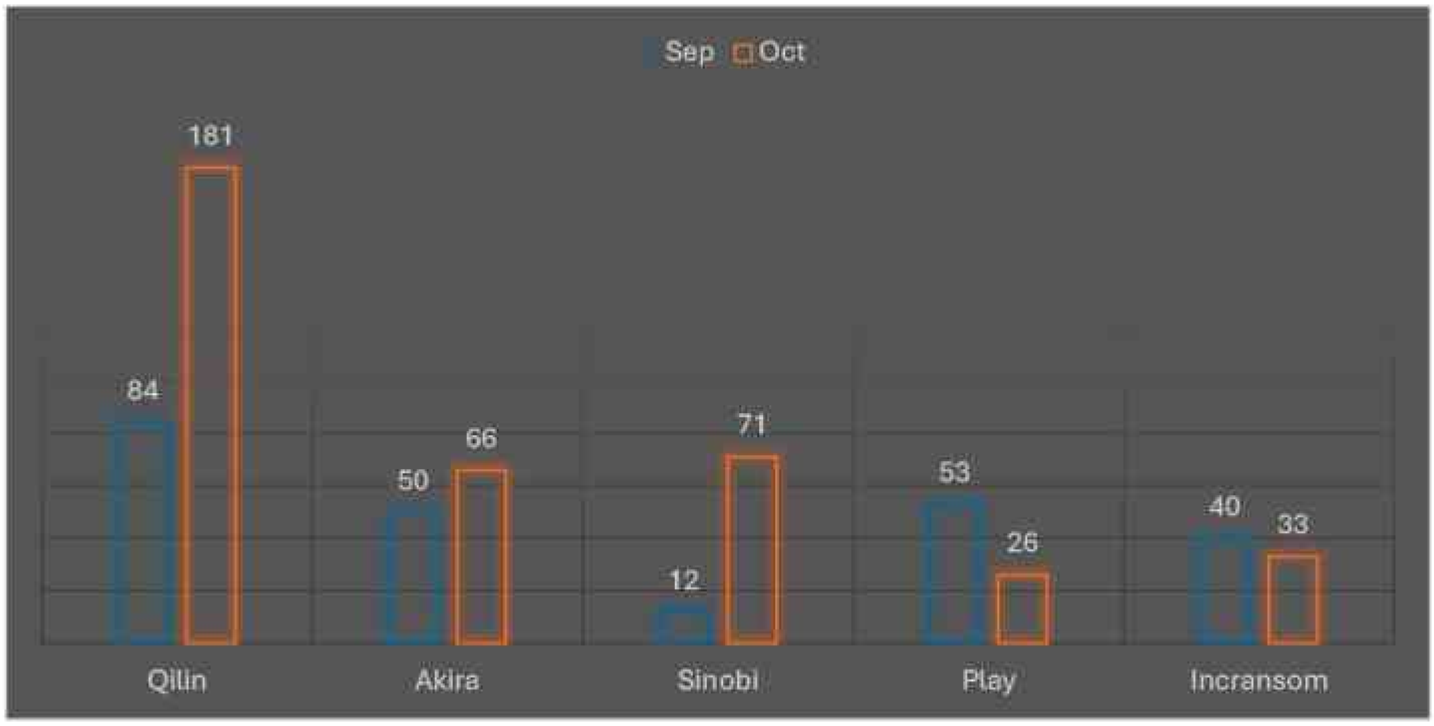
KEY POINTS

- Attackers are weaponizing long-standing kernel bugs (e.g., netfilter flaws) to gain root and deepen persistence across servers and cloud workloads.
- Adversaries run non-native encryptors inside runtime environments (WSL, containers) to evade Windows-centric EDRs and reach hybrid stacks.
- Malvertising and abused code-signing (legitimate certs, mimicked download sites) are used to trick users into installing signed-looking malware.
- Malware is shifting to plug-and-play kits with rentable modules (stealers, RaaS, plugins), lowering the bar for diverse actors to launch attacks.
- Ransomware campaigns now aim to halt production and logistics, converting outages into leverage that inflicts real-world business damage.
- Open-source DFIR/monitoring tools and signed vulnerable drivers are being repurposed as stealthy backdoors and persistence mechanisms.

