KELA

State of Cybercrime 2026

Emerging Threats & Predictions

Table of contents

Executive Summary

The zero-trust crisis:

How AI-driven attacks and supply chain exploitation redefined risk in 2025

In 2025, the 'Trust by Default' security model became the ultimate corporate liability. Threat actors have moved past your perimeter and into your identity infrastructure, weaponizing everything from your SaaS integrations to your own AI systems.

> With a **45%** surge in ransomware and a **7,000%** explosion in macOS infections, the 2026 mandate for leadership is clear.
>
> **Secure the Identity, or Lose the Enterprise."**

Davidi Carmiel, CEO, KELA Group

Kela Perspective: The Top Strategic Threats of 2025

Identity is the New Perimeter: The Infostealer Epidemic

Traditional defenses are failing because attackers aren't breaking in, they're logging in.

The Scale	KELA tracked **2.86 billion** compromised credentials this year alone.
The Mac Myth	macOS is no longer a safe haven; infections skyrocketed from under 1,000 to **over 70,000** as 'Atomic Stealer' (AMOS) professionalized Mac-targeted attacks.
The Risk	Business Cloud and Authentication services account for **over 30%** of all targeted data, making every employee a potential gateway for total network compromise.

Industrial-Scale Extortion: The Ransomware Surge

Ransomware has evolved into a high-velocity business model, prioritizing US manufacturing and professional services.

The Stats	**7,549 victims** were claimed in 2025—a massive **45% increase** from 2024.
US Victim Bias	**Over 53%** of all global ransomware victims were **US-based** organizations.
The Damage	The Jaguar Land Rover (JLR) breach alone cost the automotive economy **$2.5 billion**, proving that a single vendor compromise can trigger a national GDP contraction.

‘Vibe Hacking’ & The Autonomous Threat: The Malicious AI Frontier

Attackers have moved from using AI as a tool to making it a core part of the attack kill chain.

Vibe Hacking	Adversaries are now **contextually manipulating your AI’s** autonomous logic to bypass safety protocols without triggering technical alarms.
Agentic Attacks	State-sponsored actors (specifically from China) are now using autonomous AI agents to run **80-90%** of a campaign with minimal human oversight.
Velocity	AI-driven malware is shrinking the window between initial access and total exfiltration from **days to minutes.**

The Fragile Ecosystem: Supply Chain & Nth-Party Sabotage

The primary target is no longer your network; it is the trusted service provider you already pay for.

The Shift	Attackers have moved to "Upstream Exploitation," where a single vulnerability in a shared SaaS platform—like the recent Salesforce Aura data theft—provides a skeleton key to thousands of downstream corporate environments.
The Case Study	Groups like ShinyHunters are now weaponizing misconfigurations in Experience Cloud instances to exfiltrate sensitive data from thousands of organizations globally by targeting the provider's shared infrastructure.
The Risk	Even with robust internal security, a vulnerability in your Nth-party supply chain creates a systemic failure of the digital trust model, turning your most essential business tools into a direct gateway for total data compromise.

2026 Predictions:
The Road Ahead for Executives

The Rise of the Agentic Insider:

2026 will see the first major public breach caused not by a human, but by an autonomous AI Agent. As companies rush to deploy Agentic AI for productivity, these systems will become Non-Human Identities with over-privileged access. Attackers will use Prompt Injection to hijack these agents, turning your own automation into an insider threat that can drain accounts or leak data without a single human click.

Vibe Coding & Shadow AI:

The democratization of software creation through so called 'vibe coding' (natural language programming) will lead to a wave of unmanaged, unvetted Shadow AI applications. These vibe-coded modules will enter production with inadvertent vulnerabilities, creating a massive, invisible attack surface for 2026.

AI-Enhanced Social Engineering (The End of Tells):

The traditional red flags of phishing - bad grammar, strange URLs - are dead. In 2026, AI-driven voice cloning and hyper-realistic video deepfakes will become the standard for Business Email Compromise (BEC). Attackers will impersonate your CFO or CEO in real-time video calls to bypass MFA and authorize fraudulent wire transfers.

Zero-Day Industrialization:

Ransomware giants like Clop and Qilin will use AI to automate the discovery and exploitation of zero-day vulnerabilities in enterprise SaaS. The window to patch is closing; in 2026, the time from vulnerability disclosure to mass exploitation will be measured in minutes, not days.

The Institutionalization of Hacktivism:

2026 will mark the end of "nuisance" hacktivism as ideological groups move beyond simple website defacements toward the targeted disruption of Operational Technology (OT) and Industrial Control Systems (ICS). This "Deniable Proxy" model allows sophisticated actors to sabotage power grids, water treatment, and manufacturing plants while maintaining plausible deniability. For executives, this means disaster recovery must now account for "Total Data Loss" scenarios where decryption is never an option and the goal is physical-world consequence.

Executive Action Plan

Kill the Static Password:

Mandate phishing-resistant (FIDO2) hardware keys. Standard MFA is no longer enough to stop modern session-hijacking

Audit the Web of Trust:

Immediately review all third-party SaaS and OAuth integrations. Block overly permissive scopes like Modify All Data.

Hardening AI Assets:

Treat your AI tools and APIs as high-value infrastructure. Isolate sensitive data from AI-connected environments to prevent indirect prompt injection.

2025 Threat Landscape Summary

In 2025, the cyber threat landscape was defined by the weaponization of trust and the deep integration of artificial intelligence (AI) across the attack kill chain. Cyber operations became an undeniable core instrument of national power amid escalating geopolitical conflicts, further blurring the lines between state-sponsored actors, cybercriminals, and hacktivists. The Malware-as-a-Service (MaaS) and Ransomware-as-a-Service (RaaS) ecosystems continued to mature, driving massive increases in attack volumes and enabling rapid monetization. Furthermore, threat actors shifted away from relying solely on technical exploitation, increasingly compromising identity infrastructure, SaaS integrations, and the autonomous logic of AI systems themselves to bypass traditional security perimeters.

In this report, KELA highlights notable threats of 2025, alongside predictions and countermeasures for the evolving threat landscape of 2026.

The Identity Drain: Infostealers as the Primary Access Vector

- Infostealers remain a central cybercrime gateway, fueling account takeovers, ransomware, and espionage.
- KELA observed ~3.9 million unique infected machines globally, yielding 347.5 million compromised credentials. Overall, KELA tracked 2.86 billion compromised credentials across the broader cybercrime ecosystem.
- Lumma dominated malware infections (over 55%), followed by Redline and Vidar.
- Targeting of Apple environments surged dramatically, with macOS infections jumping from under 1,000 in 2024 to over 70,000 in 2025, driven by MaaS offerings like Atomic Stealer (AMOS).

High Velocity Extortion: The Surge in Victim Volume

- Ransomware and extortion accelerated sharply, tracking 7,549 victims - a 45% increase from 2024.
- Attacks were claimed by 147 active groups (including ~80 new entities), highlighting a highly volatile landscape. Qilin was the most prolific actor (1,130+ victims), followed by Akira and Clop, while LockBit dropped out of the top 10.
- The U.S. was the primary target (over 53% of victims); Manufacturing and Professional Services saw the most attacks.
- High-impact economic disruptions were common, causing massive operational halts at major enterprises like Jaguar Land Rover, Asahi Group, and Ingram Micro.

Exploit Industrialization: The Collapse of the Defensive Window

- Real-world exploitation surged, with 238 vulnerabilities added to CISA's KEV Catalog in 2025 (up from 185 in 2024).
- Underground markets professionalized, heavily favoring fully weaponized mass-exploitation scripts and exclusive exploits over basic PoC code.
- Attackers targeted widely deployed internet-facing technologies, primarily affecting WordPress, Chrome, Next.js, React, and Palo Alto Networks.
- Microsoft remained the most exploited ecosystem, driven by sustained focus on remote code execution and authentication bypasses for rapid initial access.

Digital Sabotage: The Weaponization of Geopolitical Sentiment

- Hacktivism solidified as a persistent hybrid threat. KELA tracked 250+ new groups claiming ~3,500 DDoS attacks - a 400% year-over-year increase.
- Operations evolved from symbolic disruptions to targeted probing of Operational Technology (OT) and critical infrastructure.
- Major geopolitical flashpoints, including the Israel-Iran escalation and the NATO Summit, triggered rapid, synchronized hacktivist campaigns.

The Deniable Proxy Ecosystem: Nation-State Convergence in 2025

- State-backed campaigns acted as core national power instruments in major geopolitical conflicts (e.g., Russia-Ukraine, Israel-Iran, U.S.-China).
- North Korean actors (e.g., Lazarus) aggressively targeted Web3 and developer ecosystems via social engineering to fund strategic programs.
- China's opaque cyber-industrial base faced unprecedented exposure via dark web leaks detailing state cooperation at major cybersecurity firms like VenusTech.

Continued Erosion of the Perimeter: 2025's 3rd Party Access Exploitation

- Attackers weaponized the 'Trust by Default' model, turning third-party SaaS integrations and automated pipelines into primary mass-compromise vectors.
- SaaS-to-SaaS (OAuth) compromises rose, enabling attackers to bypass MFA by pivoting through trusted vendors.
- Mass-exploitation of zero-day vulnerabilities in enterprise applications remained lucrative, notably Clop's rapid Oracle E-Business Suite extortion campaign.
- Threat actors deployed self-propagating threats in developer ecosystems, such as the S1ngularityNX worm infecting downstream CI/CD pipelines.

Escalation and Integration: AI Across the Attack Kill Chain

- LLM exploitation evolved from basic jailbreaking to 'vibe hacking' - contextually manipulating autonomous AI systems to execute malicious workflows.
- AI-assisted malware became a reality; strains like PromptFlux and Voidlink utilized LLMs for dynamic obfuscation and command generation.
- Attacks targeting AI companies surged, demonstrating how prompt injection and 'Inter-Agent Trust Exploitation' turn AI tools into involuntary participants in data exfiltration.

The Invisible Epidemic: Infostealers and the Billion-Credential[1] Threat

Infostealer malware continues to be one of the most pervasive and high-impact threats in the cybercrime ecosystem. These malicious programs are designed to exfiltrate sensitive data from compromised machines, including login credentials, authentication tokens, and other critical account information. Once harvested, these credentials provide threat actors with direct access to user accounts including services of corporate systems, and cloud environments, enabling account takeovers, lateral movement, and further exploitation.

The growth of Malware-as-a-Service (MaaS) and Infostealer-as-a-Service models has dramatically lowered the barrier to entry for cybercriminals. By offering ready-to-use malware, infection kits, and management panels via subscription, these platforms allow even low-skilled actors to conduct large-scale credential theft campaigns, expanding the overall pool of active threat actors in the ecosystem.

In 2025, KELA observed approximately 3.9 million unique machines infected with infostealer malware globally, which collectively yielded 347.5 million compromised credentials. Beyond malware-originating data, KELA tracked a total of 2.86 billion compromised credentials across multiple sources, including ULP lists, breached email repositories, and automatically extracted credentials from cybercrime marketplaces. These figures highlight the sheer scale and persistence of the threat, which continues to grow.

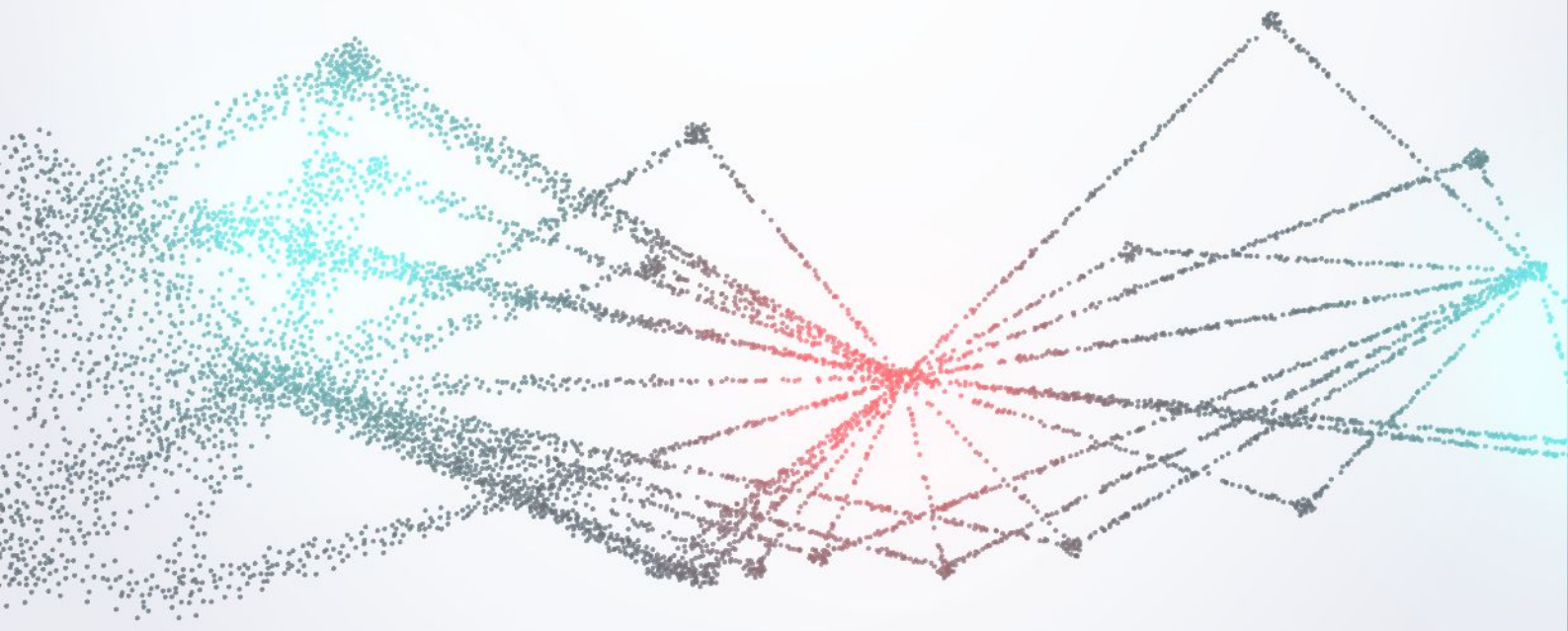
[1] In this report, 'compromised credentials' refers to authentication material (usernames, passwords, session tokens, cookies, etc.) collected from malware, breach data, or marketplace sources. These credentials may or may not be valid for successful login; the figures presented reflect exposure rather than confirmed access.

Compromised credentials are highly commoditized and monetized within the cybercrime ecosystem. They are sold individually by Initial Access Brokers (IABs) or distributed in bulk to buyers ranging from independent operators to organized ransomware groups and APT actors. These credentials are often used to gain initial access to corporate networks, launch supply chain attacks, or facilitate further intrusion campaigns, making them a cornerstone of modern cybercrime operations.

Given the volume, persistence, and monetization potential of compromised credentials, the detection, monitoring, and analysis of these threats are critical for organizations. Understanding both the scale of exposure and the types of services targeted enables proactive defensive measures, early mitigation, and informed risk management. In short, infostealer malware represents a growing, persistent, and highly profitable threat that remains a central concern for cybersecurity teams worldwide.

This chapter is structured into three main sections. The first section presents KELA's insights regarding infostealer malware–infected machines, including the top affected countries and infection trends throughout 2025, both in monthly breakdowns and overall activity. The second section expands the focus to the entire KELA data lake of compromised credentials, covering credentials originating from infostealer malware as well as additional sources across the cybercrime ecosystem, providing a comprehensive view of the scope, distribution, and monetization of compromised credentials in 2025.

The third section examines macOS-focused infostealer infections, a research area KELA prioritized in 2025 in response to the growing number of infostealer variants targeting macOS environments. This section analyzes emerging trends, attacker adaptation, and the expanding macOS threat surface, alongside KELA's assessment that this trajectory is likely to continue in the coming year.



Millions Infected: Infostealers by the Numbers

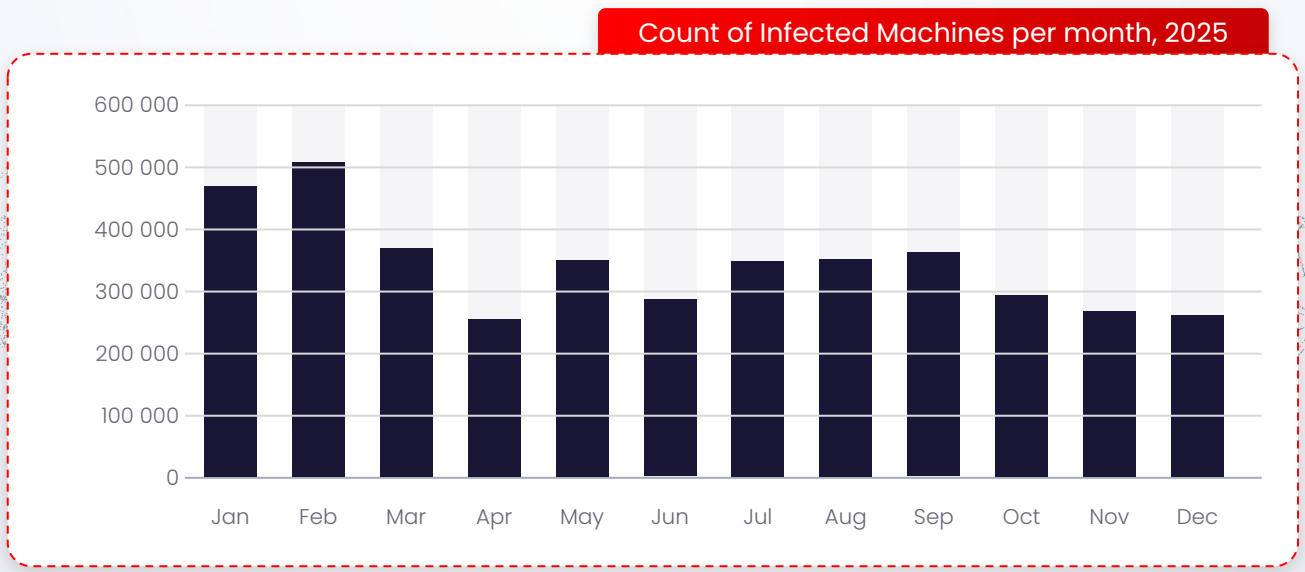
According to KELA's data lake, approximately **3,920,240** unique machines infected with infostealer malware were observed globally between January 1 and December 31, 2025. It is worth noting that this figure reflects **unique infected machines,** meaning that multiple infections on the same host are de-duplicated and counted only once.

2025 Infostealer Impact: Machines Infected and Credentials Compromised

Compromised credentials originating from infostealers represent user credentials - logins and passwords - harvested from infected machines, often encompassing multiple online services per device. Out of the observed 3.9 million infected machines in 2025, KELA identified 347.5 million compromised credentials, illustrating that a single infected machine can contain hundreds of credentials. For comparison, in 2024 KELA recorded 4.2 million infected machines and 331.4 million compromised credentials. While the number of infected hosts declined slightly in 2025, the increase in stolen credentials points to a more impactful infostealer threat, driven by higher-value infections and denser credential harvesting.

Infostealer Infections Breakdown By Month 2025[2]

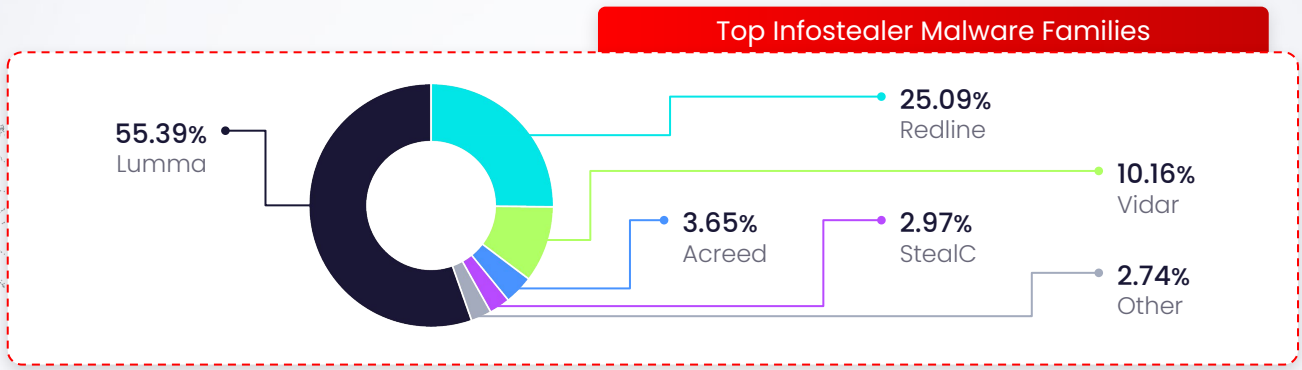
According to KELA's data lake, approximately 3.9 million unique machines were infected with infostealer malware between January and December 2025. Infection activity remained high throughout the year, peaking in the first quarter - particularly in February (12.9%), followed by January (11.9%) and March (9.4%). While the monthly breakdown shows fluctuations in infection activity, the overall perspective demonstrates a persistently high and growing infostealer threat. These numbers underscore that the infostealer threat remains significant, persistent, and a major concern for organizations worldwide.



[2] While a decrease can be seen in the graph during the last few months of the year, the real infection rate is likely not significantly lower. Since the graph uses machines' infection dates, more bots infected late in 2025 may be collected early in 2026.

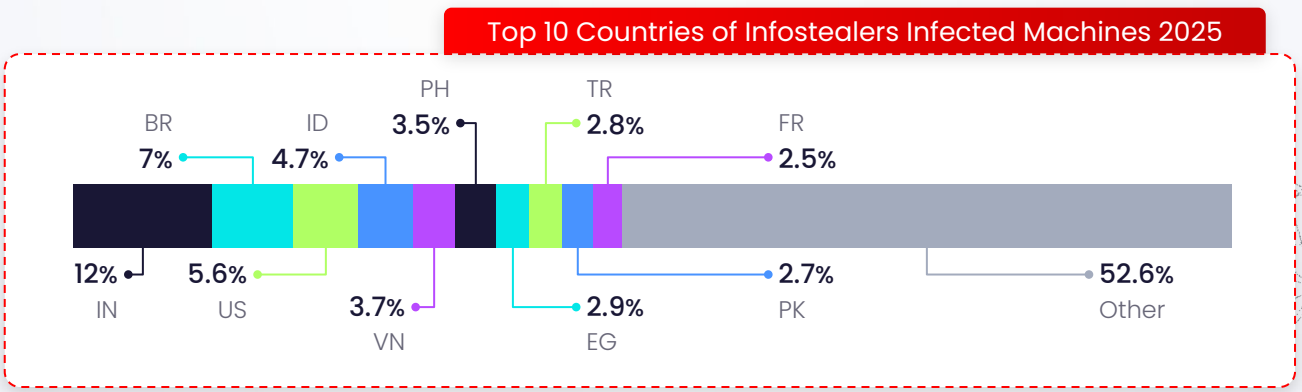
Pareto Power: Top Malware Families Leading the Infostealer Ecosystem

In 2025, analysis of 3.9 million infected machines shows that a handful of infostealer families dominate the ecosystem. Lumma accounted for 55% of infections, followed by Redline (25%), Vidar (10%), Acreed (3.6%), and StealC (3%), together representing over 97% of all observed cases. This concentration highlights that large-scale credential harvesting is driven by a few highly prevalent families, making them priority targets for monitoring and disruption.