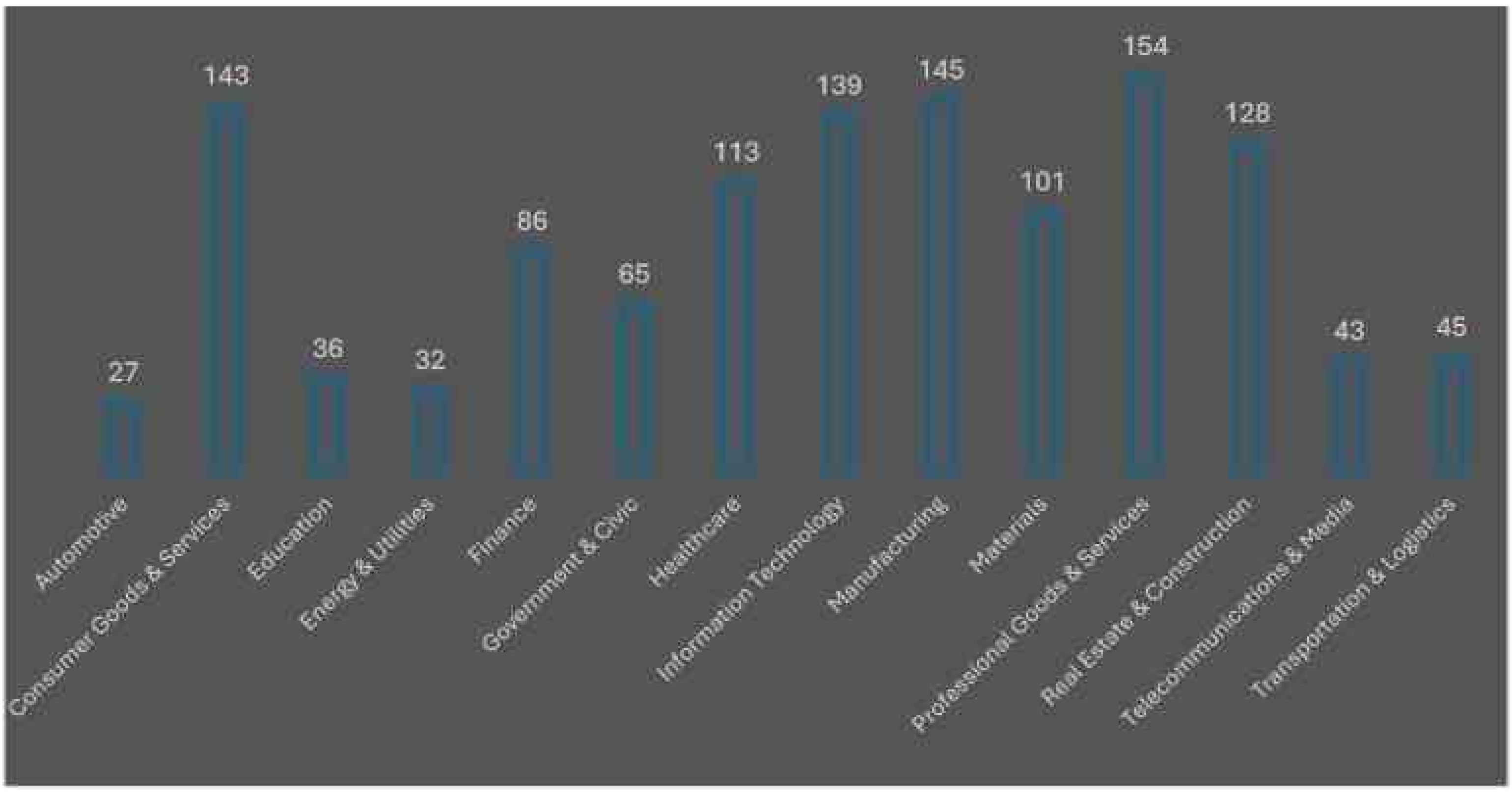
TREND COMPARISON: THE TOP 5 RANSOMWARE GROUPS

Throughout October, there was notable activity from several ransomware groups.

Here are the trends regarding the top 5:



The October comparison reveals major shifts in ransomware group activity. Qilin exhibited explosive growth, more than doubling its victims from 84 to 181, reinforcing its position as a dominant and rapidly expanding threat. Sinobi surged dramatically as well, rising from 12 to 71 incidents, a nearly sixfold increase that marks its emergence as a significant player. Akira showed moderate growth, climbing 32% (50 to 66), suggesting steady operational expansion. In contrast, Play experienced a sharp decline of 51% (53 to 26), indicating reduced campaign activity or strategic regrouping. Incransom also dipped slightly by 17.5% (40 to 33). These fluctuations highlight the evolving dynamics of the ransomware landscape, where new and resurging actors are rapidly gaining ground while others lose momentum.

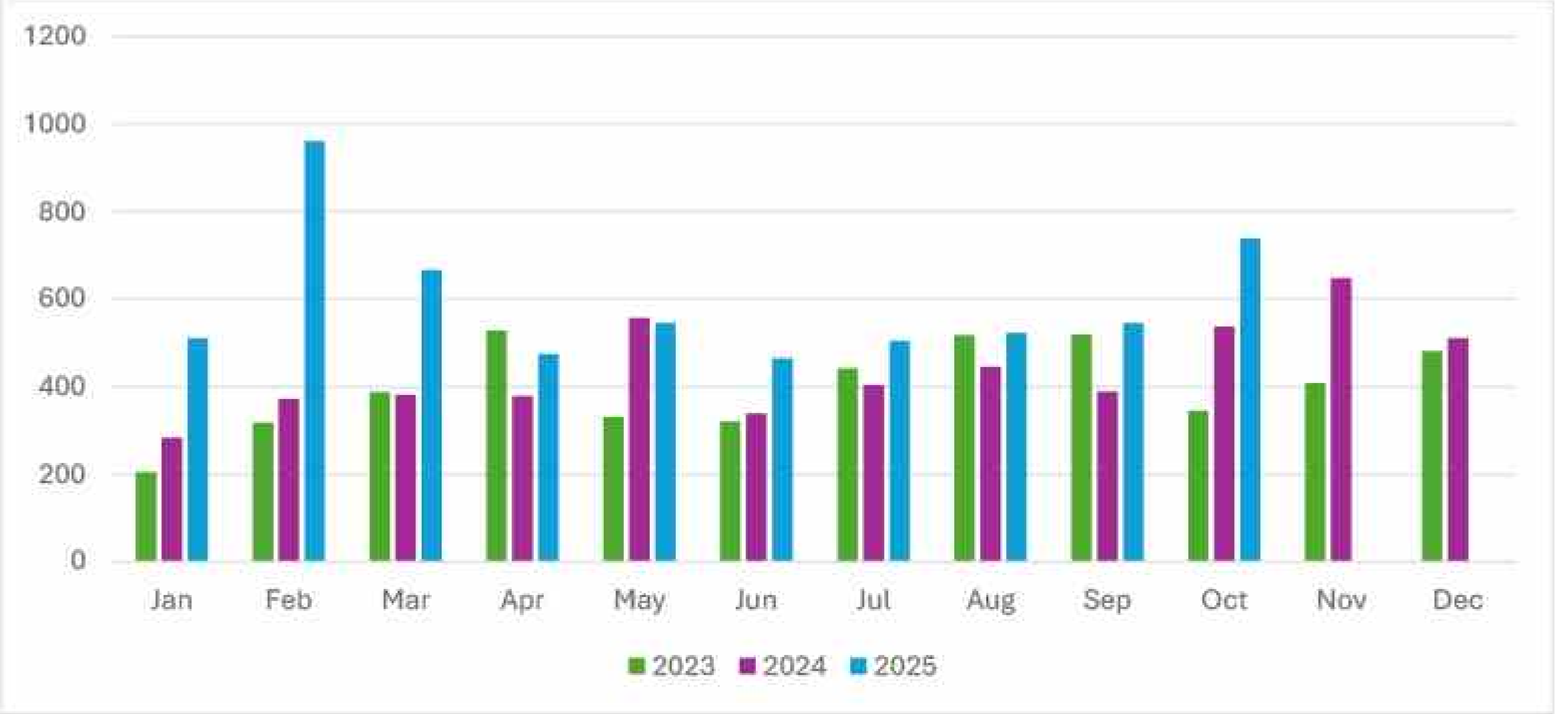


Ransomware operators intensified their focus on high-value and data-rich industries, with the Professional Goods & Services sector suffering the highest number of victims at 154, marking a sharp escalation from prior months. Manufacturing (145) and Information Technology (139) closely followed, underscoring sustained targeting of sectors vital to global supply chains and digital infrastructure. The Consumer Goods & Services (143) and Healthcare (113) sectors also faced heavy pressure, reflecting adversaries' continued exploitation of industries with critical operations and strong ransom payment incentives.

Notably, Materials (101) and Real Estate & Construction (128) recorded substantial victim counts, signaling attackers' growing interest in upstream and infrastructure-linked verticals. Finance (86) and Government & Civic (65) sectors remained consistent targets, highlighting persistent risk to both financial institutions and public entities. Mid-level exposure was observed in Transportation & Logistics (45), Telecommunications & Media (43), Education (36), and Energy & Utilities (32), while the Automotive sector (27) saw a meaningful uptick, suggesting ransomware groups' expanding reach across industrial supply chains.

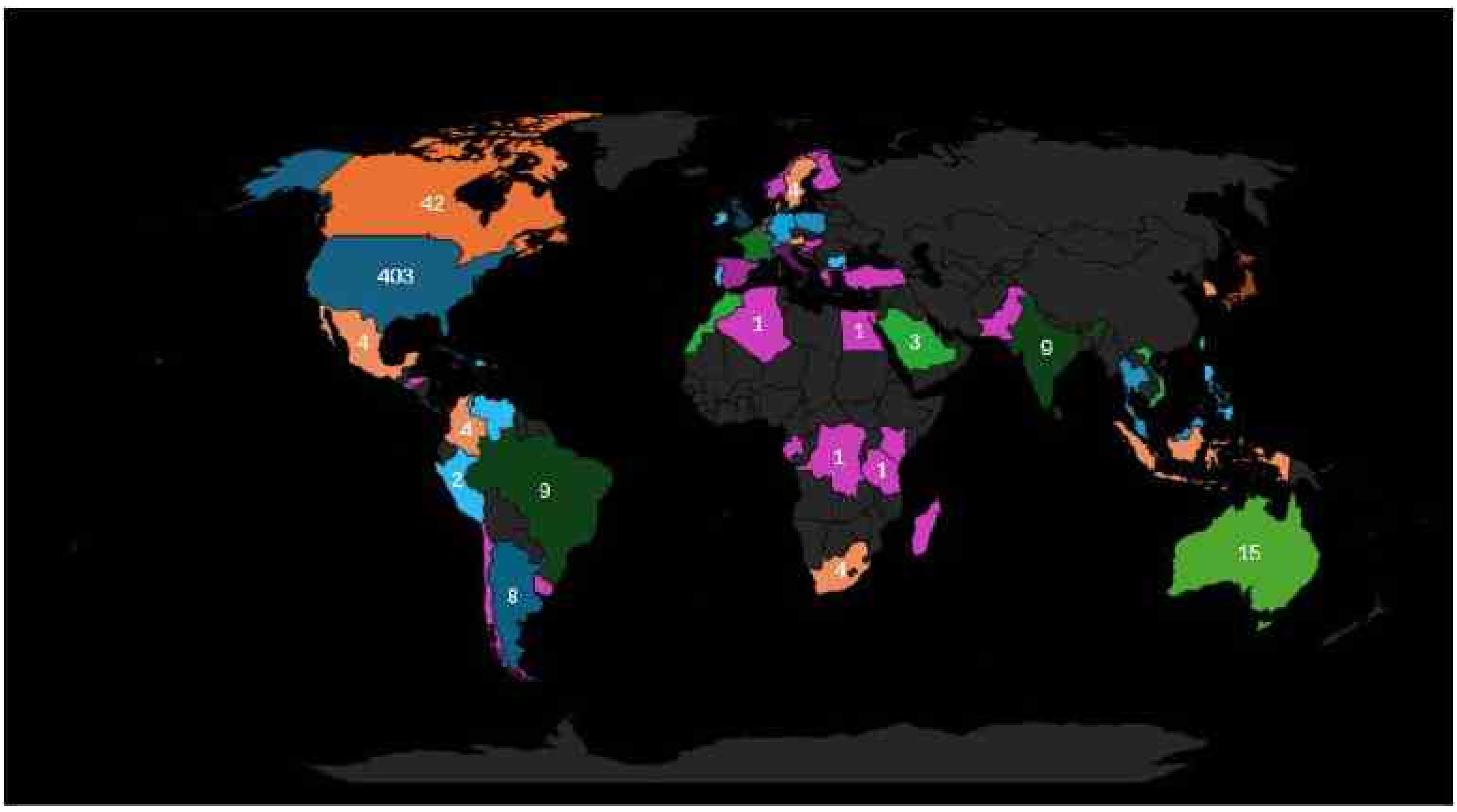
Overall, October's landscape reflects a surge in campaigns against professional services and production-centric industries, revealing a deliberate pivot toward sectors offering high disruption potential and significant ransom leverage.