Infostealer Hotspots: Top Affected Countries

In 2025, analysis of 3.9 million infected machines revealed that infostealer infections were globally distributed. India accounted for the largest share (11.9%), followed by Brazil (6.9%), the United States (5.5%), Indonesia (4.7%), Vietnam (3.6%), and the Philippines (3.5%). Egypt, Turkey, Pakistan, and France each contributed 2.5–2.8%, with the remaining countries making up roughly 52% of infections, highlighting the broad international reach of these threats.



This top-country distribution likely reflects a combination of factors, including large online populations, widespread use of devices and operating systems vulnerable to malware, variable levels of cybersecurity awareness, targeted campaigns by threat actors, and, in some regions, the higher prevalence of unlicensed or unofficial software. Such environments often lack regular security updates and may rely on cracks or keygens[3], which significantly increases the risk of infostealer infections. Collectively, these conditions make certain countries more susceptible to large-scale credential harvesting.

[3] A keygen is a small program designed to generate fake or unauthorized license keys for paid software. People use them to activate software without purchasing a legitimate license.

2.86 Billion: Mapping the 2025 Compromised Credentials Epidemic

This chapter examines the **full scope of compromised credentials** collected from multiple sources in 2025, which among others including infostealer malware logs, ULP Lists[4], breached email repositories, and automatically extracted credentials from cybercrime marketplaces. Monitoring and analyzing these credentials is critical for threat intelligence and defense, as each valid compromised credential represents a potential gateway for account takeover, lateral movement, and highly targeted attacks. In total, KELA observed 2,863,597,452 compromised credentials throughout the year, highlighting the massive scale of credential exposure.

These compromised credentials are highly valued[5] in the cybercrime ecosystem and are commoditized and monetized through multiple business models, including individual sales by Initial Access Brokers (IABs) or bulk distribution to threat actors. Buyers range from independent operators to organized groups, including ransomware gangs and APT actors, who leverage these credentials to gain initial access to victim environments. Once obtained, compromised credentials are further exploited for follow-on attacks, making the monitoring of these aggregated sources essential for identifying evolving threats that would remain invisible in isolated datasets. Additionally, having a clear perspective on exposure levels is crucial for organizations to respond proactively and in real time.

Monthly Trends in Global Credential Theft, 2025

The graph below illustrates the distribution of **2.86 billion compromised credentials** observed by KELA throughout 2025[6], showing trends and fluctuations in credential exposure by month.

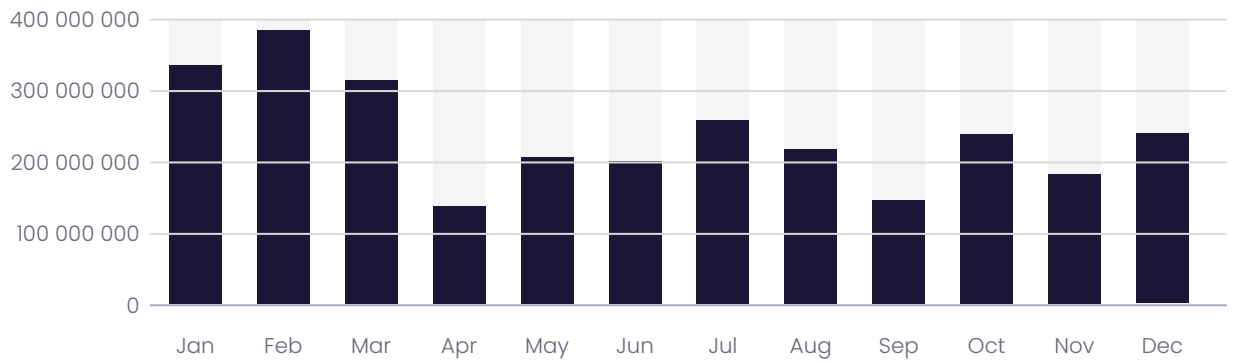
Credential harvesting peaked in the first quarter, with monthly volumes exceeding 385 million, and although activity fluctuated throughout the year, it remained consistently high. Even during periods of relative decline, large-scale credential theft persisted, highlighting the enduring and pervasive nature of the infostealer threat. Overall, the data illustrates a dynamic and sustained credential-harvesting ecosystem that continues to pose significant risks to organizations worldwide.

[4] ULP Lists are compiled collections of compromised credentials, typically aggregated from multiple sources such as infostealer malware logs, previous breaches, phishing campaigns, and dark web marketplaces. These lists often contain millions of Url(service)|usernam|password pairs and are sold or distributed to cybercriminals for account takeover, spam campaigns, credential stuffing, and other malicious operations. ULPs are considered highly valuable in the cybercrime ecosystem because they consolidate previously scattered data into a single, ready-to-use resource.

[5] KELA's **Inside the Infostealer Epidemic: Exposing the Risks to Corporate Security** (April 2025, Report Inside the Infostealer Epidemic: Exposing the Risks to Corporate Security Report • KELA Cyber Threat Intelligence), provides a detailed analysis of infostealer malware evolution and the monetization of compromised credentials, showing how threat actors leverage these credentials through sophisticated cybercrime business models.

[6] The total number of 2.86 billion compromised credentials are calculated from all types of sources including only compromised Email credentials.

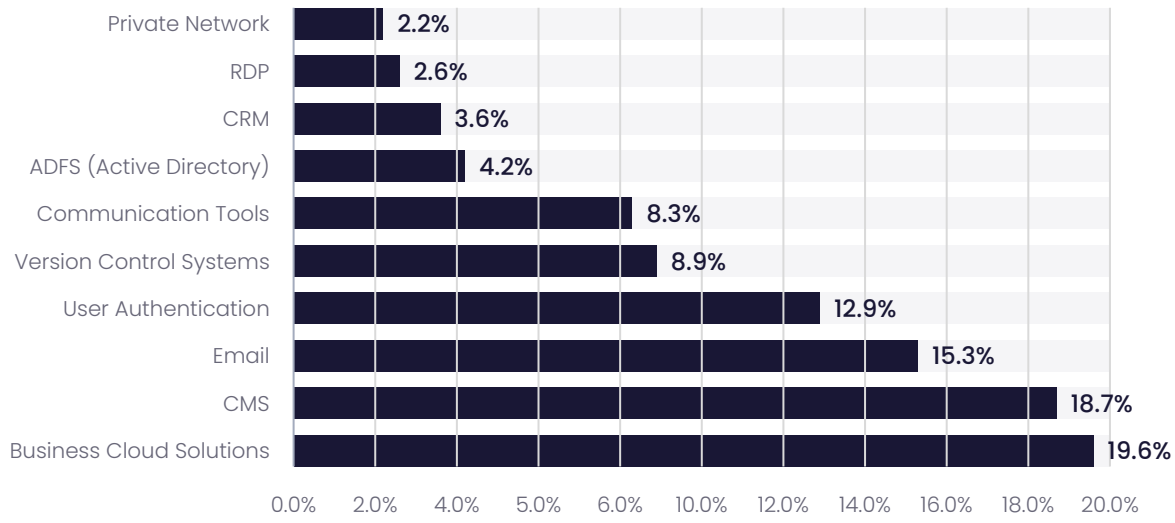
Count of Compromised Credentials by month, 2025



High-Stakes Credential Theft: Top Compromised Services, 2025

Analysis of KELA's 2025 compromised credentials data lake shows that Business Cloud Solutions (19.6%), CMS platforms (18.7%), Email services (15.3%), User Authentication services (12.9%), and Version Control Systems (8.9%) constitute the top five service categories. Together, they account for over 75% of compromised credentials, highlighting threat actors' focus on services that offer broad access and high-value data. These platforms are particularly sensitive for corporates: Business Cloud Solutions centralize critical documents and operational data; CMS platforms control public-facing content and often store user information; Email services grant access to internal communications and account recovery channels; User Authentication systems manage access across multiple applications; and Version Control Systems hold proprietary source code and intellectual property. Compromising these services can enable attackers to move laterally within organizations, exfiltrate sensitive information, or conduct large-scale fraud, making them prime targets for infostealer operations.

Top 10 Compromised Credentials to Sensitive Services 2025



From Clicks to Credentials: Infostealer Methods in 2025

The 2025 threat landscape shows infostealers increasingly relying on social engineering, supply chain attacks, and malicious software distribution to compromise victims, reflecting a more industrialized approach. The most common TTPs include:

- **Omnichannel Phishing & AI Lures:** Attackers use email, messaging apps, and AI-generated personalized scams, often bypassing MFA via Phishing-as-a-Service.
- **'Scam-Yourself' Attacks (ClickFix/FakeCaptcha):** Users are tricked into manually executing scripts, evading traditional security tools.
- **Malvertising & SEO Poisoning:** Malicious ads and search results push trojanized software, boosting infection rates.
- **Supply Chain & Developer Targeting:** Poisoned packages and DevTools impersonation target high-privilege credentials.
- **Malicious Browser Extensions:** Compromised updates enable form-grabbing and cookie theft.
- **Trojanized Software & Fake Updates:** Pirated apps and fake updates remain effective, especially against SMBs and BYOD users.

MacOS Infostealers Explode: Four Years of Growth Culminate in 2025[7]

macOS infostealers have rapidly emerged as a growing and profitable threat, challenging the long-held perception that Apple devices are largely immune to malware. Once considered secure due to built-in protections, macOS endpoints are increasingly targeted by cybercriminals seeking browser credentials, cloud service tokens, cryptocurrency wallets, and other sensitive data. These credentials are highly monetizable, either through direct exploitation or resale on underground markets, and have become a key component of modern cybercrime.

KELA's analysis shows that demand and supply for macOS infostealers have grown steadily over the past years. The rise of Malware-as-a-Service has professionalized this threat, offering subscription-based malware, updates, and support that lower the barrier to entry, enabling even inexperienced actors to target macOS systems at scale. As Apple adoption grows across high-value consumers and corporate environments, the incentive for attackers continues to expand, with compromised devices providing access to SaaS credentials, VPNs, developer tools, and other corporate assets.

The history of macOS malware illustrates the evolution of this threat. Early proof-of-concept malware, such as Renepo in 2004, gradually gave way to functional infostealers like DevilRobber in 2011, capable of exfiltrating credentials while performing additional tasks such as cryptomining. The first commercial MaaS macOS infostealer, Atomic Stealer (AMOS) in 2023, marked the start of systematic credential theft as a monetized business. Today, macOS infostealers are increasingly professionalized, widely distributed, and monetized, with pricing often higher than Windows equivalents due to their scarcity and the lucrative opportunities they provide.

KELA's findings indicate that while Windows remains the dominant target for infostealers, macOS is no longer a niche platform. The increasing number of malware families, professionalization of the tools, and variety of distribution methods show a clear upward trajectory in both demand and supply. Organizations can no longer treat macOS devices as inherently secure; monitoring, endpoint protection, and employee awareness for macOS must now match that of Windows to mitigate this growing threat.

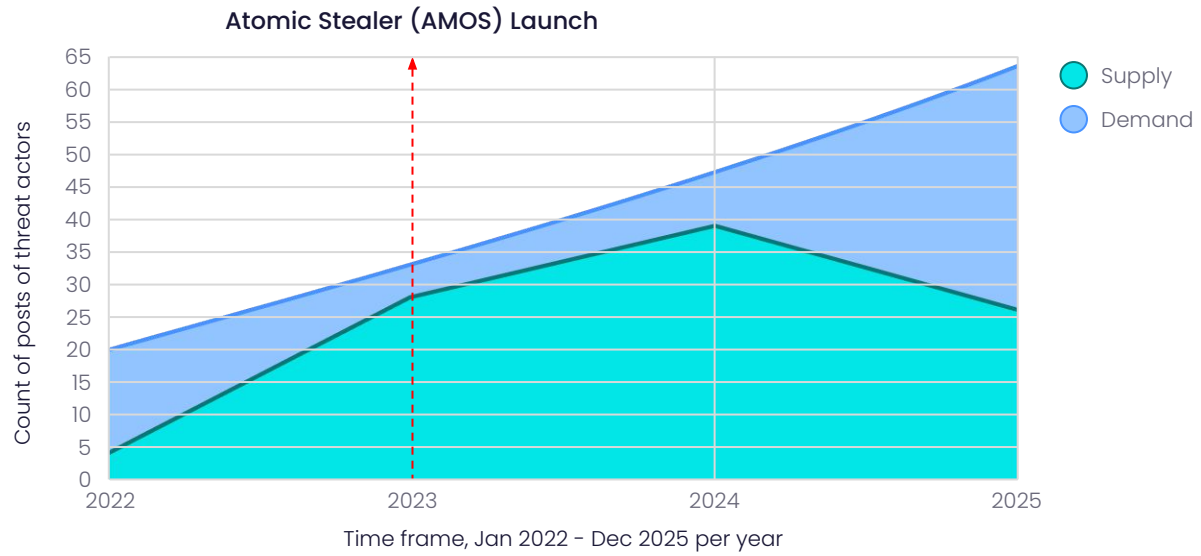
Evolving Demand and Supply for macOS Infostealers

KELA analyzed its database of threat actors' chatter on dark web forums, marketplaces, and Telegram channels - from January 2022 to December 2025 - to track trends in discussions related to macOS-targeting infostealers. Two specific queries were used: one, using keywords indicative of interest in purchasing, to identify threat actors searching for macOS-targeting infostealers (demand); and another, using keywords indicative of product listings, to detect threat actors offering or promoting such tools (supply).

[7] Based on KELA's October 2025 report, 'The Rise of macOS Infostealers: 2025 in Review', macOS infostealers have rapidly emerged as a growing and profitable threat, challenging the long-held perception that Apple devices are largely immune to malware. The full KELA report includes detailed case studies, examples, and behavioral analysis of macOS users and threat actor activity, highlighting how these devices have become attractive targets for cybercriminals. Full report - The Rise of macOS Infostealers: 2025 in Review • KELA Cyber Threat Intelligence.

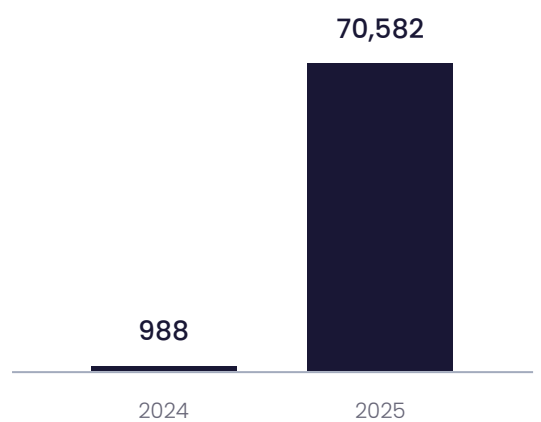
The graph below illustrates a surge in macOS infostealer interest, where buyer demand has skyrocketed tenfold since 2022 to reach an all-time high in 2025. This increase reveals a mature underground economy where the rapid professionalization of Malware-as-a-Service (MaaS) offerings - typified by high-performance stealers like Atomic (AMOS)[8] - is actively meeting an insatiable criminal appetite for high-value Apple enterprise and cryptocurrency targets.

macOS InfoStealer Economy Trend

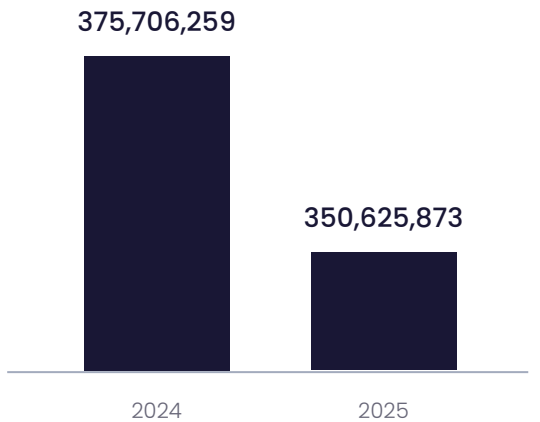


The most significant shift came when these tools evolved into commodity malware. Under the malware-as-a-service (MaaS) model, macOS infostealers are now packaged, sold, or rented through underground forums and Telegram channels, complete with subscription pricing, updates, and customer-like support. This has lowered the barrier to entry for attackers and enabled infostealers to be deployed at scale.

macOS Infostealer Infections Across 2024-2025



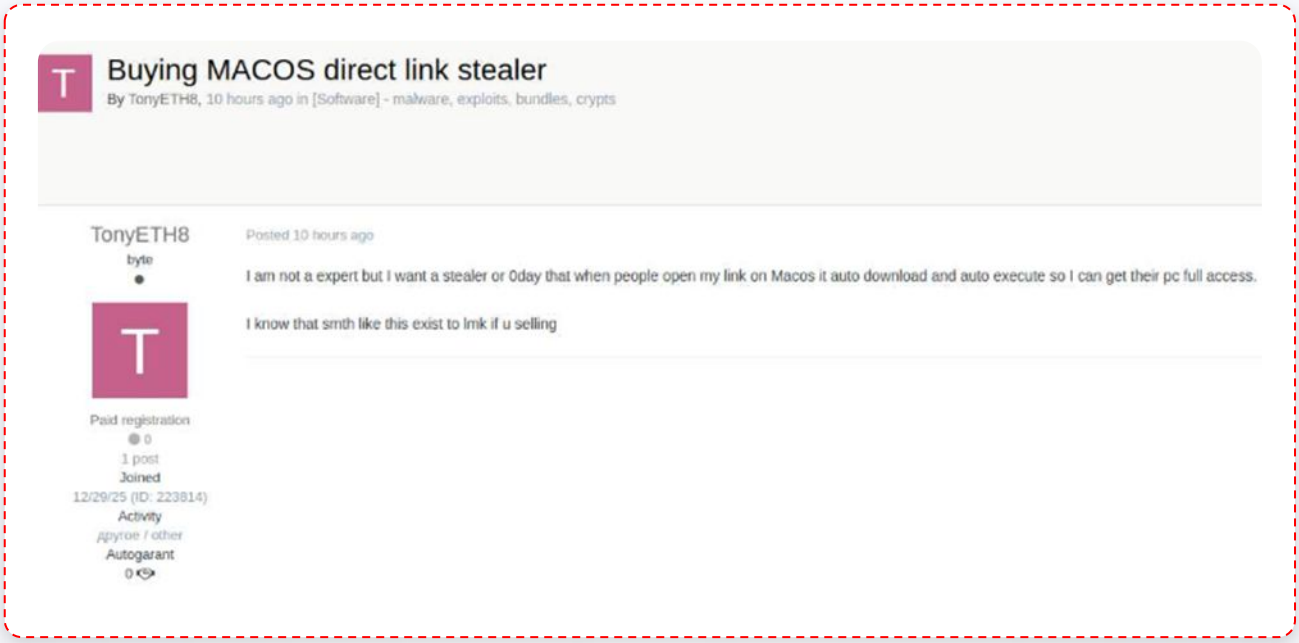
Windows + Other OS Infostealer Infections Across 2024-2025



[8] The first commercialized infostealer targeting MacOS, observed around April 2023.

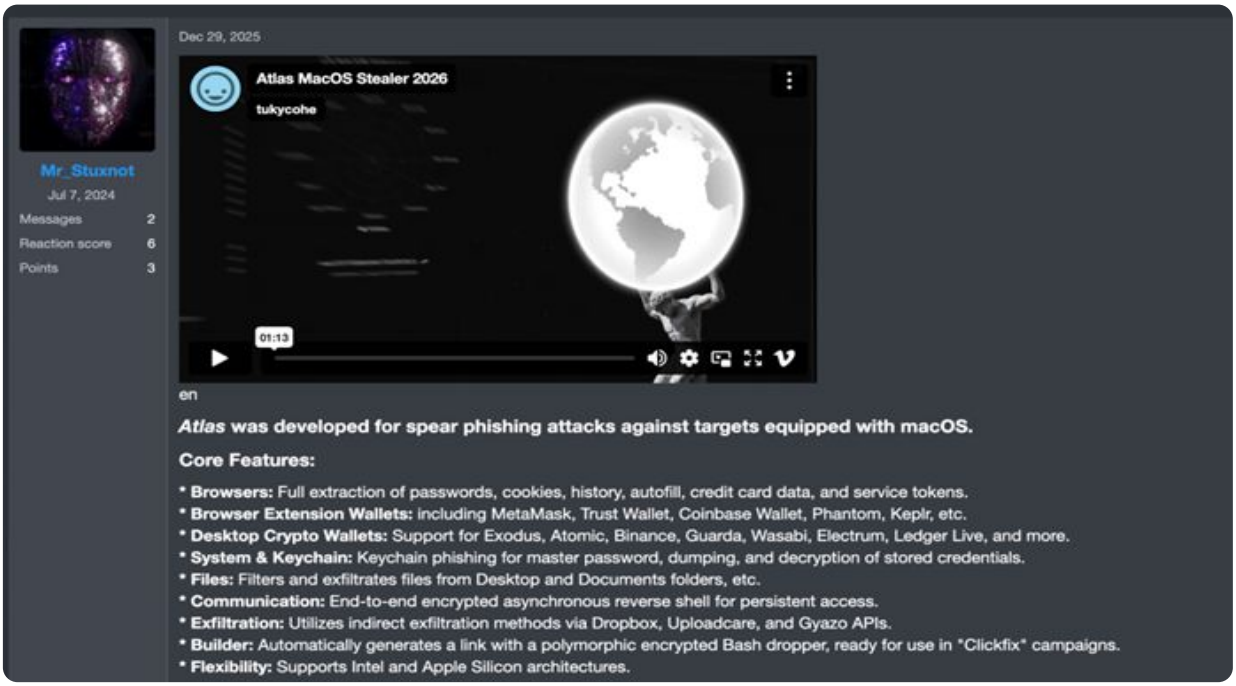
KELA's data lake shows a clear surge in infostealer-infected machines running macOS variants in 2025. While Windows remains the dominant operating system in absolute terms, macOS-related infostealer records increased from fewer than 1,000 in 2024 to over 70,000 in 2025, representing a sharp year-over-year expansion. This growth significantly outpaces the overall market trend and indicates rising demand and operational focus on macOS environments by threat actors. Although macOS activity still constitutes a small fraction of total infostealer telemetry compared to Windows, the scale and velocity of this increase reflect a maturing underground ecosystem, with macOS treated as a viable and monetizable target within the broader credential-theft economy.

KELA observed on December 29, 2025, a post on the ExploitIn cybercriminal forum where a threat actor actively sought to acquire a direct link stealer specifically for macOS. This request serves as a clear indicator of the lowering barrier to entry for macOS-based cybercrime, as the actor's phrasing - requesting a tool that works automatically by a simple click - highly suggests an entry-level or low proficiency criminal profile. This individual is explicitly seeking to bypass the technical complexities of manual exploitation, such as local privilege escalation or bypassing Apple's Gatekeeper, by purchasing a pre-configured solution that requires minimal engagement on the attacker's end and relies entirely on a single victim action.