TRENDS COMPARISON OF RANSOMWARE ATTACKS



Ransomware activity surged sharply in October, marking a major rebound after several months of relative stability. Victim counts jumped to 738, up from 545 in September, signaling renewed momentum across multiple ransomware groups. This spike likely reflects the return of previously dormant affiliates, the launch of new large-scale campaigns, and intensified targeting of high-value sectors, such as professional services, manufacturing, and IT. The October surge follows a mid-year lull driven by affiliate realignments and tactical shifts threats of 2025.

GEOGRAPHICAL TARGETS: TOP COUNTRIES



In October, the United States remained the primary target of ransomware activity, recording 403 victims, a figure far surpassing any other nation and reaffirming its position as the epicenter of global ransomware operations. Canada (42) and France (31) followed at a distance, with Germany (22), Spain (16), Australia (15), and the United Kingdom (13) also sustaining high levels of targeting. Emerging hotspots included Japan, the UAE, India, and Brazil (9 each), reflecting ransomware actors' growing focus on Asia and the Middle East. Meanwhile, Argentina (8), Italy (7), and the Netherlands (6) continued to experience steady exposure, alongside a broader cluster of countries, such as Poland, Hong Kong, Switzerland, Thailand, and Malaysia (5 each) that demonstrate the widening global distribution of attacks. Numerous smaller-scale incidents spanning Europe, Africa, and Latin America further reaffirm the geographically dispersed nature of ransomware operations. Overall, October's data highlights an intensifying global footprint, with adversaries maintaining a stronghold in digitally mature, ransom-prone economies while strategically expanding into diverse emerging markets to maximize reach and impact.

Evolutions in the Ransomware Threat Landscape:

Roots of Control: Ransomware's Descent into the Kernel

The exploitation of CVE-2024-1086 marks a notable evolution in ransomware strategy, shifting from pure software exploitation to weaponizing privilege escalation flaws within core Linux kernel components. By leveraging a year-old netfilter weakness, threat actors demonstrate increasing sophistication in adapting traditional system vulnerabilities into cross-platform ransomware entry points.

ETLM Assessment:

Future ransomware operations may integrate kernel-level privilege escalation exploits into automated intrusion kits, expanding attack surfaces beyond endpoints to servers and cloud-native workloads, enabling deeper persistence and faster privilege dominance.

Bridging Subsystems: Lateral Reach into Hybrid Environments

Qilin's use of WSL to run Linux ELF encryptors on Windows signals a tactical convergence: attackers are exploiting runtime layers and legitimate tooling to bypass Windows-centric EDRs. Combined with Bring Your Own Vulnerable Driver (BYOVD) abuse and remote-management toolchains, this shows a shift toward hybrid, cross-runtime attacks that target both host and virtualized/cloud workloads while blending living-off-the-land techniques with kernel-level tampering.

ETLM Assessment:

Expect operators to weaponize other runtime features (containers, WSL2, Windows features) and automate multi-runtime payload delivery, while increasing kernel/driver abuse for stealth and persistence. Defenders will face more encrypted toolchains that pivot across

Trust as a Vector: The New Face of Ransomware Delivery

Rhysida's campaign through malicious Teams installers reveals a maturing ransomware ecosystem that now blends malvertising, code-signing abuse, and social engineering under trusted brand impersonation. By exploiting legitimate signing authorities and exploiting user trust in Microsoft's software ecosystem, Vanilla Tempest demonstrates how ransomware operations have evolved from brute intrusion to precision deception via supply-chain-like delivery vectors.

ETLM Assessment:

Future operations may pivot toward signed SaaS installers, browser extensions, and productivity integrations as infection vectors, leveraging user familiarity and verified code to bypass endpoint and browser defenses. The growing abuse of trusted signing infrastructure hints at a larger shift toward credibility-based intrusion models.

Turning the Tools of Defense into Weapons of Persistence

The use of Velociraptor, a legitimate DFIR tool, in LockBit and Babuk ransomware operations reflects a strategic inversion of defensive technology into offensive persistence. Threat actors like Storm-2603 are now embedding blue-team tooling into attacks to achieve stealthy remote control, privilege escalation, and recovery-resistant persistence — demonstrating a sophisticated convergence between offensive tradecraft and defensive instrumentation.

ETLM Assessment:

Adversaries may increasingly weaponize open-source security frameworks (e.g., Velociraptor, Osquery, GRR) for covert operations, turning the defender's ecosystem into a post-exploitation toolkit. Expect a future wave of "dual use" tool exploitation, where forensic and monitoring agents become long-term backdoors within enterprise environments.

Bottling Disruption: When Ransomware Targets the Assembly Line

Qilin's breach of Asahi Breweries highlights the industrial pivot of ransomware operations toward high-value manufacturing and supply chain disruption. By directly impacting production across multiple facilities and exfiltrating sensitive corporate data, Qilin demonstrates the maturation of ransomware from data theft to operational sabotage targeting revenue continuity and brand stability as extortion leverage.