This post highlights the effectiveness of the Malware-as-a-Service (MaaS) model, which allows low-skilled actors to access polished, click-to-infect macOS malware. By democratizing malware, MaaS enables even non-technical criminals to target lucrative Apple and cryptocurrency sectors, driving continued growth in macOS threats in recent years with tools such as Atomic (AMOS) and other stealth-focused variants.

KELA observed on December 29, 2025, a post on the RAMP cybercriminal forum in which a threat actor, Mr_Stuxnot, advertised Atlas macOS Stealer 2026, a macOS-focused infostealer for targeted spear-phishing campaigns. The tool, claimed to be compatible with both Intel and Apple Silicon, harvests browser credentials, session tokens, credit cards, and cryptocurrency wallets, and includes advanced features such as keychain phishing and credential decryption. A polymorphic, encrypted Bash dropper optimized for ClickFix[9] campaigns, encrypted reverse-shell persistence, and cloud-based exfiltration illustrate a shift toward stealthy, turnkey malware that allows even less-skilled actors to deploy fully weaponized campaigns with minimal effort.



The post also includes a video allegedly demonstrating the management panel and proof-of-concept, showing harvested logs from an infected Mac, highlighting how cybercriminals are increasingly investing in marketing, promotion, and user experience to build credibility and differentiate offerings in the underground economy.

[9] ClickFix: A technique where attackers trick users into executing malicious commands themselves - often via fake 'fix it' prompts, CAPTCHAs, or update screens - effectively bypassing traditional security defenses by exploiting human trust.

KELA's 2026 Predictions: Growth, Automation, and Resilience

Looking ahead to 2026, the use of infostealers is expected to continue growing, driven by the further professionalization of Malware-as-a-Service (MaaS) platforms and increasingly sophisticated malware capabilities. These developments will allow a broader range of actors to launch credential-theft campaigns with minimal technical expertise, expanding the reach and impact of infostealer operations.

Emerging MaaS providers, cross-platform malware, and AI-assisted campaigns are likely to accelerate this trend, introducing more automated, resilient, and adaptable attack methods. Malware targeting macOS, Linux, and mobile platforms is expected to grow alongside traditional Windows-focused tools, reflecting an expansion in both scope and victim base.

The rapid adoption of AI across personal and professional workflows is increasing the volume and sensitivity of data handled by end users. As AI agents and copilots evolve to continuously document context, prompts, decisions, and user behavior, compromised environments infected by infostealers may expose not only credentials and API tokens, but also rich conversational histories and contextual AI interactions. This significantly elevates post-compromise risk, enabling threat actors to reconstruct user intent, operational workflows, and internal business logic, and to conduct highly targeted follow-on access, impersonation, and social engineering.

Overall, the infostealer ecosystem in 2026 is projected to become more automated, cross-platform, and industrialized, maintaining its central role in credential-theft operations and underscoring the need for proactive monitoring, strong authentication, and comprehensive endpoint protection.

Countermeasures

Intelligence & Exposure Monitoring	Leverage cyber threat intelligence (CTI) and actively monitor underground markets to detect exposed corporate credentials, session tokens, and API keys in near real-time.
Identity & Session Security	Enforce phishing-resistant MFA, implement strict session management to prevent token replay, and mandate frequent rotation of privileged credentials.
Infrastructure Hardening	Organizations should deploy behavior-based EDR on endpoints to detect and block evasive infostealer execution. In addition, advanced email filtering should be utilized to block phishing, which is the primary delivery mechanism for these threats. Finally, network segmentation is critical for isolating systems and preventing lateral movement via stolen credentials.
Proactive Threat Hunting	Routinely hunt across the network for unusual outbound traffic communicating with known malicious domains or infrastructure.
AI Environment Protection	Treat AI copilots and APIs as high-value targets. Enforce least-privilege access, limit context retention, and actively monitor for exposed AI tokens.
Security Awareness Training	Train employees to identify sophisticated phishing, avoid unverified software, secure physical work devices, and report suspicious activity immediately.
Infostealer-Specific Incident Response	Maintain tailored playbooks focused on rapid containment, mandatory credential rotation, session/token revocation, and downstream access reviews.

The Extortion Explosion: How Ransomware Scaled to 7,500+ Victims

In 2025, the ransomware and extortion ecosystem was defined by a rise in publicly claimed victims, along with a split in actor capability. While elite operations continued to refine industrial-scale ransomware campaigns, the wider landscape was simultaneously flooded by opportunistic new operations, unscaled data leaks. The top three actors of 2025, Qilin, Akira and Clop, demonstrate three differently structured operations parallely rising. **Qilin** operates as an established Ransomware-as-a-Service (RaaS)[10], while **Akira** works as an apparently closed operation. And while both these groups leverage double extortion in attacks - **Clop** spent 2025 executing attacks based on data theft along with multiple extortion techniques.

2025 also showed a notable rise in the number of attacks. KELA identified **7,549 victims claimed by 147 active threat actors in 2025,** representing a **45% increase** from 2024. This surge was not driven by sophistication alone: the emergence of approximately **80 new groups** introduced variability, with many entrants appearing short-lived. Some even recycle brands and leak content, or operate as lower-tier extortionists rather than consistently capable ransomware operators. This duality of high-precision ransomware activity alongside newcomer behavior, was a main feature of 2025.

[10] Ransomware-as-a-Service (RaaS) is a subscription-based cybercrime business model where developers create ransomware tools and infrastructure and lease them to other criminals, called affiliates, for a fee or a share of the ransom profits. This model enables individuals with limited coding skills or infrastructure to launch sophisticated and damaging cyberattacks.

Operationally, Ransomware-as-a-Service remained a dominant and competitive business structure. Tactically, most of the ecosystem continued to rely on double extortion, meaning attackers steal data and encrypt systems to maximize payment pressure. The leading actors utilizing this standard model were Qilin and Akira, followed by Play, SafePay and INC. Extortion-only (data theft without encryption) also gained visibility and will likely keep growing. An enabling factor observed throughout 2025 was the role of compromised credentials, often harvested by infostealers and circulating the web, in facilitating intrusion and extortion activity. KELA assesses that some ransomware ecosystems likely accelerate their intrusion timelines by buying ready accesses from Initial Access Brokers (IABs) or pre-compromised credentials to bypass early attack stages.

This chapter provides an in-depth analysis of these shifts, beginning with a breakdown of 2025's most targeted countries and sectors. Highlighted are some of the most active threat actors and the high-impact attacks that defined 2025's impact. Finally, KELA gives a strategic outlook for 2026, detailing the emerging monetization tactics and technological shifts expected to shape the next phase of the threat landscape.

KELA's 2025 Ransomware Insights

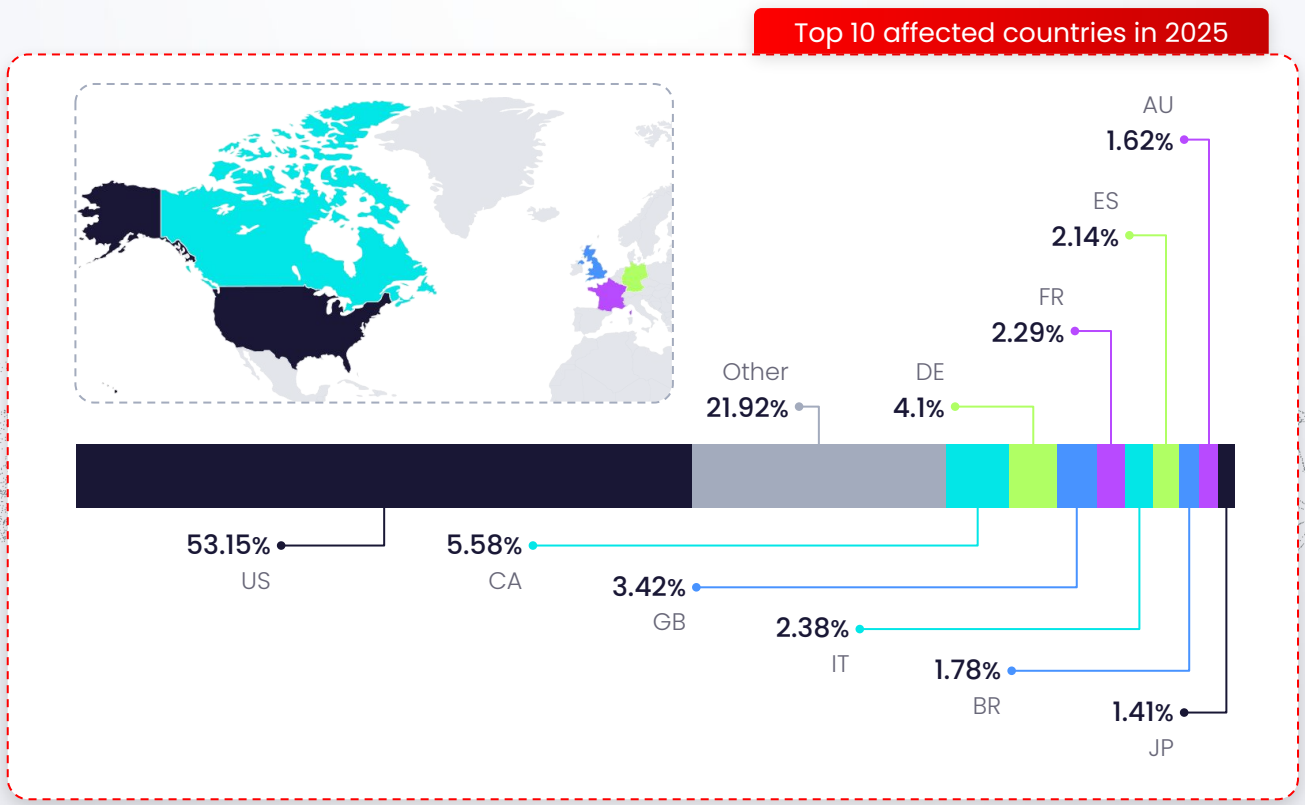
In 2025, KELA tracked **over 7,549 ransomware/extortion victims,** marking a **45%** increase from 2024. These attacks were claimed by **147 different actors,** representing a roughly **50%** increase in active threat groups compared to the previous year. Of these groups, KELA identified only about **30** as being purely **extortion/data theft groups,** while the remainder utilized encryption on the victim's network.

The ransomware landscape remained highly volatile and competitive, with approximately **80 new threat groups** emerging throughout the year. This is a notable increase from the almost 60 new groups observed in 2024, suggesting that despite law enforcement efforts, the barrier to entry remains low, with new operators continually filling the voids left by groups that have disbanded or rebranded.

Attacks per Country

In 2025, ransomware activity remained heavily concentrated within a few key nations, with the **top five countries** accounting for over **68%** of all tracked victims. The **United States** experienced the highest volume by a significant margin, representing **53.2%** (over 4,000 victims) of the global total. This was followed by Canada at 5.6%, Germany at 4.1%, the United Kingdom at 3.4%, and France at 2.5%. The sustained focus on these high-value economies, particularly the US, continues to drive aggressive and ongoing law enforcement efforts to disrupt the underlying cybercriminal infrastructure.

Compared to 2024, the geographic distribution of attacks remained quite consistent. The United States continued its long-standing trend as the primary target, showing only a slight increase from the 52% observed in the previous year.

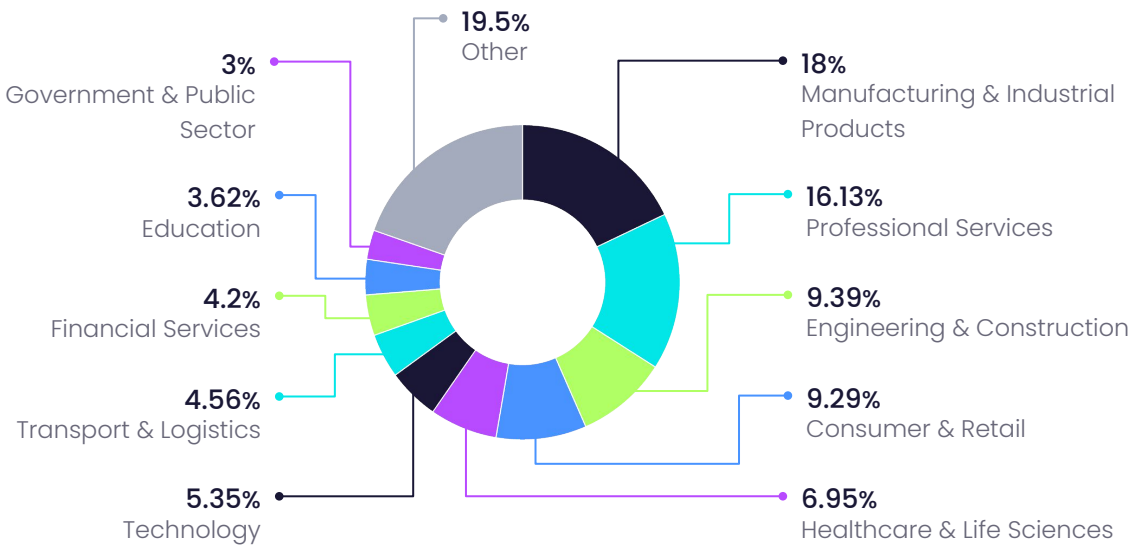


Attacks per Sector

The 2025 threat landscape saw a clear concentration of activity within two primary sectors: **Manufacturing & Industrial Products,** which led with **18%** of all attacks, and **Professional Services**[11]**,** which followed closely at **16.13%.** The Engineering & Construction sector solidified its standing as the third most targeted industry at 9.39%, followed by Consumer & Retail (9.29%) and Healthcare & Life Sciences (6.95%). This targeting reflects a focus on sectors where operational downtime or data exposure creates immediate and significant financial or reputational pressure.

When comparing these results to 2024, the data shows a mirroring of previous trends with a few notable shifts in rank. While Manufacturing & Industrial Products claimed the top spot in 2025, it was Professional Services that held a slim lead in 2024 (16.27% vs 16.14%). One of the most significant changes was in the Consumer & Retail sector, which climbed to the fourth position in 2025, surpassing Healthcare & Life Sciences, which saw its share decrease from 8.33% in 2024 to 6.95%. Other sectors, such as Technology and Financial Services, maintained a steady share of the landscape with only minor shifts in their relative rankings.

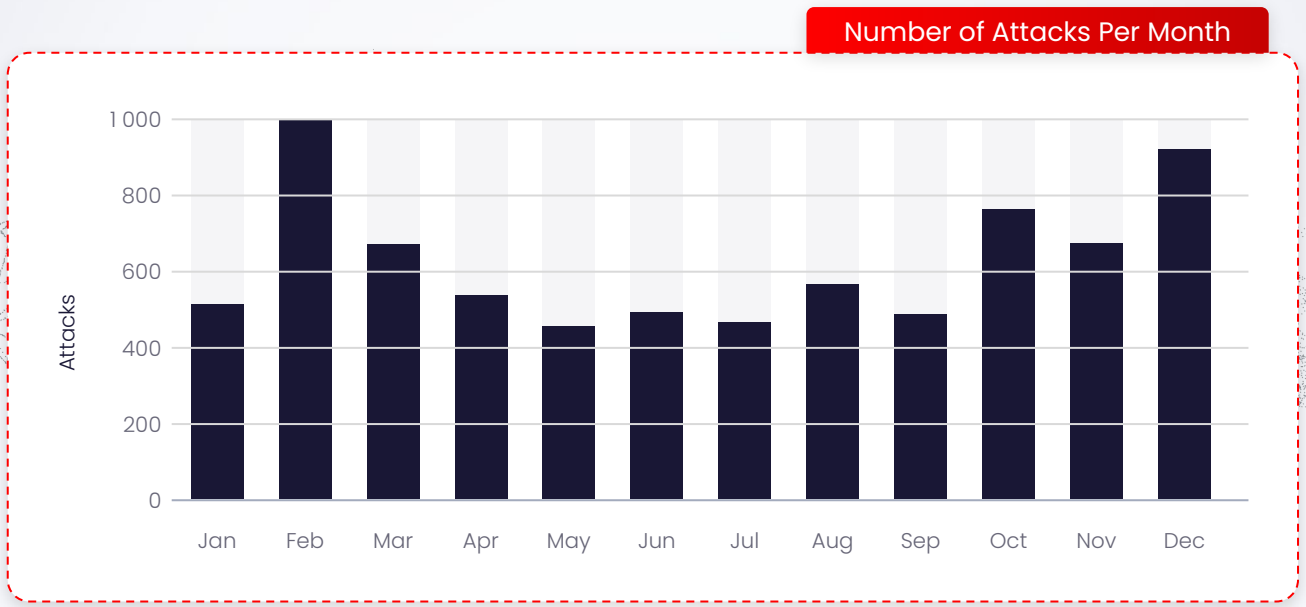
Top 10 affected sectors in 2025



[11] The Professional Services sector includes businesses in the following subsectors: consulting firms (business, IT, security), law firms, accounting & audit firms, marketing/PR agencies, etc.

Attacks per Month

2025 was characterized by distinct waves of high-intensity activity rather than a consistent baseline. While Q2 and Q3 saw a relative stabilization with counts hovering around 500 attacks per month, the year was bracketed by aggressive surges in the first and fourth quarters.



The year began with an unprecedented surge, peaking in February with over 1,000 recorded attacks. This anomaly was primarily driven by Clop, which claimed 279 victims in a single month by leveraging a mass-exploitation campaign against Cleo Managed File Transfer (MFT) vulnerabilities. Akira (113 victims) and RansomHub (98 victims) also contributed significantly to this February spike.

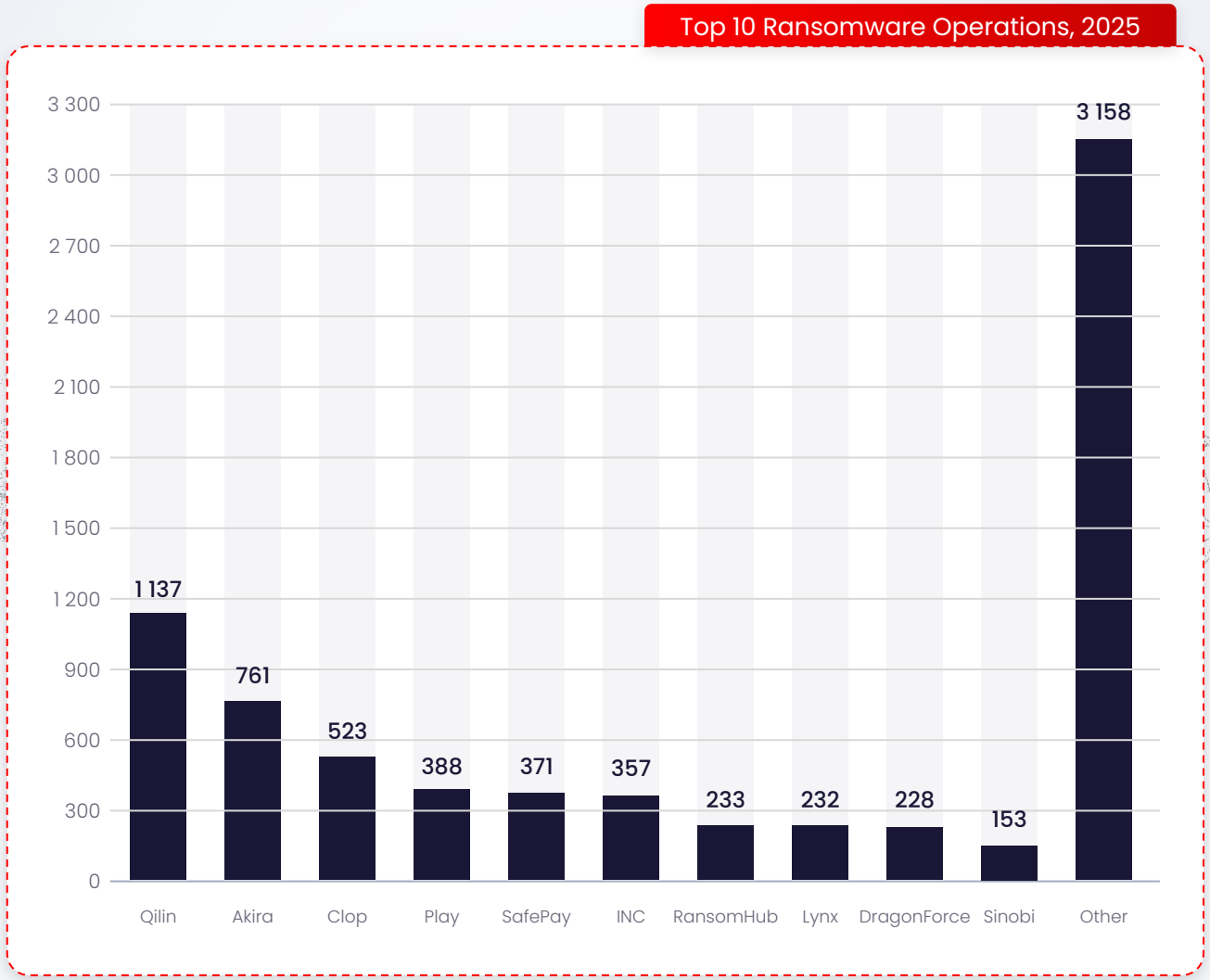
In Q4, activity accelerated sharply again. October marked the beginning of this resurgence with over 780 attacks, dominated by Qilin, which claimed 212 victims, a surge suspected as tied to the shutdown of RansomHub. This trend continued in November with Clop's return to mass-exploitation, this time targeting Oracle E-Business Suite to compromise over 100 enterprise environments.

The year concluded with a second peak in December (approximately 930 victims). This final surge was fueled by Qilin's sustained pressure (205 victims) and a defiant return from LockBit (107 victims), whose late-stage spike demonstrated the group's operational recovery despite previous law enforcement disruptions.

Top Active Ransomware Groups

During 2025, KELA's data recorded a significant number of attacks claimed by the top three groups - **Qilin, Akira** and **Clop. Qilin** leads the list with claims exceeding **1,140 victims,** a massive surge in volume compared to the activity of 2024, where RansomHub (now ranked 7th with 233 claims after the group went offline in April 2025) carried out 529 attacks. Based on KELA's data, Qilin led as the most active ransomware operation, even with activity only starting to rise from June to December of 2025.

Akira is the operation that followed as the second most active group of 2025, with a high count of 761 victims, and Clop came third claiming 523 victims. Play ransomware remained a persistent threat recording a similar number of victims compared to 2024 (388 in 2025 compared to 363 in 2024), followed closely by SafePay (371) and INC (357).



Notably, LockBit, which was long listed among the top ransomware groups in the past several years, and ranked as the second most active in 2024, has lost its position within the top 10 groups in 2025. LockBit has struggled to maintain its ranking, marking 148 victims compared to 500 in 2024, despite resurfacing with a renewed affiliate program and the release of a LockBit 5.0 variant. LockBit's shutdown and regrowth signals both resilience and a competitive change among operations, as it is possible that other groups are considered more reliable in 2025.

Victims Claimed Twice or More in 2025

According to KELA's database, **128 victims** were claimed as ransomware victims twice or three times by different ransomware operations in 2025, a **30%** rise from 2024. These instances may occur due to collaboration between groups but could also be separate attacks that took place in parallel, possibly utilizing the same initial access vector.

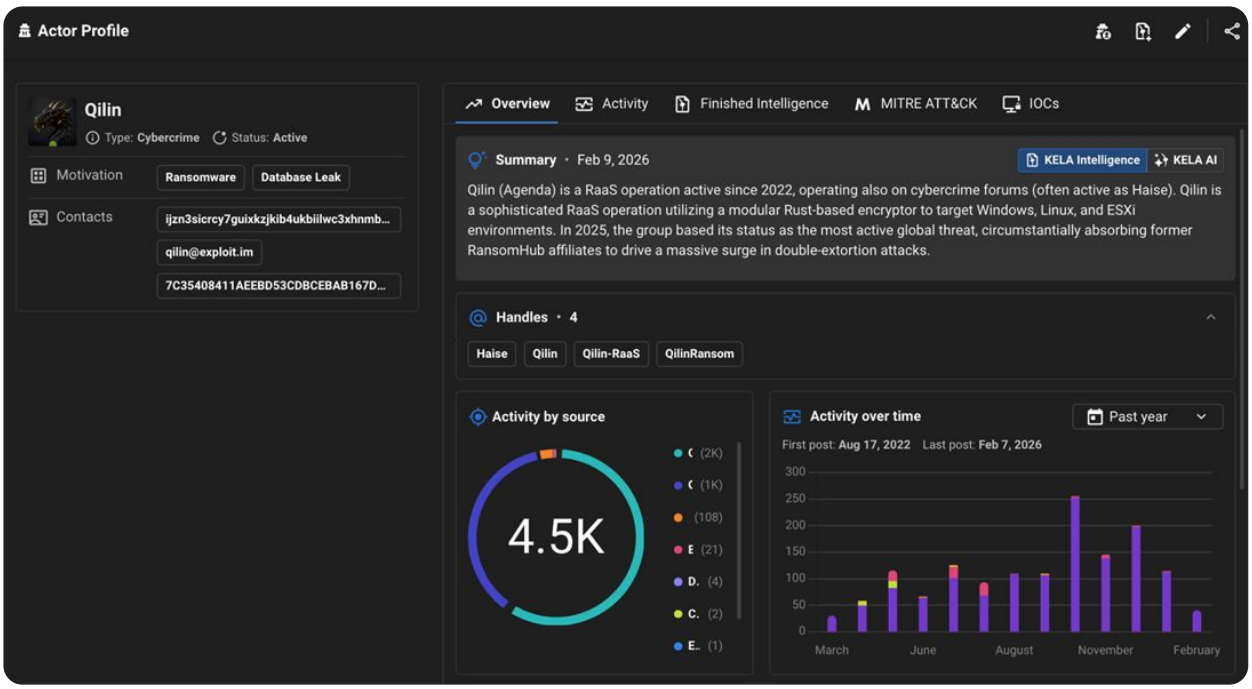
Actor Highlight

The Actor Highlight section provides a comprehensive profile of the three most active ransomware groups that defined the 2025 threat landscape, examining the operational tactics and strategic evolution of Qilin, Akira, and Clop - actors responsible for a significant portion of the year's global attack volume.

Qilin

Qilin (also known as Agenda) established its status as the most prolific threat actor of 2025, operating a sophisticated Ransomware-as-a-Service (RaaS) model that dominates the global cybercrime landscape. Originally surfacing in 2022 with a Golang-based payload, the group has since evolved to use a highly efficient Rust-based encryptor, customizable for each victim, allowing for rapid targeting of Windows, Linux, and VMware ESXi environments.[12]

Qilin's Actor Profile | KELA Platform



Activity Overview

Qilin's operations in 2025 were characterized by aggressive double-extortion tactics: encrypting critical systems while simultaneously exfiltrating vast amounts of sensitive data to pressure victims into payment.

[12] Ransomware Threat Actor Profile: Qilin | KELA Cyber

Qilin Ransomware: A Customisable Threat with Big Targets | STORM Guidance

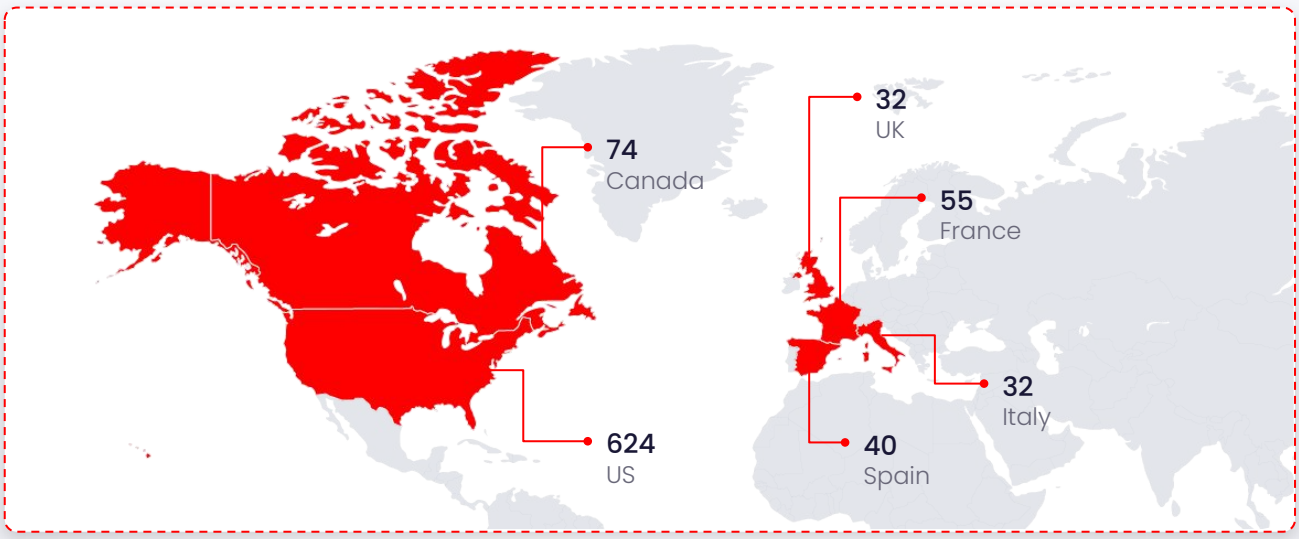
The group's rise to the top of 2025 active ransomware groups (claiming 1,137 victims in total) was affected by shifts within the ransomware cybercriminal ecosystem. Specifically, a key suspected parameter was the abrupt shutdown of the RansomHub operation in April 2025, which created a space to fill. RansomHub was a highly active RaaS operation, active since early 2024 and responsible for over 700 attributed attacks during its year of activity. In 2024 RansomHub was the top active group, and in November 2024 and February 2025, they took responsibility for an average of 100 attacks per month. In April 2025, following RansomHub's closure amidst rumors of an exit scam and internal disputes, a wave of their affiliates and partners raged that they had been mistreated. Although internal shifts within operations can be hard to detect, it is possible that Qilin, who held a stable infrastructure by that point, absorbed these displaced affiliates. This could explain Qilin's sudden ability to scale its campaigns dramatically in the second half of the year.

KELA observed this increase firsthand, recording unprecedented spikes in activity during Q4. In October alone, Qilin claimed 212 victims, followed by a sustained offensive in December with 205 victims. This late-year surge targeted organizations globally, with a heavy concentration on Western economies.

Targeted Countries & Sectors

Qilin's 2025 campaigns were heavily concentrated in North America and Western Europe. The United States was the primary target, accounting for 624 recorded victims. This was followed by Canada with 74 victims. Qilin also targeted organizations across Europe, most notably in France (55), Spain (40), the United Kingdom (32), and Italy (32).

Qilin's 2025 campaigns heavily targeted manufacturers and supply chains. Notable incidents included the breach of Asahi Group Holdings that disrupted global production, and later in the year, the Korean Leaks campaign, which further proved their reach exploiting a single MSP to compromise 28 victims simultaneously. Qilin also demonstrated its impact in the attack on Synnovis, which started in 2024 yet had lingering effects throughout 2025, crippling NHS pathology services in London for months.[13]



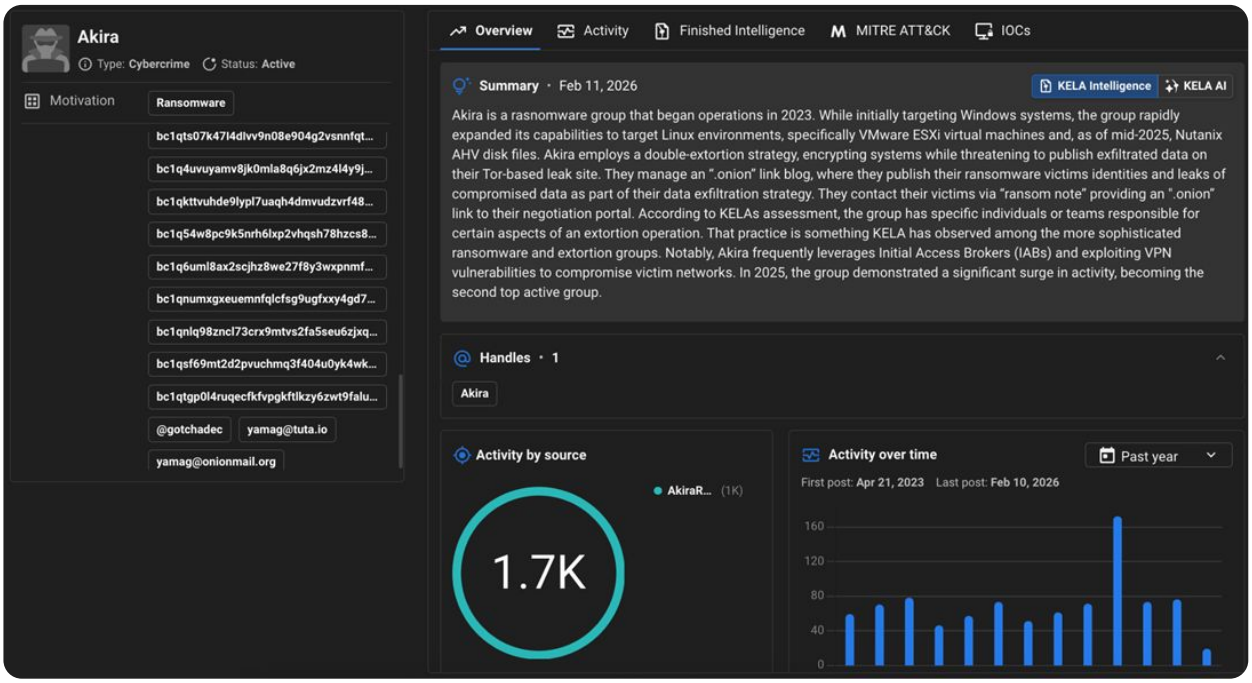
[13] NHS England » Synnovis cyber incident,

The Korean Leaks – Analyzing the Hybrid Geopolitical Campaign Targeting South Korean Financial Services With Qilin RaaS

Akira

In 2025, Akira secured its position as the second most active ransomware group globally, with 761 claimed victims. Akira was observed in 2023 with a sophisticated structure that allowed it to maintain confidentiality. While Akira initially built its reputation on targeting small-to-medium-sized businesses, 2025 saw the group successfully impact larger organizations across critical infrastructure, manufacturing, education, healthcare and finance.

Akira's Actor Profile | KELA Platform



Activity Overview

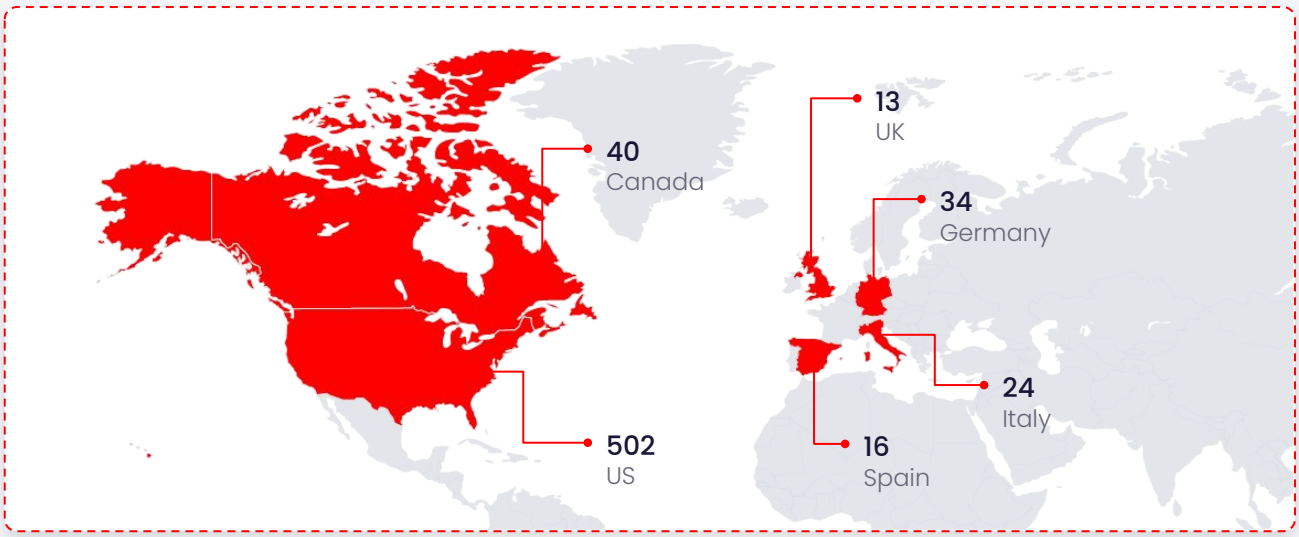
Akira's operational success in 2025 was defined by a focus on unpatched edge devices and the speed of their operations. In 2025, Akira's initial access was characterized majorly by targeting of VPN appliances, specifically exploiting vulnerabilities in Cisco and SonicWall devices (such as CVE-2024-40766), where multi-factor authentication (MFA) wasn't used. To accelerate the kill chain, Akira affiliates are assumed to have utilized Initial Access Brokers (IABs) to purchase compromised credentials to sensitive environments of organizations, allowing them to bypass early intrusion stages and move directly to lateral movement. In fact, the group is quite transparent about this methodology; and in their ransom notes and security reports provided to victims, they explicitly claim that "initial access to the network was purchased on the dark web", confirming their reliance on external cybercrime markets to fuel their operations.[14]

[14] Arctic Wolf Observes July 2025 Uptick in Akira Ransomware Activity Targeting SonicWall SSL VPN

According to researchers, a technical evolution observed in June 2025 where Akira expanded its targeting beyond standard Windows and VMware ESXi environments to be also encrypting Nutanix AHV (Acropolis Hypervisor) virtual machine disk files.[15]

Targeted Countries & Sectors

Geographically, Akira's 2025 campaigns demonstrated a relentless focus on North America and Western Europe. The United States was by far the primary target, accounting for the vast majority of attacks with 502 recorded victims. This was followed by Canada with 40 victims. Akira was also targeting organizations across Europe, most notably in Germany (34), Italy (24), Spain (16), and the United Kingdom (13).

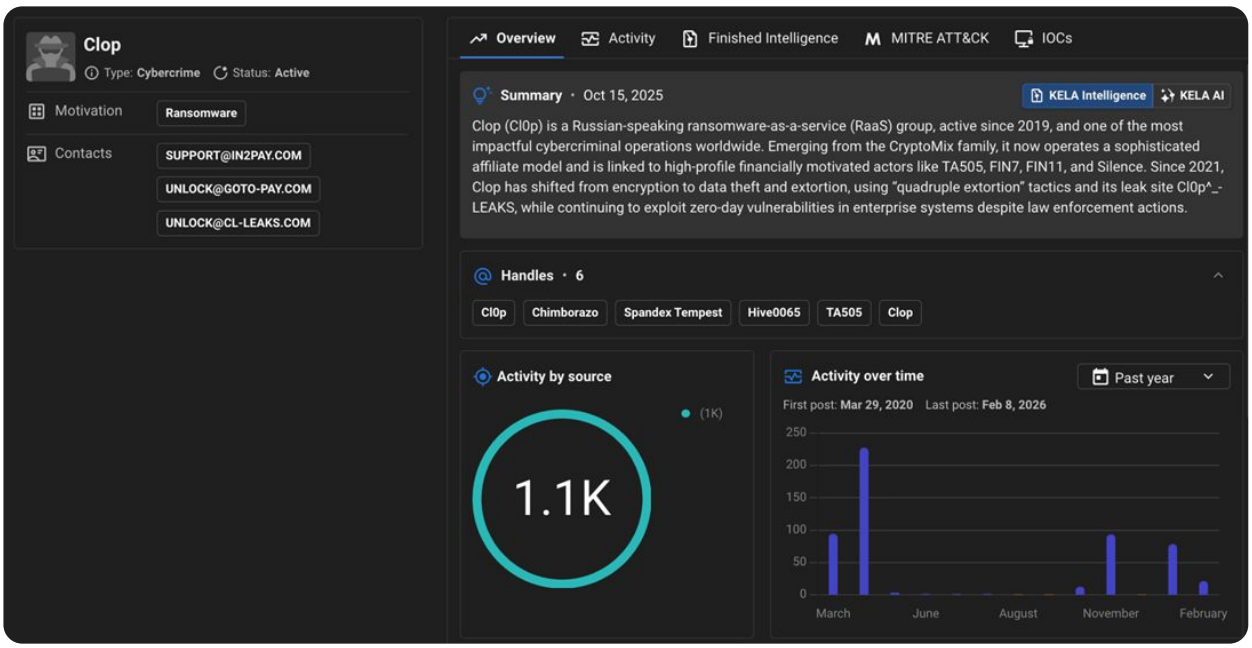


[15] #StopRansomware: Akira Ransomware | CISA (Updated to 2025)

Clop

Clop (also known as Cl0p and TA505)[16] ranked as the third most active threat group of 2025, claiming a total of 523 victims. Clop utilizes a hybrid extortion model that fluctuates between traditional ransomware deployment and data theft depending on the target and access method. As such, the group is notorious for its industrial-scale supply chain attacks that often bypass encryption in favor of rapid data exfiltration. This dual threat is amplified by their quadruple extortion tactics, where pressure is applied not just through encryption and data leaks, but also by DDoS attacks and by directly contacting victims' customers and partners to force payment.[17]

Clop's Actor Profile | KELA Platform



Activity Overview

Clop's 2025 activity was defined by two massive 'zero-day' waves that accounted for the majority of their victim volume. The year opened with a continuation of the aggressive, late 2024 surge driven by Clop's mass exploitation of CVE-2024-55956 in Cleo Harmony, VLTrader, and LexiCom file transfer platforms. After determining that a prior patch (for CVE-2024-50623) was insufficient, Clop operators used this new zero-day to deploy a JavaScript backdoor known as Malichus. This campaign fueled the group's unprecedented peak in February (279 victims), allowing them to exfiltrate data from hundreds of organizations simultaneously.

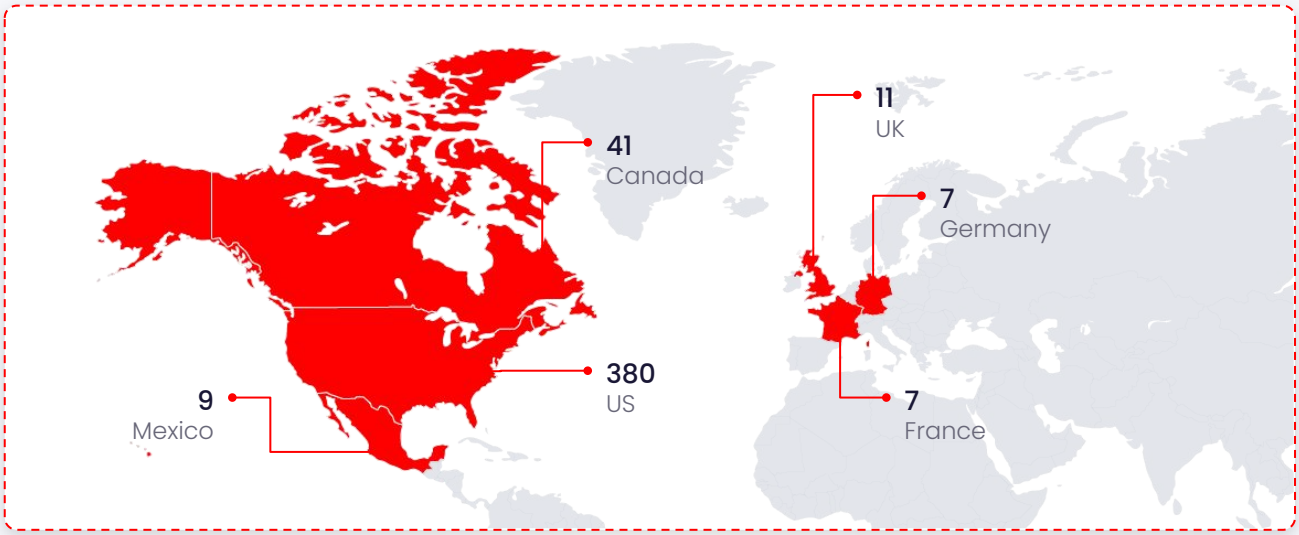
[16] #StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability | CISA

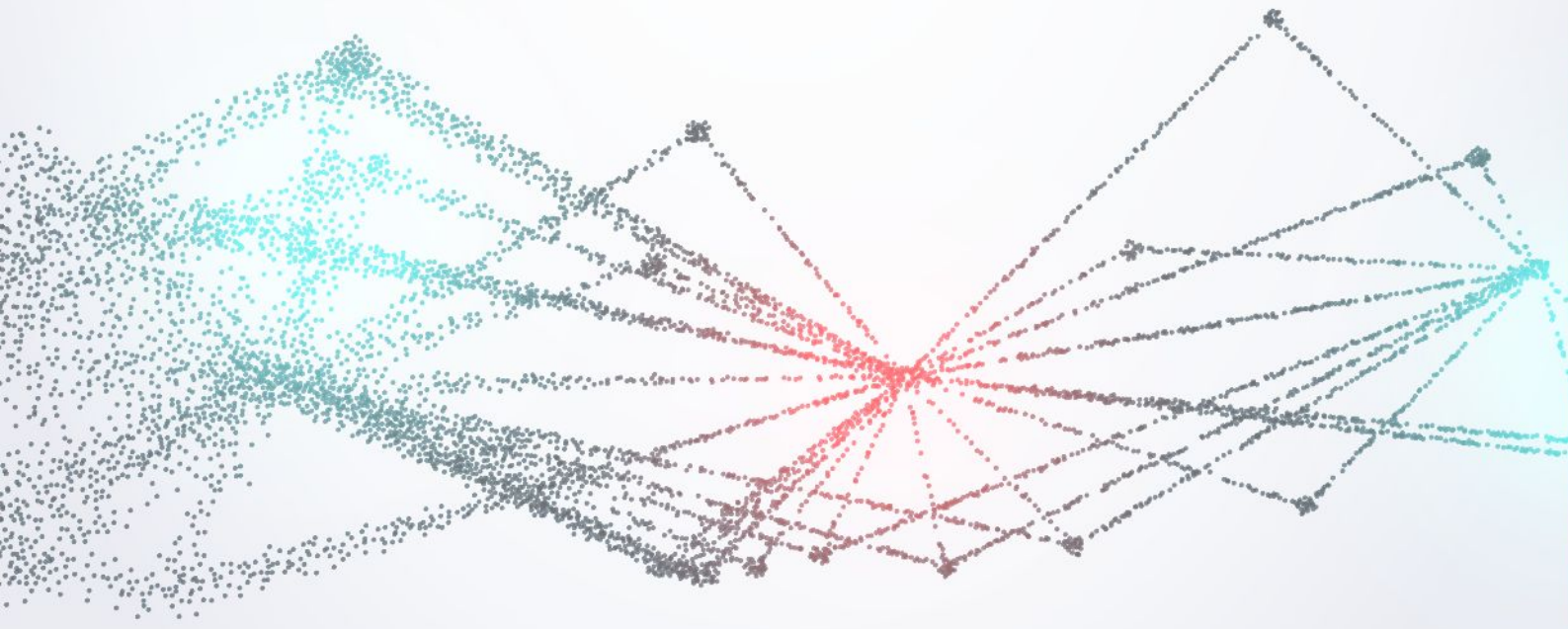
[17] Cl0p ransomware: The skeezy invader that bites while you sleep | Barracuda Networks Blog

In Q4, Clop launched a campaign targeting Oracle E-Business Suite (EBS) by exploiting CVE-2025-61882, a critical unauthenticated remote code execution (RCE) vulnerability. This campaign focused on data theft and extortion, and Clop went as far as attempting extortion with email campaigns. The group bypassed encryption to focus entirely on stealing sensitive data from over 100 enterprises, including Mazda, Harvard, Envoy Air, and The Washington Post, and threatening publication if ransom demands were not met.[18]

Targeted Countries & Sectors

Similarly to the other top actors, Clop's 2025 campaigns demonstrated a strong focus on North America. The United States was by far the primary target, accounting for 380 recorded victims. This was followed by Canada with 41 victims. Clop also targeted organizations in the United Kingdom (11) and Mexico (9), with additional activity recorded in Germany (7) and France (7).