ETLM Assessment:

Expect ransomware groups like Qilin to further integrate OT (Operational Technology) targeting and timed disruption strategies to maximize financial and reputational pressure. Future iterations may employ automated shutdown triggers or supply chain manipulation, evolving attacks from IT compromise to full-scale business interruption.

From Access to Extortion: The Modular Evolution of XWorm

The resurfacing of XWorm with over 35 plugins and a built-in ransomware module represents a critical shift from specialized malware to multi-functional attack platforms. Evolving from a simple RAT into a modular ecosystem, XWorm now merges espionage, data theft, and encryption capabilities, signaling the convergence of infostealers, botnets, and ransomware into single, adaptive frameworks controlled by diverse threat actors.

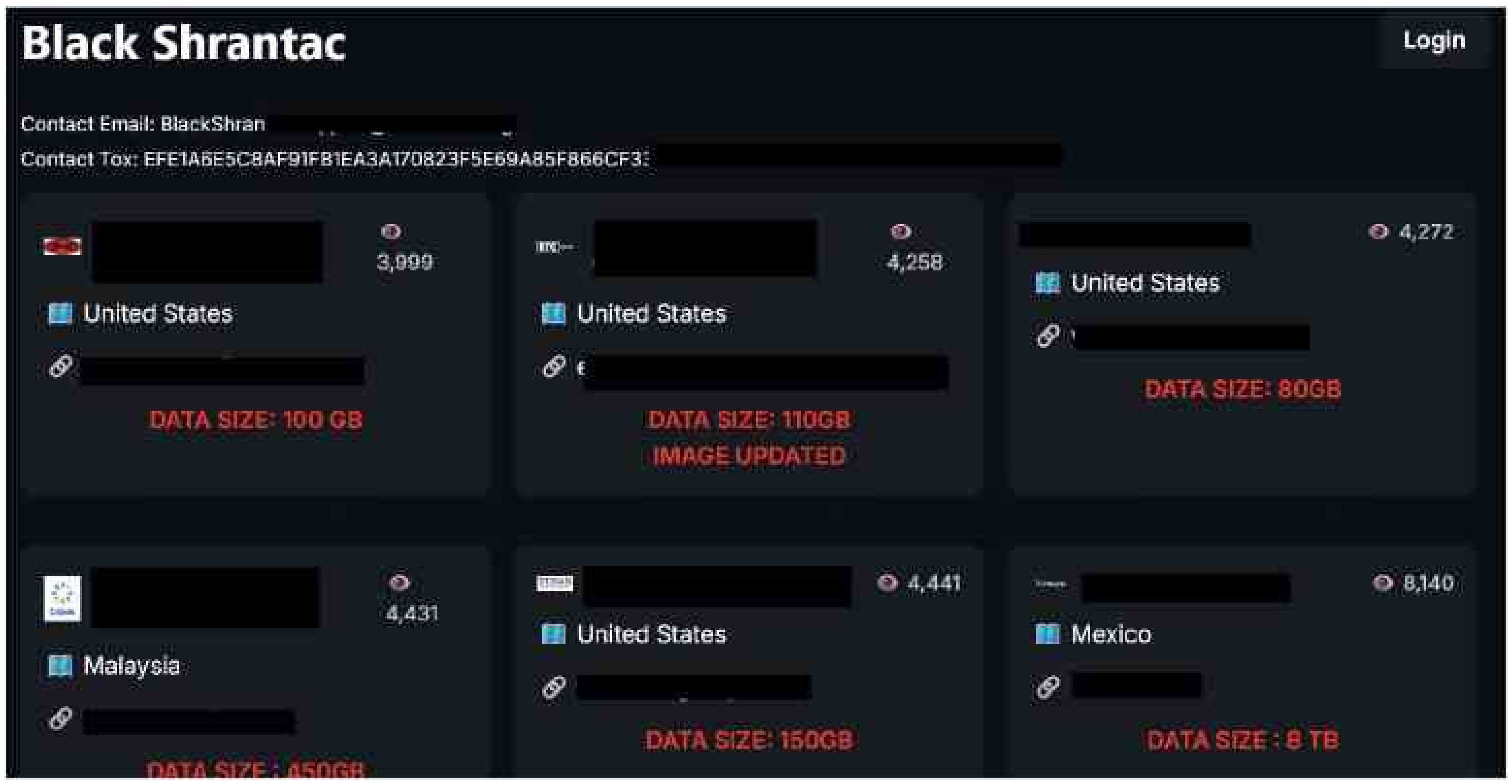
ETLM Assessment:

Future XWorm variants may transition into plug-and-play cybercrime kits, integrating AI-driven payload orchestration and autonomous decision-making for payload deployment. Expect further code reuse across ransomware families and the emergence of marketplace ecosystems where modules are traded or leased to lower-tier actors.

EMERGING GROUPS

Black Shrantac

Black Shrantac is an emerging ransomware group that has continued to gain momentum through 2025, expanding its footprint across multiple sectors. In October, the group claimed 14 victims, up from 8 in September, indicating a steady escalation in activity and growing sophistication and confidence, positioning it as an early-stage but fast-maturing threat actor with the potential to evolve into a more prominent player in the ransomware landscape.



Black Shrantac

Login

Contact Email: BlackShran [redacted]

Contact Tox: EFE1A6E5C8AF91FB1EA3A170823F5E69A85F866CF3 [redacted]

[redacted] 3,999
United States
[redacted]
DATA SIZE: 100 GB

[redacted] 4,258
United States
[redacted]
DATA SIZE: 110GB
IMAGE UPDATED

[redacted] 4,272
United States
[redacted]
DATA SIZE: 80GB

[redacted] 4,431
Malaysia
[redacted]
DATA SIZE : 450GB

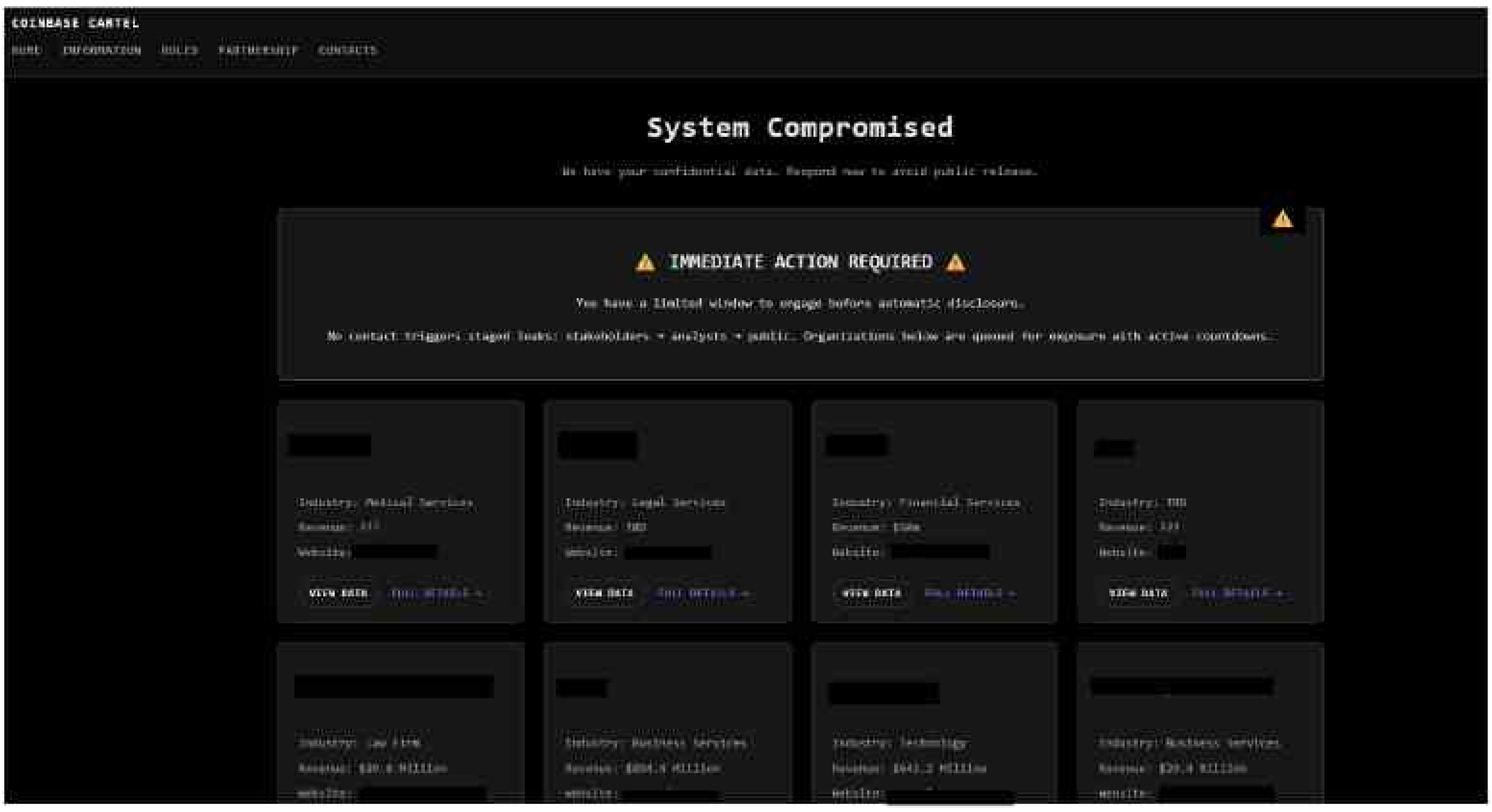
[redacted] 4,441
United States
[redacted]
DATA SIZE: 150GB

[redacted] 8,140
Mexico
[redacted]
DATA SIZE : 8 TB

Source: Underground forum

Coinbase Cartel

Coinbase Cartel is an emerging ransomware and data extortion group that continued to attract attention in 2025 for its methodical and financially driven operations. In October, the group claimed 12 victims, primarily focusing on online platforms and web services. Known for publishing stolen data on its dedicated leak sites, Coinbase Cartel maintains an emphasis on financial and reputational coercion rather than large-scale encryption-based attacks. The slight decline in victim count from September suggests a strategic consolidation phase, as the group refines its targeting and operational methods, reinforcing its position as a structured and evolving threat actor with potential for sustained activity in the coming months.



COINBASE CARTEL

HOME INFORMATION RULES PARTNERSHIP CONTACTS

System Compromised

We have your confidential data. Respond now to avoid public release.

⚠ IMMEDIATE ACTION REQUIRED ⚠

You have a limited window to engage before automatic disclosure.

No contact triggers staged leaks: stakeholders → analysts → public. Organizations below are queued for exposure with active countdowns.