[18] Alleged Cl0p Extortion Emails Linked to July 2025 Oracle E-Business Suite Vulnerabilities - Arctic Wolf
University of Phoenix Data Breach Exposes 3.5 Million in Oracle E-Business Suite (EBS) Zero-Day Attack

Notable Ransom Attacks

This chapter highlights notable ransomware attacks of 2025, focusing on those that caused significant disruption to linked economies and global supply chains. While not all incidents were equally impactful, the most severe cases are assessed by both ransom payments and the broader financial and operational damage to victim organizations and their partners.

Jaguar Land Rover: The Costliest Cyberattack in British History

In September 2025, the UK-based automotive giant Jaguar Land Rover (JLR) confirmed that it suffered a major cyber-attack.[19] JLR was targeted in a sequence of attacks involving the threat actor Rey (admin of Hellcat) and the hybrid extortion group Scattered Lapsus$ Hunters (SLH).

The initial attack occurred in March 2025, when Rey claimed a breach of JLR's network, executed using Atlassian Jira credentials stolen from an employee of the JLR supplier LG Electronics. These credentials had been harvested by an infostealer infection, as seen in different campaigns led by Hellcat ransomware. Later in September, the incident escalated when Scattered Lapsus$ Hunters claimed responsibility for a massive financially motivated cyber attack on JLR.

The two incidents are suspected as linked, as Rey was later identified as an administrator for Scattered Lapsus$ Hunters, suggesting the initial supplier access could have facilitated the broader operation.[20]

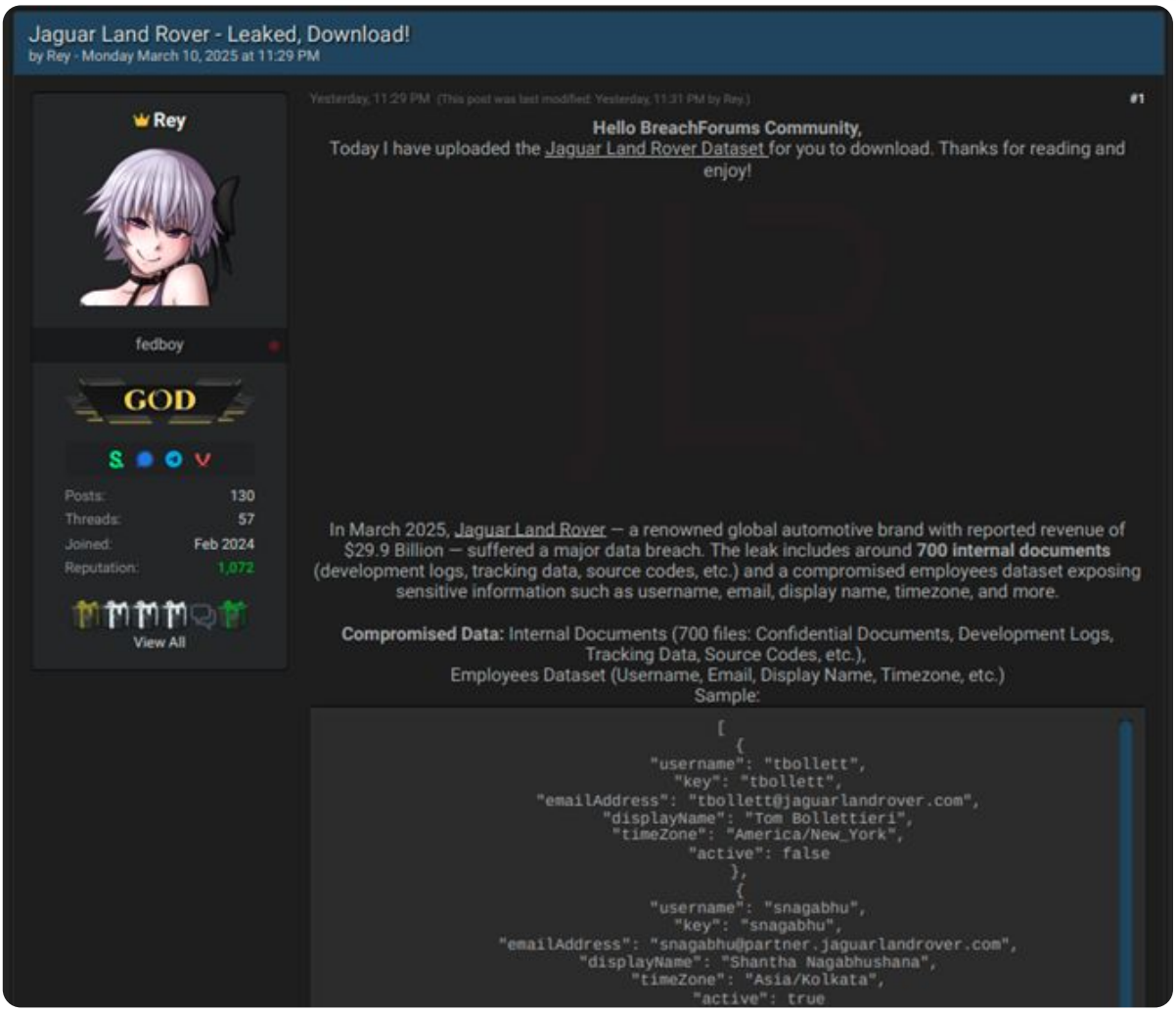
The incident is considered as one of the most economically damaging cyber events of the year, with an estimated total cost to the UK economy of £1.9 billion ($2.5 billion). The attack forced a six-week production halt across JLR's global plants, which reversed the company's profitability into a £485 million quarterly loss and caused wholesale sales to plummet by nearly 43%. The disruption cascaded through the supply chain, affecting over 5,000 independent organizations and triggering a 0.17 percentage point contraction in the UK's GDP. The operational paralysis was so severe that the UK government authorized a £1.5 billion loan guarantee to prevent a collapse of the dependent supplier ecosystem.[21]

[19] Statement on Cyber Incident | JLR Media Newsroom

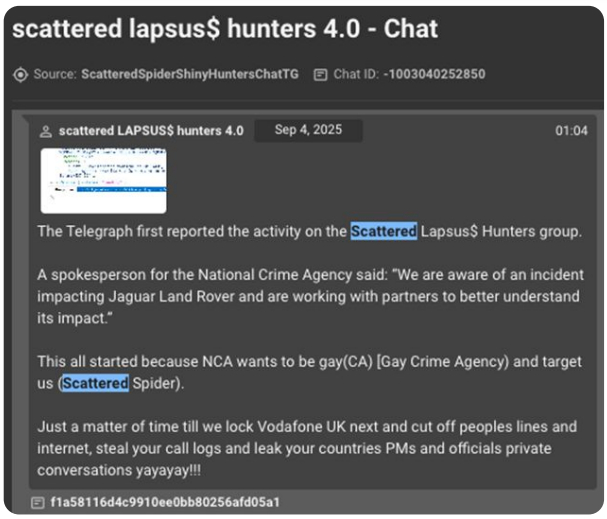
[20] Meet Rey, the Admin of 'Scattered Lapsus$ Hunters' – Krebs on Security

[21] JLR Q3 SALES IMPACTED BY CYBER INCIDENT AS PREVIOUSLY INDICATED | JLR Media Newsroom,
Jaguar Land Rover slides to loss of almost £500m after cyber-attack,
Jaguar Land Rover expected to restart some production after cyber-attack - BBC News,
Ministers' claims to have helped JLR in doubt as £1.5bn support left untouched | Jaguar Land Rover,
Jaguar Land Rover: how a cyber attack cost the British economy £1.9 billion

Rey (Hellcat) Claims the March Breach to Jaguar Land Rover



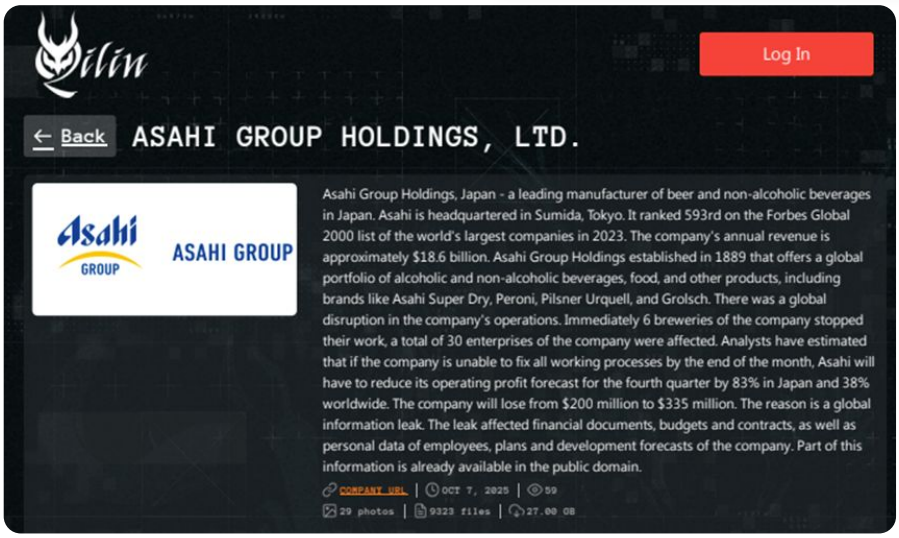
Scattered Lapsus$ Hunters (SLH) refers to the September attack on Jaguar Land Rover | KELA Platform



Asahi Group: The Manufacturing Halt

On September 29, 2025, Asahi Group Holdings, Japan's largest brewer, disclosed a major ransomware attack that disrupted domestic operations. Qilin Ransomware claimed responsibility, exfiltrating 27 GB of financial and employee data.[22] Asahi Group later confirmed that personal information for up to 1.94 million individuals, including 1.525 million customers, may have been exposed.[23]

Qilin Claims the Attack Against Asahi

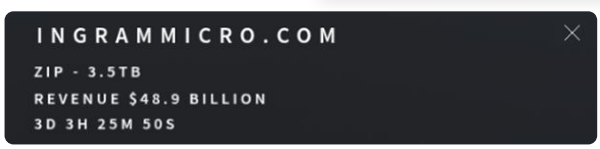


The attack's impact extended well beyond digital systems, forcing a physical shutdown of production lines at 30 domestic factories, which led to immediate product shortages across major retailers. This operational paralysis drove a financial decline with soft drink sales lowered by nearly 40%. The severity of the disruption rendered the company unable to finalize its accounts, compelling Asahi to indefinitely postpone its financial results for both the third quarter and the full fiscal year.[24]

Ingram Micro: Global IT Distribution Paralysis

In July 2025, an attack on the American technology distributor and business-to-business service providers Ingram Micro by the SafePay ransomware group demonstrated how a single attack can sever the core arteries of global technology distribution.[25]

SafePay Claims the Attack Ingram Micro



[22] Notice of System Failure Due to Cyberattack | Newsroom | ASAHI GROUP HOLDINGS

[23] Investigation Results and Future Measures on Cyberattack Data Exposure | Newsroom | ASAHI GROUP HOLDINGS,
Asahi admits possible leak of 1.91 million personal records | The Asahi Shimbun: Breaking News, Japan News and Analysis

[24] Japan days away from running out of Asahi Super Dry due to cyber attack – reports,
Decoding the Asahi Brewery Ransomware Attack | Qilin TTP Breakdown & OT Security Insights,
Business Progress Update in View of Delayed FY2025 Q3 Results Announcement | Newsroom | ASAHI GROUP HOLDINGS

[25] Ingram Micro Issues Statement Regarding Cybersecurity Incident, information | Ingram Micro

Reportedly, the threat actors gained initial access via Ingram Micro's GlobalProtect remote-access environment using compromised credentials; reporting later clarified the VPN gateway itself was not exploited.[26]

The ransomware took down the transactional platforms of Ingram Micro, which powers supply chains for over 160,000 customers in 200 countries, for nearly a week. According to analysis, the company stood to lose more than $136 million in sales for each day it could not fulfill orders. Managed Service Providers worldwide were left unable to track shipments, manage licenses, or process returns, causing project delays and SLA breaches for thousands of small and medium-sized enterprises.[27] Beyond the operational paralysis, Ingram Micro confirmed that the breach exposed the personal information of more than 42,500 individuals. The compromised data included sensitive employment records, names, and Social Security numbers.[28]

The Co-operative Group: The Human Factor in Retail Collapse

In late April 2025, the British consumer Co-operative Group, which operates thousands of grocery stores and other businesses in the UK, faced a wide cyber attack, suspected to be attributed to the hybrid English-speaking hacker collective Scattered Spider (deploying DragonForce ransomware-as-a-service)[29]. The breach did not begin with a technical exploit but with a social engineering attack that allowed threat actors to reset a single employee's password.

This initial foothold spiraled into a systemic paralysis, forcing the retailer to shut down IT infrastructure, resulting in empty shelves and the suspension of digital orders across thousands of stores. The financial toll was severe: analysts estimated the disruption cost the group approximately $275 million in lost revenue and operational recovery expenses.[30]

The incident was part of a broader, highly coordinated campaign by the Scattered Spider collective that simultaneously targeted other major UK retailers. This spree included a devastating attack on Marks & Spencer during the 2025 Easter weekend, which crippled their automated stock systems and led to an estimated loss of over $400 million. Harrods was also targeted in the same period, though the British luxury retailer successfully thwarted the attempt by preemptively restricting internal system access.[31]

In July 2025, the UK's National Crime Agency (NCA) arrested four individuals, including a 17-year-old and three young adults, connected to this series of attacks on M&S, the Co-op, and Harrods.[32]

[26] Ingram Micro Cyberattack: Lessons for UK SMEs on Supply Chain Risk

[27] Ingram Micro Issues Statement Regarding Cybersecurity Incident, The Ingram Micro Ransomware Attack: Lessons Learned - Proven Data

[28] Maine.gov - Data Breach Notifications

[29] Scattered Spider | CISA

[30] Customers complain as empty shelves continue at Co-op after hack - BBC News, Co-op says cyber-attack cost it £206m in lost sales - BBC News

[31] Marks & Spencer Breach: How A Ransomware Attack Crippled a UK Retail Giant | BlackFog, Final Results - 07:00:08 20 May 2025 - MKS News article | London Stock Exchange

[32] Retail cyber attacks: NCA arrest four for attacks on M&S, Co-op and Harrods - National Crime Agency

KELA's 2026 Predictions: Encryption, Extortion, and the Race for Fast Monetization

In 2026, traditional ransomware operations built on the RaaS model will remain dominant, with double extortion (data theft and encryption) continuing as the primary monetization strategy. Encryption and operational disruption are not expected to decline; rather, the most impactful campaigns will continue to be driven by mature, well-structured RaaS programs capable of sustaining affiliates, tooling, and scale, as demonstrated by Qilin's late-year surge in 2025. At the same time, data theft and extortion without encryption will continue to expand, used both by mature actors pursuing rapid, large-scale monetization and by newer entrants. A likely addition to either module are extra layers of extortion that can add a human, psychological, pressure on the victims.

KELA expects the competitive wave of new groups to continue: some will try to capitalize on momentum by launching small operations, while many will gravitate toward established RaaS brands like Qilin, and rising operations such as DragonForce and Nova. The appearance of new groups and actors is anticipated to be joined by new reputation games and monetization scams: actors will attempt to impersonate or fabricate successful ransomware and extortion activity to build reputation from nothing and to scam victims, partners, or would-be affiliates. This trend already emerged in 2025 with fake or recycled leak claims such as Babuk2, and it is already visible in 2026 with newly surfaced operations such as 0APT, which from the start attracted attention due to fake and exaggerated claims.

Also expected is more AI-assisted enablement among newer groups; mainly as an assisting means to weaponization, platform building, and possibly also as an aiding factor in running negotiation chats. However it is too soon to tell whether operations heavily built on AI will be at a level that outcompetes well-structured RaaS programs.[33]

Meanwhile, Law enforcement activity and takedown operations will likely still shape the ransomware ecosystem in 2026. Continued disruption efforts are likely to influence both the scale of certain operations, and how actors structure their infrastructure, partnerships, and public promotion of malicious services. Groups are anticipated to try and adapt their branding, communication channels, and operational visibility in order to stay active and maintain affiliate confidence.

[33] First known AI-powered ransomware uncovered by ESET Research,
Nine Emerging Groups Shaping the Ransomware Landscape | TRM Blog

Countermeasures

Monitor RaaS and Affiliate Trends	Leverage cyber threat intelligence (CTI) to continuously track evolving Ransomware-as-a-Service (RaaS) groups, affiliate tools, and sector-specific targeting patterns, allowing defenses to be adjusted proactively.
Disrupt Initial Access and Infostealers	Monitor underground markets for stolen credentials, session data, and initial access sales targeting your organization. Promptly revoke compromised sessions, reset affected accounts, and investigate impacted hosts to break the attacker's kill chain before deployment occurs.
Adopt Zero-Trust Architecture	Implement a zero-trust model based on continuous verification to strictly limit resource access and drastically reduce opportunities for ransomware lateral movement.
Harden Helpdesk and Account Recovery	Enforce strict identity verification and multi-stage approvals for password resets and privileged recovery actions to thwart social-engineering-led account takeovers.
Deploy XDR and Advanced Endpoint Defenses	Utilize Extended Detection and Response (XDR) to correlate threats across endpoints, networks, and cloud environments. Deploy advanced, behavior-based anti-malware to block known and unknown evasive strains, explicitly extending this hardening and monitoring to servers and virtualization hosts to prevent large-scale encryption.
Data Segmentation and Encryption	Encrypt sensitive data and segment critical repositories from less critical resources. Enforce strong access controls to limit cross-environment reach, reducing both the theft and encryption blast radius.
Deploy Exfiltration Tripwires	Alert on unusual bulk file access, data staging or compression, and large outbound network transfers to detect and disrupt extortion-only operations early in the attack lifecycle.

Accelerated, Prioritized Patching	Conduct frequent patch management across all systems. Prioritize critical updates for internet-facing systems and high-impact enterprise applications to minimize the attack surface for mass exploitation and supply-chain exploits.
Strengthen Supply Chain Security	Perform rigorous security assessments of third-party vendors, requiring adherence to recognized robust security frameworks. Enforce baseline controls and least-privilege access, and continuously monitor vendor privileges to detect and respond to external risks.
Harden Backup Strategies	Maintain offline, immutable, and regularly tested backups of all critical data to ensure rapid recovery capabilities in the event of a successful attack.
Simulate Ransomware Attacks	Conduct regular tabletop exercises and penetration tests to continuously evaluate, stress-test, and refine your organization's ransomware response strategy.

Zero-Day Industrialization: The Collapse of the Patching Window

In 2025, cybersecurity threats continued to evolve and outpace patching, with significant vulnerabilities emerging across a range of high-profile systems. These vulnerabilities were widely discussed on cybercrime forums, where threat actors share and sell public or unique PoCs for publicly disclosed vulnerabilities, as well as for zero days.

According to CISA's 2025 Year in Review[34], real-world exploitation activity remained high throughout the year with 238 high-risk vulnerabilities added to the Known Exploited Vulnerabilities (KEV) Catalog in 2025 alone. Compared to 185 KEV additions in 2024[35], this reflects a year-over-year increase in vulnerabilities confirmed to be actively exploited. CISA assessed more than 43,000 vulnerabilities to support remediation prioritization, and reported blocking more than two billions of malicious connections across federal networks and more than 300 millions within critical infrastructure. These findings highlight continued exploitation activity in 2025 and the importance of timely patching and proactive exposure reduction.

This chapter analyzes 2025 exploitation trends based on underground cybercrime activity observed on the KELA platform. It highlights patterns in underground chatter and reported exploitation activity, identifying the most discussed CVEs and targeted technologies, including WordPress plugins, Google Chrome, Next.js, React Server Components, and Palo Alto Networks GlobalProtect, with remote code execution emerging as a dominant vulnerability type. The chapter also examines supply-and-demand dynamics in exploit markets, highlighting exploit tools exclusive PoC sales, and limited-copy offerings, supported by graphical analysis of chatter trends and targeted services.

[34] 2025 Year in Review | CISA

[35] Known Exploited Vulnerabilities Catalog | CISA

Top CVEs Discussed by Threat Actors

According to threat actors chatter in cybercrime forums and Telegram chats as observed on KELA platform, the most mentioned CVEs from 2025 were:

CVE-2025-5287:

Affects the WordPress Likes and Dislikes Plugin (≤1.0.0), allows unauthenticated SQL injection via the post parameter.

CVE-2025-6554:

A type confusion flaw in Google Chrome V8 (prior to 138.0.7204.96), allows remote arbitrary memory read/write via a crafted HTML page.

CVE-2025-29927:

Affects multiple Next.js versions, allows authorization bypass when checks are implemented in middleware.

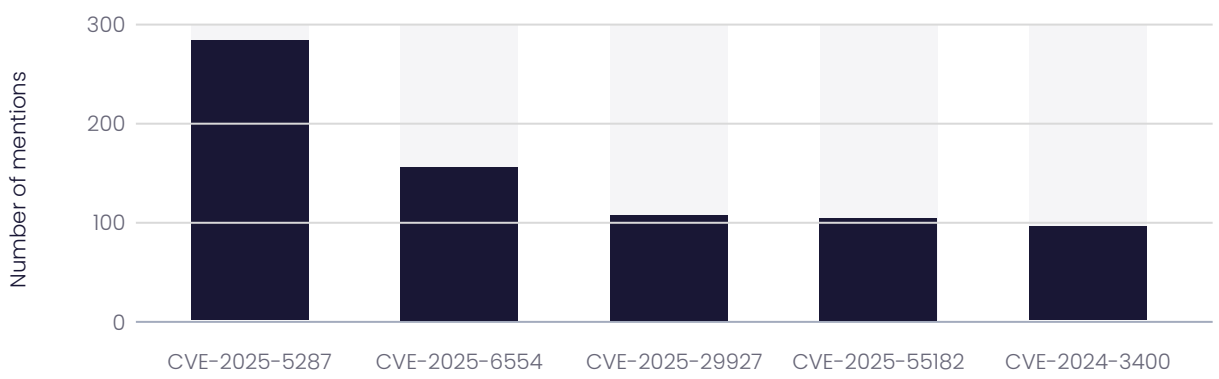
CVE-2025-55182:

Affects React Server Components (19.0.0–19.2.0), allows pre-authentication remote code execution.

CVE-2024-3400:

Affects Palo Alto Networks PAN-OS GlobalProtect, allows unauthenticated remote code execution with root privileges.

Top 5 CVEs mentioned on cybercrime forums and Telegram channels in 2025 (KELA platform)



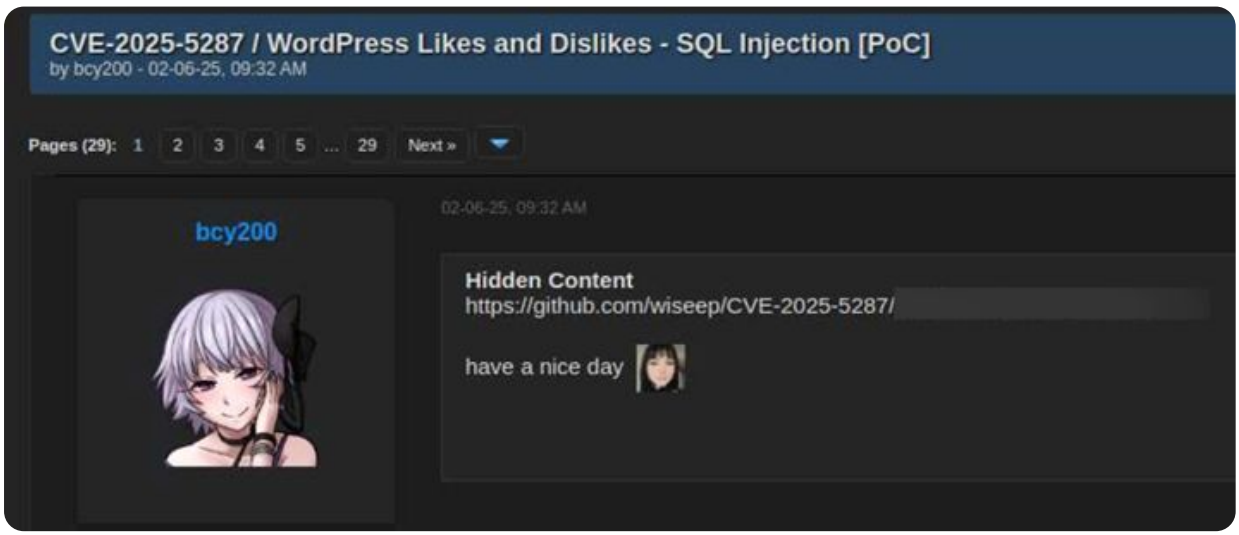
Underground Activity Surrounding the Top 5 CVEs

The following examples demonstrate the chatter observed on the KELA platform regarding the two most frequently mentioned CVEs - CVE-2025-5287 and CVE-2025-6554.

CVE-2025-5287: WordPress Plugin SQL Injection

In the screenshot presented below, the actor bcy200 shared on the cybercrime forum Darkforum, a GitHub link containing a Python script that automates time-based SQL injection testing for CVE-2025-5287 in WordPress installations. The tool enables bulk scanning and automated vulnerability validation. While not a fully weaponized exploit, it moves beyond a simple PoC by allowing large-scale identification of vulnerable targets, lowering the barrier for further exploitation. This post had sustained engagement over several weeks, with dozens of replies expressing interest, validation attempts, and appreciation for the shared code.

PoC advertised for this vulnerability in WordPress (DarkForum)

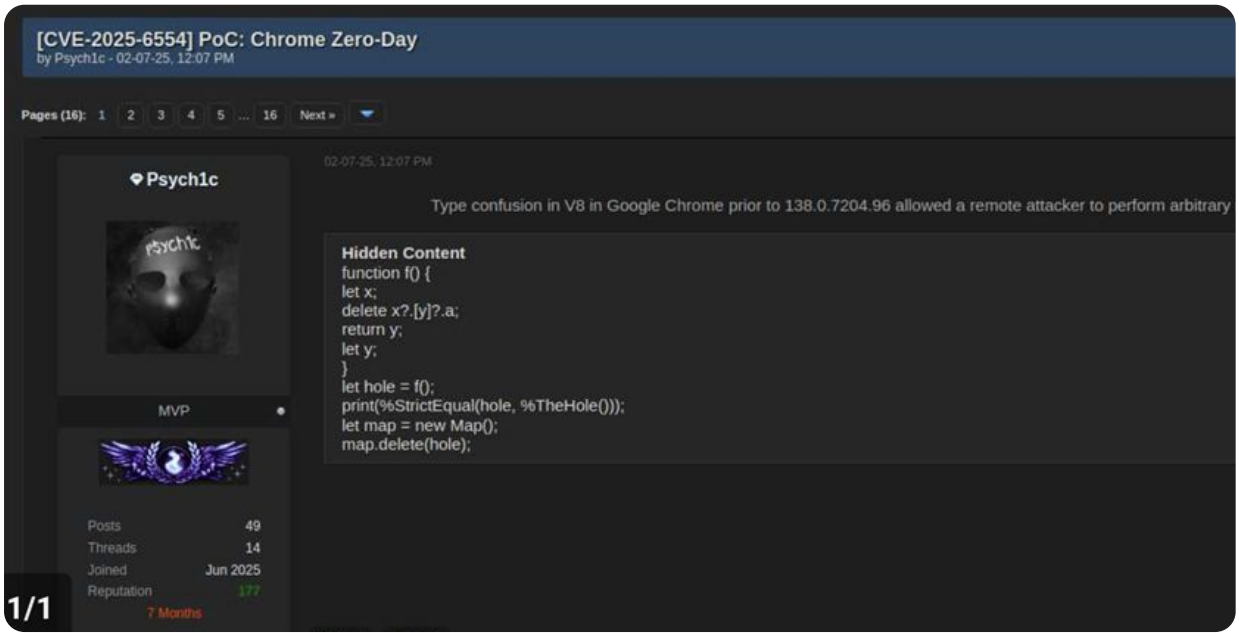


Although CVE-2025-5287 has not been listed in CISA's Known Exploited Vulnerabilities (KEV) Catalog, the lack of a vendor patch increases its risk. Public disclosure and readily available scanning tools leave exposed WordPress sites vulnerable until the plugin is removed or otherwise mitigated, creating conditions for potential future exploitation.

CVE-2025-6554: Google Chrome V8 Type Confusion

In addition, in the screenshot below, the actor Psych1c shared on Darkforum a code that serves as a technical PoC designed to trigger a type confusion vulnerability in Chrome's V8 engine (CVE-2025-6554). While the snippet itself does not directly enable data theft or remote code execution, it demonstrates a memory corruption condition that could serve as a foundation for further exploit development.

PoC advertised for this vulnerability in Google Chrome (DarkForum)



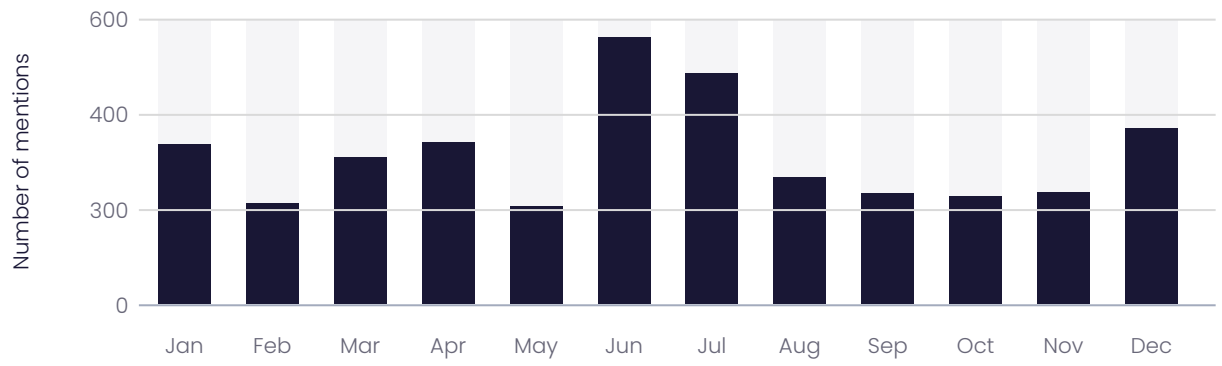
The presence of this PoC in cybercrime forums, with numerous users expressing intent to test and validate the PoC, indicates interest among actors, and highlights early-stage exploit research that could evolve into operational threats. Notably, the vulnerability was confirmed as exploited in the wild and added to CISA's KEV Catalog in July 2025. Google addressed this flaw, but systems that failed to update remained vulnerable to active exploitation.

These vulnerabilities highlight the continued exploitation of widely deployed web applications, browsers, network security appliances, and development frameworks. WordPress plugins, Google Chrome, Next.js, React Server Components, and Palo Alto Networks PAN-OS represent high-value targets due to their broad adoption, with remote code execution being a prominent vulnerability type discussed.

Tracking Threat Actor Engagement: Underground Chatter Timeline

Throughout the year, we observed steady chatter volume among threat actors, with a noticeable surge in June and July. Few of the most discussed vulnerabilities in 2025 according to KELA's sources, were disclosed or confirmed as actively exploited around the time of observed chatter spikes, underscoring the strong and immediate interest threat actors show in newly disclosed, high-impact vulnerabilities. CVE-2025-5287 (WordPress) was publicly disclosed in late May 2025, followed by CVE-2025-6554 (Chrome V8), which was confirmed as actively exploited at disclosure in late June 2025.

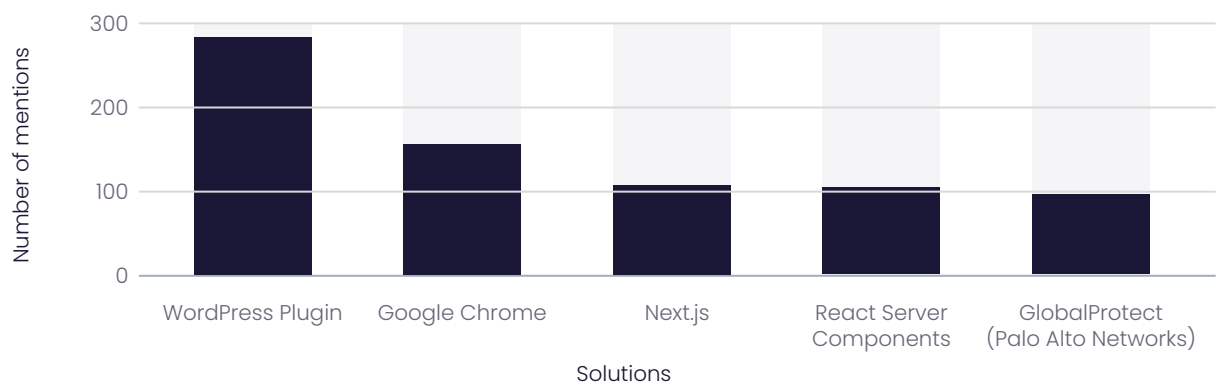
CVE mentions in cybercrime forums and Telegram channels in 2025



Top Mentioned Solutions in Cybercrime Underground

The most frequently discussed solutions and tools, as observed on KELA platform, included WordPress Plugins, Google Chrome, Next.js, React Server Components and GlobalProtect (Palo Alto Networks).

Top 5 solutions related to CVEs discussed on cybercrime forums and Telegram channels



A comparison to last year's KELA findings[36] reveals a shift in targets, though a recurring theme remains: Last year, the most frequently discussed and targeted solutions and tools, included FortiOS,, D-Link Cloud Network Storage devices, Microsoft Outlook, Windows Kernel, alongside various Wordpress plugins. Notably, **WordPress plugins remain a frequent target discussed by threat actors.** This repeated focus suggests that WordPress plugins represent a persistently exposed and scalable attack surface that continues to attract threat actor interest.

[36] The State of Cybercrime 2025 Report • KELA Cyber Threat Intelligence

2025 CVE Supply & Demand Chatter Analysis

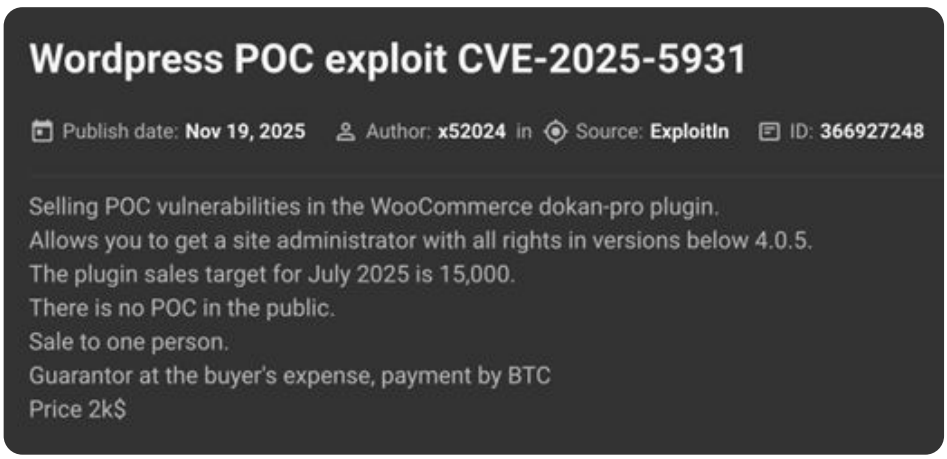
Analysis of underground chatter in 2025, as observed in KELA platform, reveals a commoditized ecosystem around recently disclosed CVEs, particularly those affecting widely deployed services (WordPress plugins, Fortinet appliances, etc.). The ecosystem spans public PoC sharing, private exploit sales, and the conversion of disclosed vulnerabilities into scalable mass-exploitation scripts. In addition, LLM-based text analysis of over 500 forum posts and Telegram messages related to supply and demand chatter, revealed trends in actors' chatter.

Limited-Copy and Exclusive Exploit Marketing

The analysis revealed that threat actors in 2025 increasingly promote limited-copy or **'exclusive' exploit sales** as a core business model. Advertisements frequently reference scarcity tactics such as 'sold one copy, two remaining' or 'single buyer only,' positioning the exploit as private and high-value. This controlled distribution model could be designed to increase perceived exclusivity while limiting widespread deployment that could accelerate detection and patching.

The screenshot below presents a post by the actor x52024 in the hacking forum Exploit, advertising an **exclusive** WordPress WooCommerce (dokan-pro) plugin PoC exploit (CVE-2025-5931), claiming administrator access, limited to a single buyer, and priced at $2,000 via BTC.

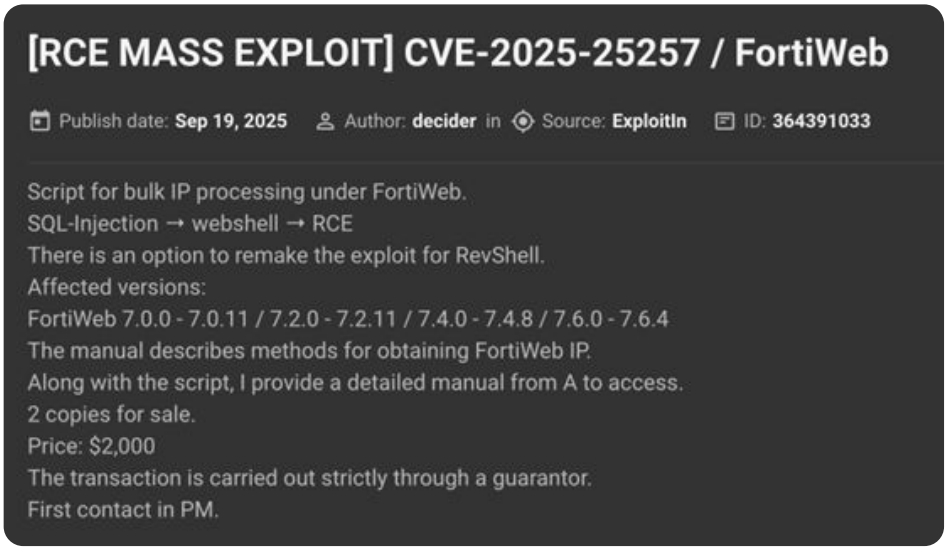
PoC advertised for exclusive sale (translated from Russian, KELA platform)



In addition, there is demand for fully weaponized exploit source code rather than simple proof-of-concept scripts. Sellers often provide turnkey packages that include integrated scanning and exploitation capabilities, bulk targeting functionality, and in some cases additional abuse features such as automated email or spam modules. These offerings significantly lower the technical barrier for buyers, enabling mid-tier actors to conduct mass exploitation campaigns without developing their own tooling, and further industrializing the exploitation ecosystem.

Furthermore, the screenshot below presents a post by the actor decider in Exploit forum, advertising a limited-copy mass exploitation RCE script for FortiWeb (CVE-2025-25257), featuring bulk targeting and a full attack chain, exemplifying the sale of a fully weaponized exploit packages rather than proof-of-concept code.

RCE exploit for FortiWeb advertised for sale (translated from Russian, KELA platform)



CISA's KEV Catalog: Confirmed Exploitation Activity

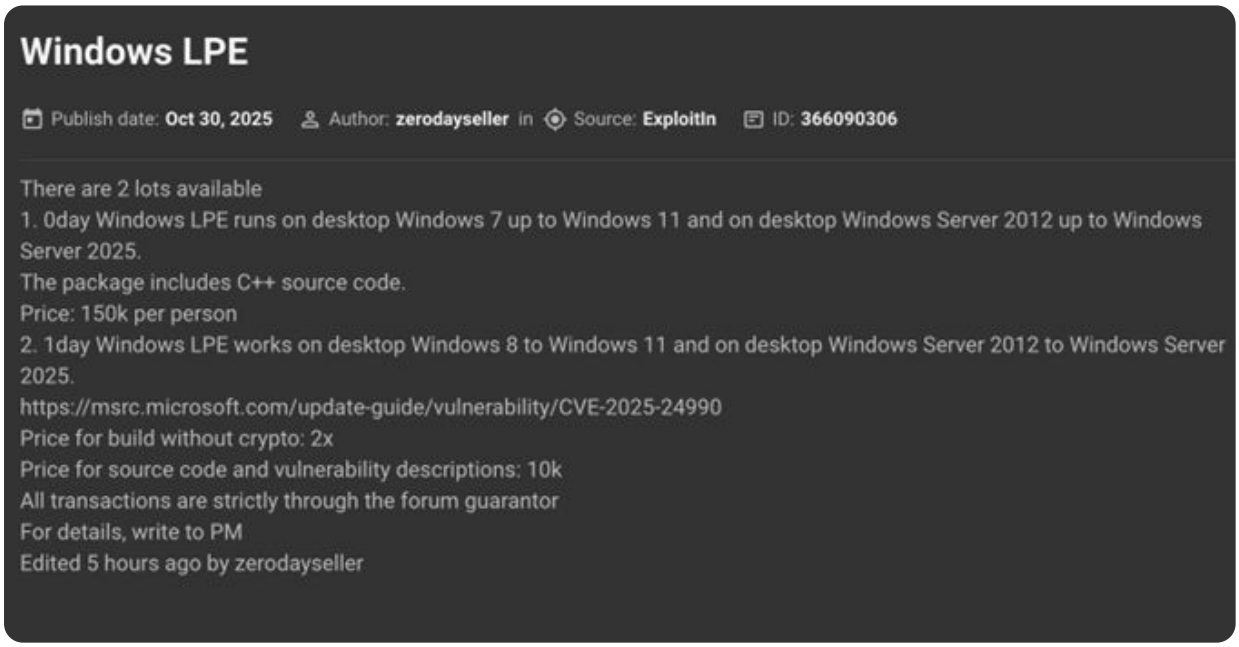
In the past two years, the most exploited product seems to be vulnerabilities in Windows. According to CISA Known Exploited Vulnerabilities Catalog[37], in 2025 alone 245 vulnerabilities were added to the catalog that have been exploited in the wild. In this, the most exploited vendor was Microsoft, followed by Apple, Cisco, Adobe and Google. Within that, the top 5 product names are Windows, Chromium V8, Internet Explorer, Flash Player, and Office.

Forum engagement around CVE-2025-6554 (Chrome V8), as observed in chatter on KELA platform (see example in "Underground activity surrounding the Top 5 CVEs section of this chapter), further reflects strong underground interest in widely deployed Google ecosystem products, particularly browser engine vulnerabilities that enable scalable exploitation.

In addition, CVEs related to Microsoft products that were added to the KEV Catalog were discussed in nearly 200 underground forum posts over the past year, as observed in the KELA platform. For example, the actor zerodayseller offered on the Exploit forum, exploits for CVE-2025-24990, a Windows local privilege escalation vulnerability, as presented in the screenshot below. The thread included price negotiations, discounts, and comments from users claiming successful transactions and confirming the exploit remained effective after patch cycles, indicating active underground interest in KEV-listed vulnerability.

[37] Known Exploited Vulnerabilities Catalog | CISA

Windows exploit advertised for sale (translated from Russian, KELA platform)



Compared to that, in 2024, 186 vulnerabilities were added to the catalog that have been exploited in the wild. In this, the most exploited vendor was Microsoft, followed by Ivanti, Google, Adobe and Apple. Within that, the top 5 product names are Windows, Chromium V8, Kernel (Android or Linux), Flash Player and PAN-OS. This year-over-year increase in exploited vulnerabilities shows that exploitation activity is growing and becoming more persistent, indicating a more active and evolving threat landscape.