[redacted]
Industry: Medical Services
Revenue: ???
Website: [redacted]
VIEW DATA FULL DETAILS →

[redacted]
Industry: Legal Services
Revenue: TBD
Website: [redacted]
VIEW DATA FULL DETAILS →

[redacted]
Industry: Financial Services
Revenue: $50M
Website: [redacted]
VIEW DATA FULL DETAILS →

[redacted]
Industry: TBD
Revenue: ???
Website: [redacted]
VIEW DATA FULL DETAILS →

[redacted]
Industry: Law Firm
Revenue: $20.0 Million
Website: [redacted]

[redacted]
Industry: Business Services
Revenue: $804.4 Million
Website: [redacted]

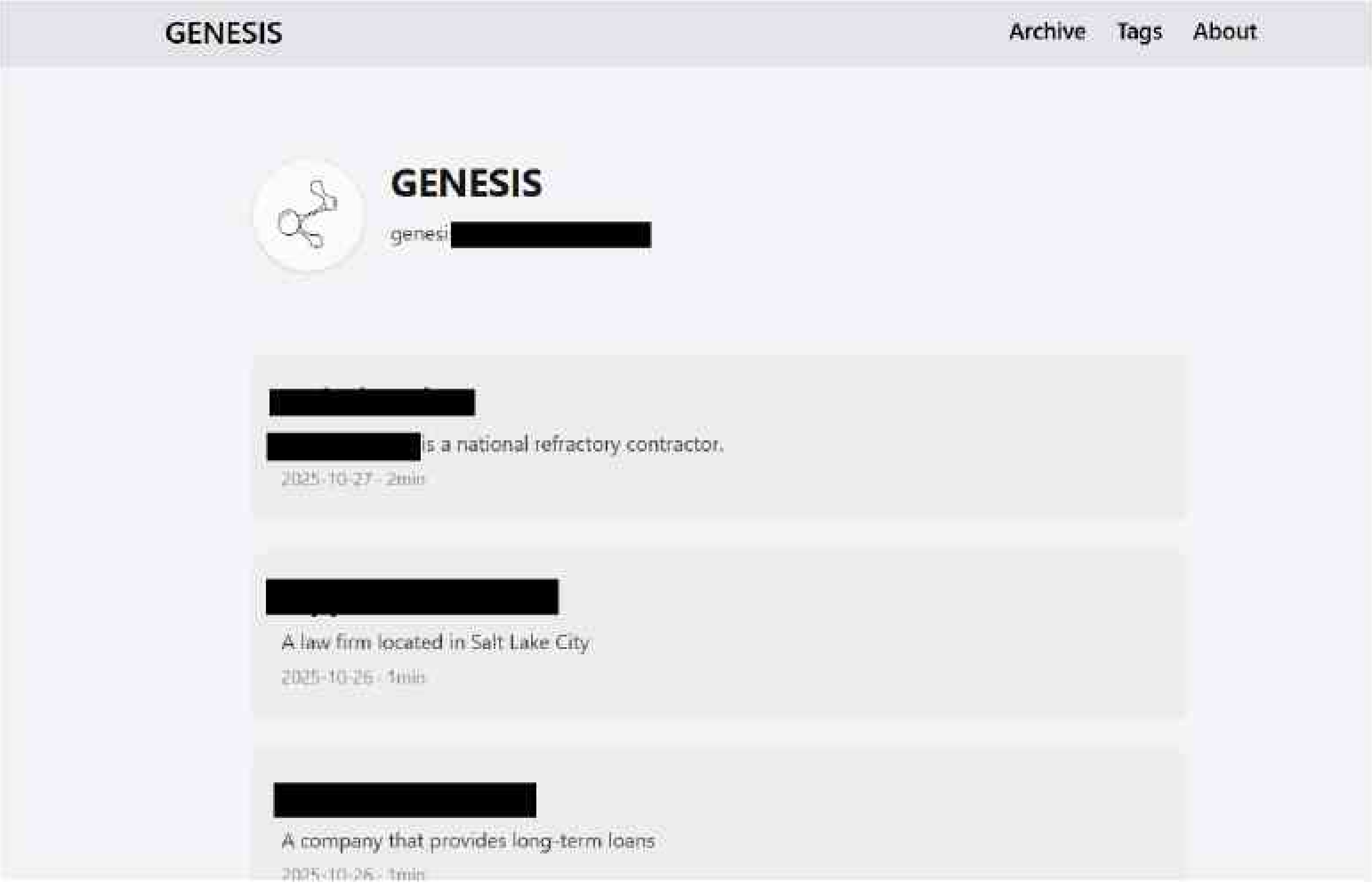
[redacted]
Industry: Technology
Revenue: $641.2 Million
Website: [redacted]

[redacted]
Industry: Business Services
Revenue: $20.4 Million
Website: [redacted]

Source: Underground forum

GENESIS

GENESIS is a newly emerged ransomware and data extortion group that surfaced in October, quickly gaining traction with 12 confirmed victims across sectors such as legal services, healthcare, finance, manufacturing, retail, and professional services. The group primarily focuses on data exfiltration and public leaks rather than encryption, using exposure to exert financial and reputational pressure on its victims. Its early activity demonstrates a strategic targeting approach concentrated on U.S.-based organizations handling sensitive or ecosystem.



GENESIS

genesi[redacted]

[redacted]

[redacted] is a national refractory contractor.

2025-10-27 · 2min

[redacted]

A law firm located in Salt Lake City

2025-10-26 · 1min

[redacted]

A company that provides long-term loans

2025-10-26 · 1min

Source: Underground forum

KEY RANSOMWARE EVENTS IN OCTOBER

When Operations Halt: The Rising Cost of Industrial Extortion

Asahi's confirmation of a ransomware-driven outage demonstrates how targeted attacks on industrial enterprises are escalating from data-centric extortion to production paralysis. The group's quick transition to manual operations reflects both resilience and the growing reality that ransomware campaigns now aim for business process disruption rather than mere encryption, weaponizing downtime as leverage.