KELA's Conclusion 2026 Predictions

The 2025 threat landscape demonstrates a sustained and structured exploitation economy centered on widely deployed and internet-facing technologies. Cybercrime forums, marketplaces and Telegram chatter indicate that publicly disclosed vulnerabilities are rapidly operationalized, commercialized, and distributed through organized underground channels. The prominence of remote code execution and authentication bypass vulnerabilities, particularly in WordPress plugins, enterprise web frameworks, browsers, and network security appliances, shows that attackers continue to focus on widely used, internet-facing systems that provide easy initial access. When these systems are not patched quickly, they can be exploited at scale, making timely patching and regular updates critical.

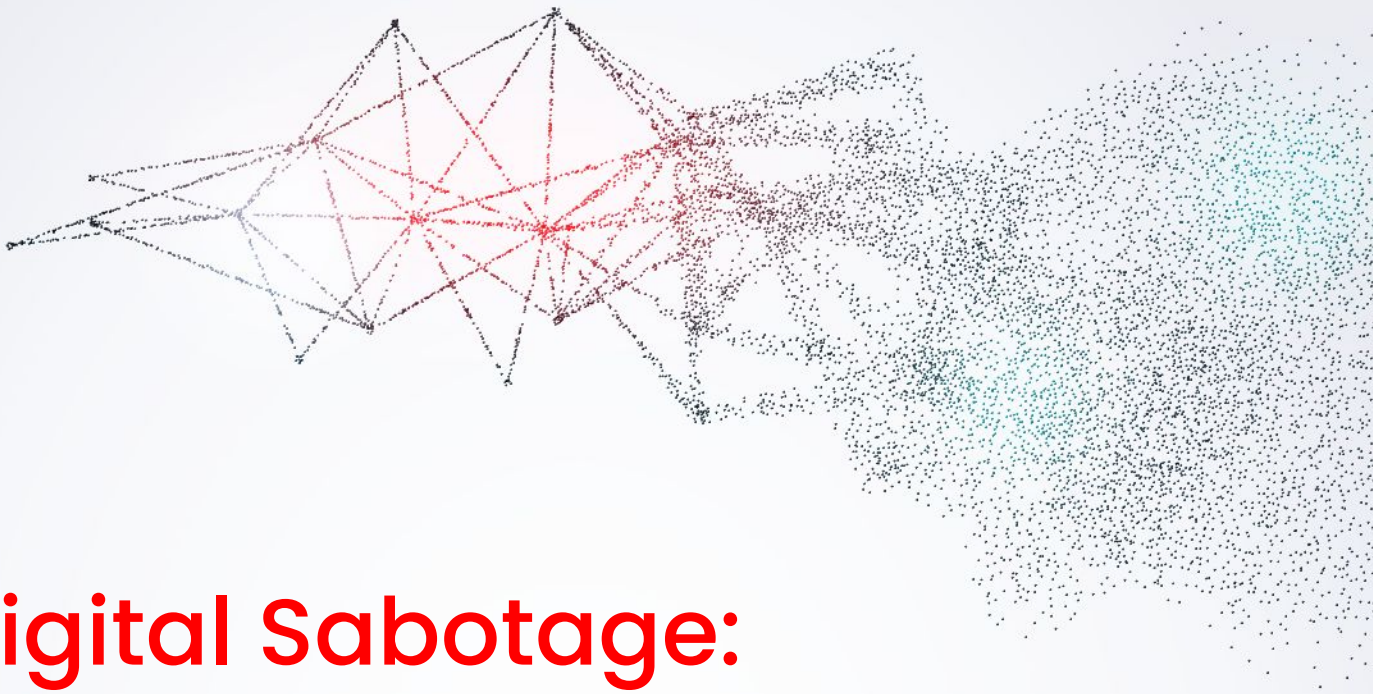
The convergence between underground discussions and entries added to CISA's Known Exploited Vulnerabilities (KEV) Catalog further highlights a strong correlation between publicly disclosed vulnerabilities, exploit commoditization, and real-world exploitation. Microsoft products, particularly Windows and browser-related components, remain consistently targeted.

Looking ahead, exploitation activity is expected to remain high in 2026, particularly targeting widely deployed and internet-facing technologies such as browser engines, enterprise frameworks, network security appliances, and Windows ecosystem components. The continued growth in KEV additions, combined with underground demand for exploit tools, indicates that weaponization timelines will remain short. Increased use of automation and AI-assisted research is likely to further accelerate exploit development and prioritization of high-impact vulnerabilities.

Countermeasures

Asset Tracking and Surface Monitoring	Utilize robust asset inventory tools to track all hardware and software. Regularly monitor your external attack surface to quickly identify and remediate exposed vulnerabilities.
Minimize Exposure and Harden Endpoints	Reduce externally exposed services by severely limiting unnecessary internet-facing systems. Adopt endpoint hardening by applying security configuration baselines, disabling unused services, ports, and components, and strengthening access controls for all critical services.
Risk-Based Vulnerability Management	Establish a patching program that prioritizes remediation based on criticality and real-world exploitation evidence, rather than just CVSS scores.
Continuous Threat Intelligence	Regularly monitor cybercrime forums, vulnerability databases, CISA KEV listings, and threat actor chatter to identify active abuse and track both emerging threats and the long-term targeting of older flaws.
Streamline Patch Timelines	Reduce time-to-patch by streamlining internal testing and approval processes. Mandate rapid patching for internet-facing and widely deployed infrastructure, specifically targeting remote access solutions, firewall and switch operating systems, email clients, and network storage devices.
Implement Virtual Patching	Deploy Intrusion Prevention Systems (IPS) or Web Application Firewalls (WAF) to actively shield unpatched systems from exploitation until permanent software updates can be safely deployed.
Regular Security Assessments	Conduct frequent vulnerability scans and penetration testing to proactively uncover and remediate undisclosed weaknesses before threat actors can exploit them.

Exploitation Indicator Monitoring	Deploy advanced detection tools tuned to identify the specific behavioral patterns and indicators that suggest the active exploitation of known vulnerabilities.
Targeted IT Training	Train IT staff on the rapid identification and remediation of vulnerabilities, heavily emphasizing the necessity of long-term monitoring and defense against older, disclosed flaws that remain actively targeted by attackers.



Digital Sabotage: The Weaponization of Geopolitical Sentiment

Throughout 2025, hacktivism solidified its role as a persistent, geopolitically-driven hybrid threat, characterized by a high operational tempo and low technical barriers. No longer a mere nuisance, this threat layer saw groups converge with state-aligned interests and cybercriminal tactics to function as a durable instrument of low-cost pressure. Activity was dominated by high-volume Distributed Denial-of-Service (DDoS) campaigns designed to maximize psychological impact and narrative amplification. Crucially, the year was marked by a decisive shift in targeting, with hacktivists increasingly focusing on exposed industrial and operational technology (OT) environments, critical infrastructure, and public-facing civic services, demonstrating a capacity to impose operational, political, and informational effects disproportionate to their technical sophistication.

Tactically, 2025 confirmed the entrenchment of Telegram as the primary coordination and amplification platform for hacktivist ecosystems. Campaigns were increasingly organized through hashtags, alliances, and dissemination of post-facto claims, enabling near real-time mobilization and global reach. Some groups attempted to expand beyond disruption into ransomware and monetization models, as illustrated by CyberVolk's flawed VolkLocker RaaS effort, highlighting both the ambition and technical limitations present within much of the hacktivist landscape.

Throughout 2025, hacktivism evolved from predominantly symbolic disruption toward selective experimentation with OT and critical infrastructure. Pro-Russian collectives showed the most consistent progression in this direction, while the Israel–Iran cyber escalation, for example, illustrated how hacktivism now operates as a rapid-mobilization force multiplier during geopolitical crises - combining operational friction with narrative warfare.

Notable Hacktivist Attacks and Campaigns (2025)

Israel–Iran Cyber Escalation (June 2025)

The mid-June 2025 Israel–Iran escalation significantly boosted hacktivist activity, establishing cyberspace as a key conflict domain. Pro-Iranian, pro-Palestinian, and pro-Israeli groups launched intense campaigns, utilizing DDoS, data leaks, and influence operations in parallel with kinetic and political events.

These operations targeted critical sectors, including government, finance, telecom, academia, and infrastructure. While many claims were unverified, confirmed incidents caused service disruptions and heightened public anxiety. Notably, the fewer but more destructive pro-Israeli operations inflicted material damage, data loss, and financial disruption on Iranian infrastructure. This campaign demonstrates hacktivism's role as a low-cost force multiplier in modern conflict, imposing operational friction and psychological pressure, defined by narrative warfare and rapid alliance-building despite limited technical sophistication.

Denmark Water Utility Disruption (Public Attribution: December 2025)

Danish authorities publicly attributed a late 2024 disruptive water utility incident to the pro-Russian hacktivist group Z-Pentest, a pivotal disclosure in 2025 reporting. This operation, which caused localized service disruption and infrastructure damage, involved manipulating operational parameters like pump pressure, leading to burst pipes and remediation efforts affecting hundreds of homes. The case is a clear example of hacktivism evolving beyond symbolic DDoS attacks into tangible Operational Technology (OT) impact, heightening concerns over low-barrier access to exposed industrial systems.

TwoNet OT/ICS Targeting (September 2025)

In September 2025, the pro-Russian hacktivist group TwoNet claimed a compromise of a Dutch water facility. The target was actually a security honeypot, not an operational utility. Despite this, telemetry recorded OT-specific behaviors, including configuration changes and alarm suppression, mirroring real-world ICS intrusion techniques. This incident is significant because it demonstrates the hacktivist progression toward OT-aware tradecraft and experimentation with industrial environments, moving beyond purely IT-focused disruption, even though no actual utility was impacted.

NATO Summit Ecosystem DDoS (The Hague, June 23–24, 2025)

During the NATO Summit in The Hague, pro-Russian hacktivist actors, primarily NoName057(16), launched DDoS attacks against multiple Dutch municipalities and related organizations. Consistent with NoName057(16)'s established pattern, targets were chosen for their high visibility and symbolic value rather than for operational leverage. This campaign is a clear example of summit-driven hacktivism, focused on achieving high-visibility political signaling, media attention, and psychological impact, not technical compromise.

NoName057(16) Sustained DDoS Operations and International Takedown (July 2025)

Throughout 2025, the pro-Russian hacktivist group NoName057(16) executed persistent DDoS campaigns against European public-sector and infrastructure-adjacent targets. The group became the leading pro-Russian DDoS actor of the year by industrializing its operations using crowdsourced botnets and volunteer tooling. Despite an international law enforcement disruption operation (Operation Eastwood) in July targeting its infrastructure and operators, NoName057(16) proved to be the most operationally consistent hacktivist threat of 2025, demonstrating how loosely organized collectives can achieve persistent, large-scale impact.

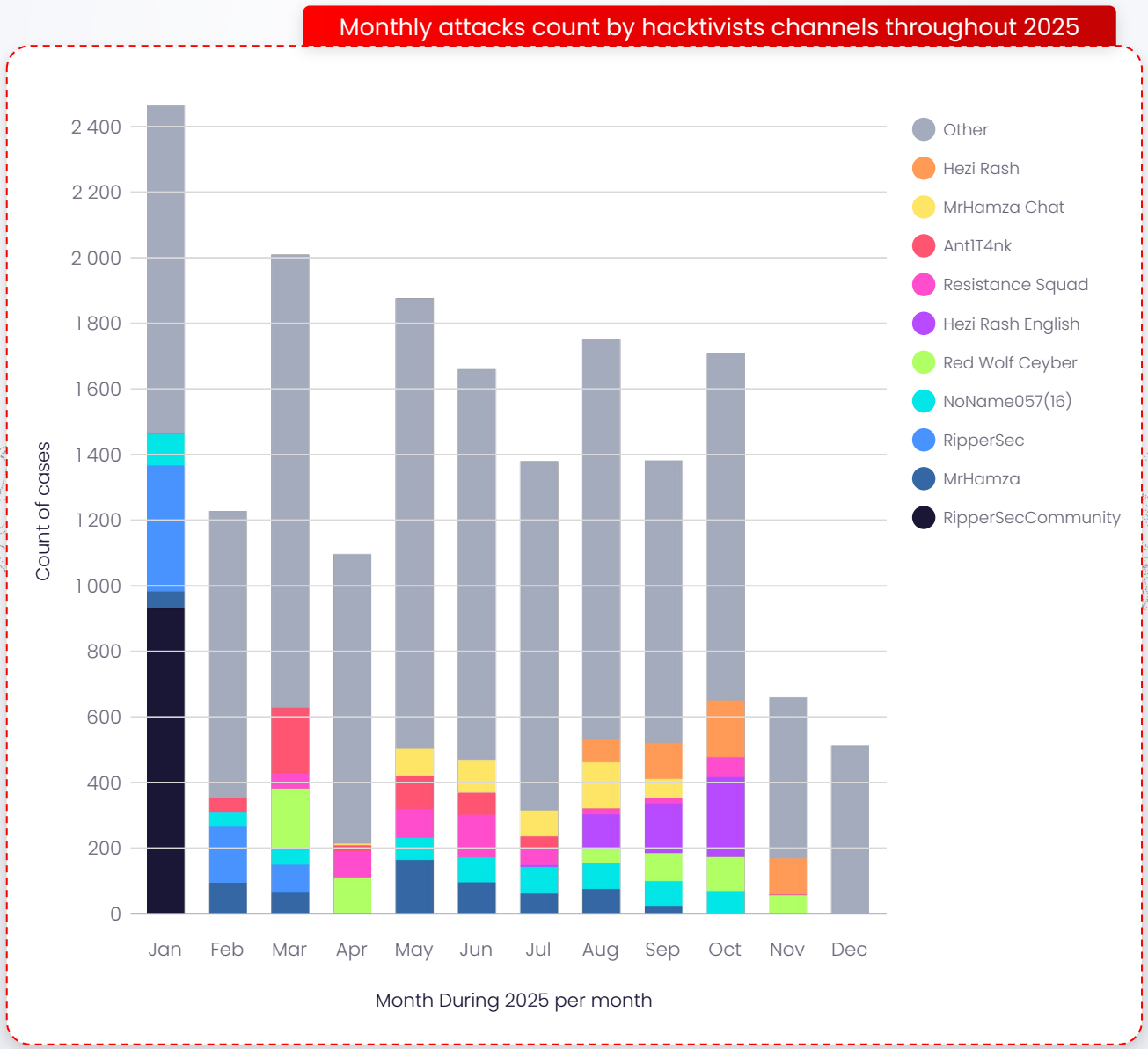
Opportunistic Pro-Russian Hacktivist OT Targeting (Trend Validation, Late 2025)

A joint advisory from late 2025 documented that pro-Russian hacktivist groups are conducting opportunistic intrusions into global Operational Technology (OT) environments, primarily by exploiting exposed remote-access services. These attacks involve exploiting unsecured VNC and using basic credential access to achieve limited but real interaction with industrial systems. This activity confirms a 2025 trend where hacktivist actors increasingly probe OT/ICS environments, significantly blurring the line between simple nuisance and genuine infrastructure risk.

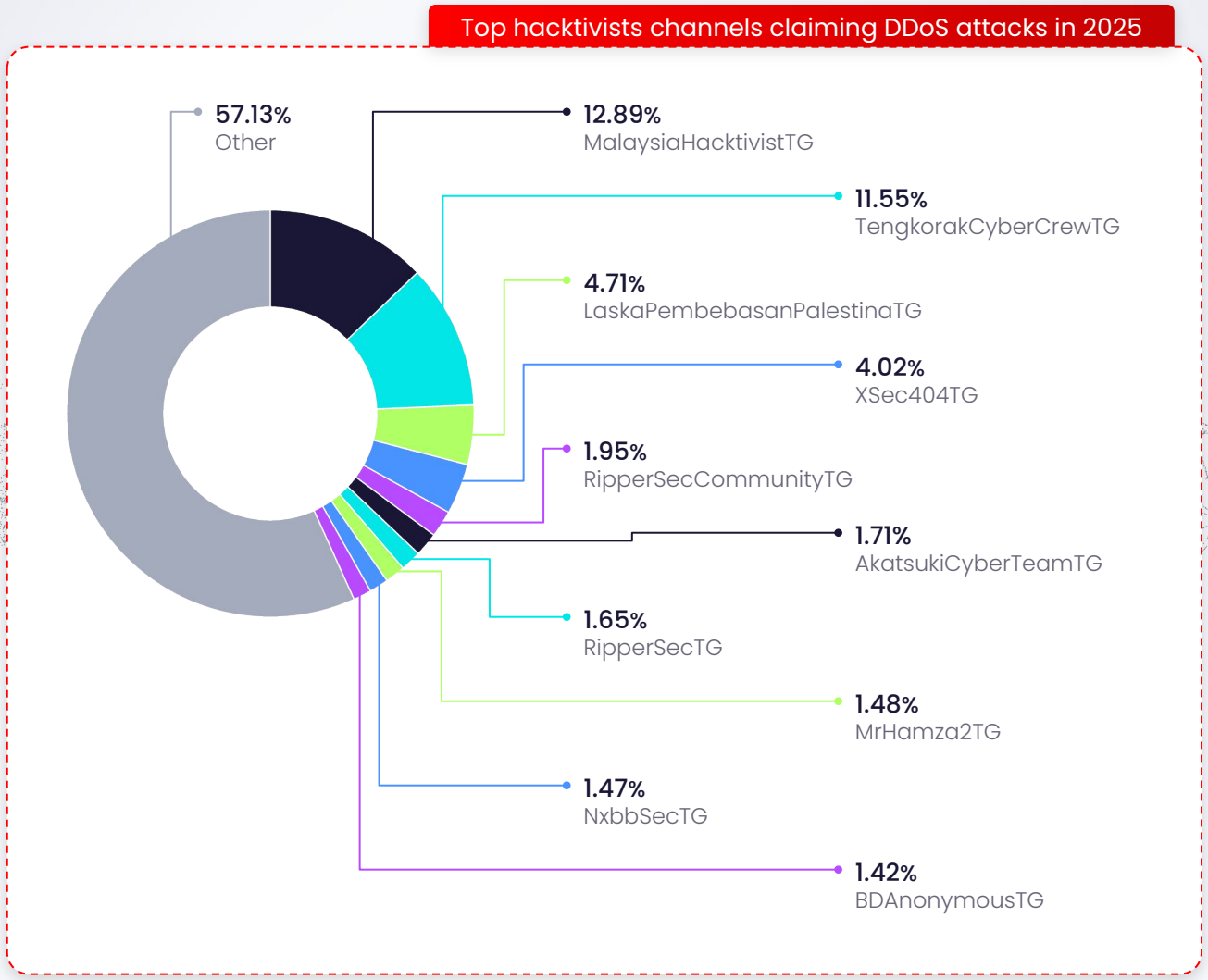
Statistics of Hacktivism in 2025

- In 2025, KELA added over 250 new hacktivist groups to its database, with over 500 notable groups active throughout the year, mostly from the Pro-Palestinian and Pro-Russian hacktivist sectors.
- KELA's data identified RipperSec (pro-Palestinian), Mr. Hamza (pro-Palestinian), NoName057(16) (pro-Russian), Red Wolf Cyber (pro-Palestinian), Hezi Rash (pro-Israeli), and Resistance Squad (pro-Palestinian) as among the most prominent hacktivist groups in 2025. These groups recorded the highest number of victim domains in their messages - a metric associated with claimed DDoS attacks, **website defacements, data theft, and related disruptive activity.**
- Around **3,500 DDoS attacks were claimed by top actors,** representing an increase of **approximately 400% compared to 2024.**

Monthly attacks count by hacktivists channels throughout 2025, based on the attacked websites accessibility reports provided as proof (based on KELA data lake):



Top hacktivists channels claiming DDoS attacks in 2025 (based on KELA data lake):



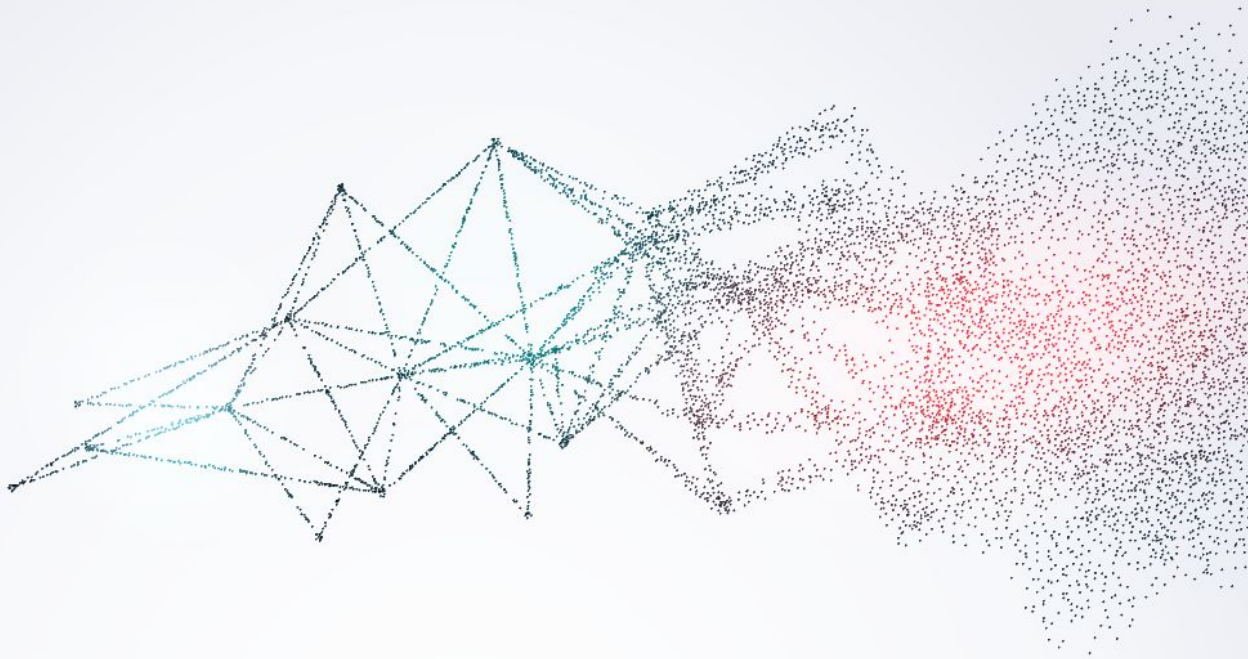
KELA's 2026 Predictions: Growth of Hacktivism

Based on patterns observed throughout 2025, hacktivist activity in 2026 is expected to further institutionalize as a persistent layer of hybrid conflict rather than episodic, protest-driven disruption. The normalization of high-tempo DDoS campaigns, expansion into exposed OT and ICS environments, and growing convergence between hacktivism, cybercrime tooling, and state-aligned narratives indicate that future operations will prioritize scalability, visibility, and deniability over technical novelty. Hacktivist alliances formed in 2025 - often transient but operationally effective - demonstrated an ability to rapidly mobilize around geopolitical flashpoints. This suggests that election cycles, military escalations, and diplomatic crises will continue to trigger synchronized, multi-actor campaigns across regions.