ETLM Assessment:

Future ransomware campaigns will likely focus on synchronized disruptions across IT and OT systems, exploiting production scheduling, logistics, and order management dependencies. The next wave of industrial ransomware could incorporate automation-aware payloads capable of halting supply chains at scale to amplify negotiation pressure.

BUSINESS IMPACT ANALYSIS

Based on available public reports, approximately 31% of enterprises are compelled to halt their operations, either temporarily or permanently, in the aftermath of a ransomware onslaught. The ripple effects extend beyond operational disruptions, as detailed by additional metrics:

- A significant 40% of affected organizations are forced into downsizing their workforce due to the financial strain caused by the attack.
- The aftermath sees 35% of businesses experiencing turnover at the executive level, with C-suite members stepping down in the wake of the security breach.
- The financial toll of cyber incidents is staggering, with the average cost burden to companies, irrespective of their size, estimated at around $200,000. This figure underscores the substantial economic impact of cyber threats.
- Alarmingly, 75% of small to medium-sized enterprises (SMEs) face existential threats, admitting the likelihood of closure should cybercriminals extort them for ransom to avoid malware infection.
- The long-term viability of these entities is also in jeopardy, with 60% of small businesses shutting down within six months post-attack, highlighting the enduring impact of such security breaches.

EXTERNAL THREAT LANDSCAPE MANAGEMENT (ETLM) OVERVIEW

Impact Assessment

Ransomware remains a major threat to both organizations and individuals, locking critical data and demanding payment for its release. The consequences extend well beyond the ransom, often leading to costly recovery efforts, extended downtime, reputational harm, and potential regulatory fines. Such disruptions can destabilize operations and erode stakeholder trust. Addressing this growing risk demands a proactive cybersecurity posture and stronger collaboration between public and private sectors to build resilience against future attacks.

Victimology

Cybercriminals are increasingly targeting industries that manage vast amounts of sensitive data, ranging from personal and financial information to proprietary assets. Sectors such as manufacturing, real estate, healthcare, FMCG, e-commerce, finance, and technology remain high on the threat radar due to their complex and extensive digital infrastructures. Adversaries strategically exploit vulnerabilities in economically advanced regions, launching well-planned attacks designed to encrypt critical systems and extract significant ransom payments. These operations are calculated to yield maximum financial returns.

CONCLUSION

The ransomware threat landscape in October revealed a shift toward modular, evasive, and high-impact operations. While overall victim numbers declined slightly, key groups like Qilin demonstrated technical maturity by exploiting zero-day vulnerabilities and introducing legal pressure tactics. Emerging groups such as Fog and Anubis showcased complex toolchains, indicating a strategic pivot to stealth and long-term compromise. Established actors also began leveraging legitimate tools and cloud platforms for persistence and data exfiltration. Organizations must enhance resilience, as ransomware now operates as a service ecosystem, rapidly adapting to security counter measures.

RECOMMENDATIONS

STRATEGIC RECOMMENDATIONS:

Strengthen cybersecurity measures: Invest in robust cybersecurity solutions, including advanced threat detection and prevention tools, to proactively defend against evolving ransomware threats.

Employee training and awareness: Conduct regular cybersecurity training for employees to educate them about phishing, social engineering, and safe online practices to minimize the risk of ransomware infections.

Incident response planning: Develop and regularly update a comprehensive incident response plan to ensure a swift and effective response in case of a ransomware attack, reducing the potential impact and downtime.

MANAGEMENT RECOMMENDATIONS:

Cyber Insurance: Evaluate and consider cyber insurance policies that cover ransomware incidents to mitigate financial losses and protect the organization against potential extortion demands.

Security audits: Conduct periodic security audits and assessments to identify and address potential weaknesses in the organization's infrastructure and processes.

Security governance: Establish a strong security governance framework that ensures accountability and clear responsibilities for cybersecurity across the organization.

may exploit.

Network segmentation: Implement network segmentation to limit the lateral movement of ransomware within the network, isolating critical assets from potential infections.

Multi-Factor authentication (MFA): Enable MFA for all privileged accounts and critical systems to add an extra layer of security against unauthorized access.

Singapore

Hong Leong Building, 16 Raffles Quay, Floor #09-01 & #10-01, Singapore 048581

India

2nd Floor, Workhub by Novel Office, Doddanakundi Industrial Area, Graphite India Main Rd, Whitefield, KEB Colony, Industrial Area, Mahadevapura, Bengaluru, Karnataka 560048

Japan

Otemachi One Tower, 6th Floor, 1-2-1 Otemachi, Chiyoda-ku, Tokyo, 100-0004 Tokyo, Japan

USA

501 Fifth Avenue Suite 805, New York, NY 10017

Germany

Opernplatz 14, 60313 Frankfurt am Main

CYFIRMA
DECODING THREATS

South Korea

10F, 373 Gangnam-daero, Seocho-gu, Seoul, Korea 06621

Australia

Unit 20 270 Blackburn Road, Glen Waverley, VIC, 3150

Taiwan

9F, Second Building, No.96, Sec. 2, Zhongshan N. Rd., Taipei, Taiwan

Vietnam

14th Floor, HM Town building, 412 Nguyen Thi Minh Khai, Ward 5, District 3, Ho Chi Minh City

Dubai

Unit JLT-PH2-RET-5, Cluster R, Jumeirah Lakes Towers, Dubai, UAE

ISO 27001 EU GDPR COMPLIANT AICPA SOC