Looking ahead to 2026, KELA assesses that ideologically motivated hacktivists will increasingly adopt ransomware, wiper-style malware, and access-based intrusions to target under-secured critical infrastructure and public-sector organizations. While most of these actors lack nation-state sophistication, the leverage of publicly available tooling, leaked credentials, and AI-assisted automation will further lower barriers to entry, driving higher attack volumes and greater operational ambition. As their capacity to impose real-world friction continues to rise - particularly during geopolitical crises - organizations must treat hacktivism not as peripheral noise, but as a persistent threat layer demanding proactive intelligence, resilient infrastructure, and coordinated response frameworks.

Countermeasures

Leverage cyber threat intelligence (CTI)	Monitor Telegram and underground chats for specific operational indicators (e.g., target lists, tool distribution) rather than relying on generic sentiment tracking.
Geopolitical Monitoring	Track global events that typically trigger hacktivist activity to proactively scale defenses during high-risk periods.
Attribution Capabilities	Partner with CTI providers and law enforcement to distinguish genuine hacktivists from state-sponsored APTs, enabling appropriate defensive, legal, and diplomatic responses.
OT/ICS Hygiene	Address basic access failures by securing remote access, eliminating default credentials, accelerating patching, and hardening internet-facing assets.
Data Protection	Enforce strict access controls and encrypt sensitive data at rest and in transit to minimize exfiltration risks.
Scalable DDoS Defense	Deploy real-time, highly scalable DDoS protection to absorb sustained, multi-source traffic spikes—an absolute necessity for public sector, telecom, and utility enterprises.
Counter-AI Tools	Implement specialized defenses to detect and block AI-generated threats, such as automated phishing, fake personas, and adversarial AI attacks.
Tailored Playbooks	Develop and maintain scenario-specific response plans for ransomware, data theft, and DDoS, focusing on rapid containment.
Crisis Communication	Issue rapid, verified, and transparent stakeholder communications to counter psychological impacts, limit narrative amplification, and reduce uncertainty.
Collaborative Takedowns	Engage in international and cross-sector partnerships to degrade hacktivist infrastructure, targeting their hosting services, C2 channels, and monetization pathways.



The Geopolitical Offensive: APTs and Influence Operations in 2025

In 2025, major geopolitical flashpoints directly translated into sustained, state-backed cyber campaigns, confirming cyber operations as a core instrument of national power rather than a supporting capability. Conflicts involving Russia-Ukraine, Israel-Iran, U.S.-China strategic rivalry, cross-Strait tensions, and North Korea's sanctions-driven posture all featured persistent cyber activity spanning espionage, disruption, influence operations, and revenue generation. State-aligned APTs, proxy actors, and hacktivist collectives operated in parallel with kinetic and diplomatic pressure, targeting critical infrastructure, defense and technology supply chains, financial systems, and democratic processes.

Across these theaters, 2025 highlighted three defining trends: the normalization of cyber operations as part of hybrid warfare, the deepening entanglement between state intelligence services and commercial cyber ecosystems, and the increasing use of financially motivated cybercrime to fund national objectives. The convergence of espionage, influence, and monetization, combined with growing exposure of state-linked cyber capabilities through leaks and public attributions, underscores a global environment where cyber risk is inseparable from geopolitical instability.

Major Events Triggered State-Backed Cyber Campaigns

Russia - Ukraine War: Persistent Cyber Conflict

Throughout 2025, the cyber dimension of the Russia-Ukraine war has remained highly active as digital operations became an integral complement to kinetic conflict. Western allies including the U.K., U.S., France, and Germany issued joint advisories warning that Russian military intelligence has been targeting Western logistics, defense, IT services, and critical infrastructure in support of Russia's war efforts - part of broader attempts to weaken Ukraine's allies and military support networks.[38]

Russian-linked groups such as APT28[39] (also tracked as Fancy Bear), COLDRIVER (also tracked as Callisto)[40] and Sandworm[41] have been associated with espionage and destructive attacks against Western and Ukrainian governments, energy, and logistics sectors, including data wipers against economic infrastructure like the grain sector - a strategic target given Ukraine's export role. Ukraine and other countries' volunteer hacktivist collectives (e.g., IT Army of Ukraine and Cyber Partisans[42]) have responded with offensive cyber operations against Russian targets, from infrastructure disruption to data exfiltration, highlighting the two-sided nature of cyber war in this conflict.

Israel - Iran Strategic Escalation: Hybrid Cyber Warfare

The broader Israel-Iran confrontation in 2025 has rapidly evolved into hybrid warfare, where digital operations are used to complement, and sometimes compensate for, kinetic limitations. Shortly after Israeli airstrikes on Iranian strategic targets in June 2025, an Israeli hacker group known as Predatory Sparrow claimed attacks, allegedly disrupting financial operations and destroying digital assets tied to Iran's strategic ecosystem.

Iranian actors - including APT34 (OilRig), APT35 (Charming Kitten)[43], APT39 (Remix Kitten)[44], and MuddyWater[45] - have been observed staging phishing campaigns, fake alert messages, and DDoS attacks against Israeli and other political rival's infrastructure as part of psychological and digital pressure tactics. These operations have employed both technical and social engineering approaches aimed at eroding trust and sowing confusion. It is worth noting that in the escalating Israel - Iran conflict, both cyber espionage and disruptive operations are being leveraged, with Israel targeting financial and state networks and Iran deploying broader hybrid cyber tactics.

[38] Russian GRU Targeting Western Logistics Entities and Technology Companies | CISA

[39] Dark Web Profile: APT28

[40] Threat Advisory: COLDRIVER

[41] APT Activity Report: Russia-Aligned APTs Ramp Up Attacks Against Ukraine and its Strategic Partners (April 2025 – September 2025)

[42] TTPs of Cyber Partisans Activity Aimed at Espionage and Disruption

[43] Educated Manticore Reemerges: Iranian Spear-Phishing Campaign Targeting High-Profile Figures - Check Point Blog

[44] The Amnban Files: Inside Iran's Cyber-Espionage Factory Targeting Global Airlines - Nariman Gharib

[45] MuddyWater: Snakes by the riverbank

Heightened U.S.-China Strategic and Economic Tensions

Geopolitical tensions between the U.S. and China in 2025, driven by disputes over advanced technology, export controls, and military posturing, have coincided with intensified cyber operations on both sides. Chinese state-aligned threat actors such as Volt Typhoon[46], APT41 (Winnti)[47], APT31 (Zirconium)[48], Mustang Panda (APT10)[49], and Salt Typhoon[50] have been linked by Western intelligence and cybersecurity agencies to sustained espionage campaigns targeting U.S. defense contractors, semiconductor manufacturers, telecommunications providers, and high-technology research institutions. These operations have reportedly focused on intellectual property theft, strategic intelligence collection, and long-term pre-positioning within critical infrastructure and research environments.

At the same time, Chinese government agencies and domestic cybersecurity firms have published reports accusing U.S.-aligned intelligence services, including the NSA and CIA, of conducting cyber espionage against Chinese telecommunications networks, universities, and aerospace and defense research entities. Beijing has framed these activities as evidence of reciprocal cyber pressure and persistent foreign intelligence collection targeting China's strategic industries.[51] [52]

The U.S. - China strategic rivalry continues to fuel asymmetric cyber operations centered on economic and technological dominance, with both espionage and influence tactics in play.

Taiwan Strait Pressures and Post-Election Cyber Activity

Rising tensions across the Taiwan strait, especially around Taiwan's elections and increasing military pressure, drove a marked escalation in cyber operations in 2025, with Taiwan's National Security Bureau (NSB) reporting an average of 2.6 million daily cyberattacks attributed to China-linked threat actors targeting government systems, critical infrastructure, energy networks, healthcare, and telecommunications throughout the year.[53]

The NSB[54] identified multiple China-aligned hacking groups as active in these campaigns, including BlackTech (Circuit Panda / Canary Typhoon), Flax Typhoon (Ethereal Panda), Mustang Panda, APT41 (Brass Typhoon), and UNC3886, which employed tactics such as hardware/software exploitation, distributed denial-of-service (DDoS), social engineering, and supply-chain attacks across key sectors. Taiwanese cyber defense authorities, supported by allied information-sharing with partners such as the U.S. and Japan[55], have emphasized resilience measures, including enhanced counter-phishing training, network segmentation, and rapid incident response, while publicly highlighting disinformation campaigns and 'grey-zone' activity linked to China's broader political pressure strategy.

[46] Dragos Littleton Electric Water Case Study

[47] Going Underground: China-aligned TA415 Conducts U.S.-China Economic Relations Targeting Using VS Code Remote Tunnels | Proofpoint US

[48] Disrupting active exploitation of on-premises SharePoint vulnerabilities | Microsoft Security Blog

[49] LOTUSLITE: Targeted espionage leveraging geopolitical themes

[50] China-linked Actors Maintain Focus on Organizations Influencing U.S. Policy | SECURITY.COM

[51] Source

[52] China Says It Found Evidence of US Cyber Attack on State Agency - Bloomberg

[53] China launched 2.63 million daily cyberattacks against Taiwan in 2025: NSB

[54] NSB — 國家安全局National Security Bureau

[55] Japanese government adopts new cybersecurity strategy - The Japan Times

Overall, in 2025, cross-Strait tensions were reinforced by a dense cyber ecosystem combining state-aligned APT operations, election-adjacent influence activity, and exposure of China's cyber-industrial base through dark web leaks, underscoring how cyber operations, commercial entities, and state interests are increasingly intertwined in the Taiwan Strait confrontation.

North Korea's Ongoing Cryptocurrency and Revenue-Generation Operations

In 2025, North Korea continued to intensify revenue-driven cyber operations, blending long-standing espionage tradecraft with financially motivated intrusions aimed at cryptocurrency and blockchain ecosystems. The Lazarus Group[56], along with TraderTraitor[57] and Kimsuky[58], remained central to this activity. A landmark event was the FBI's public attribution of the USD 1.5 billion ByBit cryptocurrency exchange theft to North Korean state-linked hackers[59], emphasising Pyongyang's reliance on cybercrime to offset international sanctions and fund strategic programs.

Alongside high-value exchange compromises, North Korean operators expanded the 'Contagious Interview' campaign throughout 2025, targeting software developers, Web3 engineers, and cryptocurrency professionals[60]. Attributed primarily to Lazarus-linked infrastructure, the campaign relies on fake job offers and recruiter impersonation across platforms such as LinkedIn and GitHub, luring victims into downloading trojanized interview tasks, malicious repositories, or developer tools. These payloads, often identified as BeaverTail, InvisibleFerret, or related malware, enable credential theft, wallet compromise, and persistent access to corporate environments. It is worth noting that complexity of such campaigns grows, including fake interview portals, ClickFix[61]-style social engineering, and abuse of legitimate developer platforms to evade detection.

Overall, North Korea's 2025 cyber posture reflects a mature hybrid strategy, where traditional intelligence collection, social-engineering-driven developer compromise, and large-scale cryptocurrency theft operate in parallel.

2025 has shown that cyber conflict is no longer peripheral to geopolitical competition - it is central. Nation-state cyber campaigns have moved beyond isolated espionage to sustained operations that directly reflect kinetic tensions, economic rivalries, and strategic competition. From large-scale cryptocurrency thefts by North Korean actors to hybrid cyber offensives in the Middle East and Russia-Ukraine theater, state-backed malware, phishing, influence campaigns, and infrastructure probing continue to shape the cyber risk landscape globally.

[56] How North Korea-Backed Lazarus Group Is Weaponizing Open Source to Target Developers

[57] Slow Pisces Targets Developers With Coding Challenges and Introduces New Customized Python Malware

[58] North Korean Kimsuky Actors Leverage Malicious QR Codes in Spearphishing Campaigns Targeting U.S. Entities

[59] North Korea Responsible for $1.5 Billion Bybit Hack — FBI

[60] Threat Actors Expand Abuse of Microsoft Visual Studio Code

[61] From Contagious to ClickFake Interview: Lazarus leveraging the ClickFix tactic

KELA's 2025 Insights: Spotlight on Hybrid Warfare and Cyber-Industrial Exposure

Israel - Iran Escalation Drives Overt Cyber Disruption and Hacktivist Alignment

In 2025, the Israel-Iran confrontation visibly crossed into overt cyber disruption, with operations closely synchronized to kinetic events. Shortly after Israeli airstrikes on Iranian strategic targets in June, the pro-Israel hacktivist group Predatory Sparrow (Gonjeshke Darande) claimed destructive attacks against Iran's Bank Sepah and the Nobitex cryptocurrency exchange, alleging data destruction and financial disruption tied to institutions accused of supporting the IRGC and sanctions evasion. Iranian state media, including FARS, confirmed service outages affecting banking operations and gas stations nationwide, while Israeli sources circulated videos corroborating real-world impact. Although some claims appeared via affiliated or satellite channels rather than Predatory Sparrow's official Telegram presence, concurrent activity, such as the posting of allegedly stolen Iranian parliamentary documents and hints referencing the Tehran Stock Exchange, suggests a coordinated campaign blending disruption, signaling, and psychological pressure.

Exposure of China's Cyber-Industrial Ecosystem through Dark Web Leaks

Adding a new dimension to state-linked cyber activity in 2025, KELA identified multiple dark web leak events that potentially expose the intersection between Chinese APT operations, commercial cybersecurity firms, and state institutions. In May, two separate listings on DarkForums drew attention: actor IronTooth claimed to sell internal documents from VenusTech, a major Chinese cybersecurity company, while ChinaBob offered data allegedly originating from Salt Typhoon, a state-linked advanced threat group. Both actors shared sample materials and asserted that the datasets were sold within days. KELA conducted document analysis, open-source corroboration, and technical network traffic review of infrastructure allegedly linked to Salt Typhoon, consolidating recovered materials into an internal analytical appendix.

This trend intensified in late October 2025 with the appearance of a large dataset allegedly belonging to Knownsec Information Technology Co., Ltd., one of China's most prominent cybersecurity firms. The leak, reportedly exceeding 12,000 files and primarily dated to 2023, was offered for sale by an actor known as T1g3r and later claimed to have been sold to a single buyer. KELA's review of shared samples suggests that, if authentic, the materials provide rare visibility into Knownsec's alleged cooperation with Chinese state bodies, including the Ministry of Public Security, alongside internal tooling, reconnaissance databases spanning 26 countries, and references to personnel linked to historically documented Chinese APT activity. Collectively, these leaks underscore how China's cyber-industrial base - long opaque - has become an increasingly exposed and contested element of global cyber power in 2025.

KELA's 2026 Predictions: Geopolitical Conflict and AI as Key Drivers of APT Activity

In 2026, APT activity is expected to expand geographically, with Central Asia emerging as a higher-risk region due to its strategic position between Russia, China, and the Middle East and its growing role in energy and logistics corridors. Central Asia is likely to face increased espionage, pre-positioning, and influence operations, particularly against government, telecommunications, and critical infrastructure, as major powers compete for regional leverage.

Beyond geographic expansion, APT groups will also deepen their use of AI and large language models, especially for spearphishing, social engineering, reconnaissance, and content generation. LLM-assisted lures, automated victim profiling, and adaptive malware development will further reduce operational costs while increasing scale and plausibility, accelerating the pace and reach of state-aligned campaigns.

Furthermore, APT groups will further expand their integration of AI beyond content generation into semi-autonomous and 'agentic' systems capable of executing tasks directly within compromised environments. The emergence of ecosystems such as OpenClaw, assessed in KELA's recent Threat Assessment of the OpenClaw Ecosystem report, illustrates how Local-First AI agents with system-level execution capabilities could significantly expand attacker persistence, adaptive decision-making, and lateral movement. Early indications, including reporting on suspected Chinese APT experimentation with commercial LLM platforms such as Claude, suggest that state-aligned actors are already exploring operational use of advanced AI tools. As these capabilities mature, AI-enabled automation is likely to enhance reconnaissance, privilege escalation, and real-time social engineering, further accelerating the scale, complexity, and resilience of nation-state cyber campaigns.

Looking ahead, APT activity will remain tightly aligned with geopolitical tensions and emerging conflicts, with cyber operations increasingly used as a flexible tool alongside diplomatic, economic, and military pressure in flashpoints involving Iran, the Arctic/Greenland region, and the Americas.

Finally, North Korean actors are expected to continue prioritizing Web3 and developer ecosystems, building on campaigns like Contagious Interview to steal credentials, compromise wallets, and infiltrate software supply chains. More broadly, APT activity will remain tightly aligned with geopolitical tensions and emerging conflicts, with cyber operations increasingly used as a flexible tool alongside diplomatic, economic, and military pressure in flashpoints involving Iran, the Arctic/Greenland region, and the Americas.

Countermeasures

Align cyber posture with geopolitical exposure	Continuously map your digital footprint against 2025/2026 geopolitical flashpoints, specifically monitoring Central Asia, energy and logistics corridors, Taiwan Strait supply chains, and Web3 ecosystems.
Intelligence-Led Scenario Planning	Combine geopolitical intelligence with standard CTI to anticipate shifts before technical indicators emerge. Conduct tabletop exercises tied to specific actors (e.g., China-aligned pre-positioning, North Korean crypto operators, Iran-linked disruption) to simulate destructive critical infrastructure attacks, election influence operations, and sanctions-driven crypto theft.
Defend Against 'Contagious Interview' Tactics	Counter North Korea's developer-focused infiltration by enforcing strict identity verification and MFA for all contractors and freelancers. Mandate formal vetting (verification calls, sandboxed technical assessments) for candidates sourced via LinkedIn, GitHub, or Web3 communities.
Secure Code Environments	Require isolated execution environments for candidate-submitted code and interview tasks to prevent malware deployment (e.g., BeaverTail, InvisibleFerret). Actively monitor GitHub and CI/CD pipelines for anomalous package uploads or dependency changes.
Zero Trust & Identity Controls	Apply Zero Trust principles across cloud, developer, and SaaS environments. Enforce phishing-resistant MFA (FIDO2/WebAuthn) for privileged accounts, and implement strict session/token lifecycle management with automated revocation for suspicious activity.
Counter AI-Assisted Social Engineering	Shift from looking for linguistic errors to monitoring behavioral anomalies, using advanced tools to detect high-coherence, LLM-generated lures. Train employees to identify hyper-personalized recruitment scams and AI-enhanced impersonation attempts.

Detect Living-off-the-Land (LotL) Abuse	Counter low-noise, persistence-focused techniques by expanding behavioral monitoring of native tools (PowerShell, WMI, admin utilities). Deploy anomaly-based EDR/NDR and establish proactive threat-hunting programs focused on long dwell-time indicators.
Harden Edge Devices	Prevent router and edge-device pre-positioning by accelerating patch cycles for VPN gateways and firewalls. Segment management interfaces, restrict the internet exposure of critical network appliances, and conduct regular penetration testing.
Rehearse Hybrid Incident Response	Critical sectors (infrastructure, finance, energy, telecom, supply chains) must simulate coordinated cyber disruption combined with disinformation campaigns. Prepare for data leaks aimed at psychological impact rather than financial extortion, and establish predefined communication channels with government agencies and ISACs.
Geopolitically Aware Vendor Vetting	Perform enhanced due diligence on MSSPs and tech providers operating in sensitive jurisdictions, particularly in light of exposure within China's cyber-industrial ecosystem (e.g., VenusTech, Knownsec). Shift to continuous third-party risk monitoring and strictly review contractual obligations for data access, logging transparency, and subcontractor disclosure.
Influence & Narrative Control	Develop coordinated communication strategies to counter hacktivist claims, false narratives, and information operations. Actively monitor dark web and social channels for early warnings of reputational targeting or leak campaigns.

The Collapse of Trust: 2025's Supply Chain Exploitation

Supply chain attacks have evolved from a niche threat into a primary and highly efficient vector for cybercriminals. By targeting the intricate web of trust between organizations and their software suppliers, threat actors are developing methods for achieving maximum impact with minimal effort. This approach has proven devastatingly effective, making a comprehensive understanding of the supply chain threat landscape essential for modern cybersecurity.

The core strategic advantage of this vector for threat actors lies in its efficiency. Instead of laboriously breaching each target individually, a single compromised vendor be it a software vendor, a managed service provider (MSP), a cloud integration, or an open-source library - can result in multiple downstream businesses suffering a data breach. This allows attackers to compromise many targets from a single point of entry, perfectly aligning with their goal of maximizing impact. This vector weaponizes the very mechanisms designed to maintain security and functionality, such as software updates, continuous integration/continuous deployment (CI/CD) pipelines, and trusted third-party integrations. Additionally, vendors often require access to private data to integrate their services, creating a shared pool of data that can be compromised if the vendor is breached.[62]

Campaigns observed throughout 2025 have demonstrated that trust is the new vulnerability. The 'Trust by Default' model, where signed components and verified vendors are implicitly trusted by security controls, has become a significant blind spot. From the mass exploitation of enterprise resource planning (ERP) systems to the abuse of widely used marketing tools, attackers have demonstrated a nuanced understanding of the modern digital mesh. Hackers are not just hacking code; they are hacking the web of identities, tokens, and relationships that connect the global digital economy together.[63]

[62] Software Supply Chain Attacks Risk on the Rise | Ivanti

[63] The Growing Risk of Supply Chain Attacks in 2025

Trends in Supply Chain Attacks

While no drastically new trends have emerged during the year 2025, some that appeared in previous years have crystallized into more sophisticated methods and led to significant escalations regarding the technical scale and economic impact of the attacks observed.[64] Following are notable observed types of supply chain attacks:

Upstream Server Attacks:

Compromising an upstream system, such as a code repository, to inject a malicious payload that then spreads to downstream users via legitimate software updates.

SaaS-to-SaaS (OAuth) Compromise:

Abusing the web of trust and permissions between integrated Software-as-a-Service (SaaS) applications, leveraging a vendor's authorized access to pivot into customer environments.

CI/CD Infrastructure Attacks:

Targeting automated development and deployment pipelines to inject malware, steal high-value secrets, or trojanize build artifacts that are then shipped to customers.

Dependency Confusion and Typosquatting:

Deceiving developers or automated systems into downloading compromised software packages from public repositories by using names similar to legitimate internal libraries or popular open-source projects.

[64] Software Supply Chain Attacks Risk on the Rise | Ivanti

Major Case Studies Observed in 2025

Case Study

The Salesloft Drift SaaS-to-SaaS Compromise

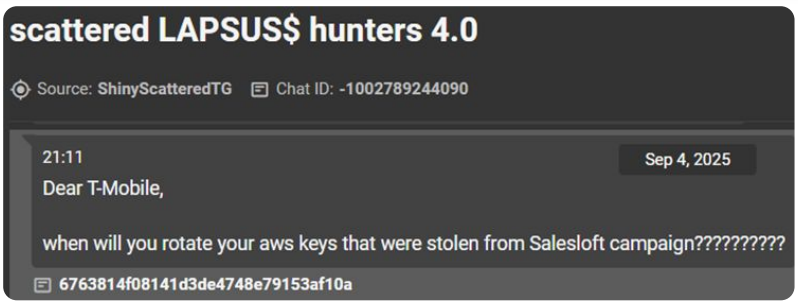
This incident exemplifies a multi-stage SaaS supply chain compromise that exploited the trusted connection between integrated cloud platforms. The attack unfolded in a clear sequence: a threat actor first compromised the Salesloft platform, from which they stole OAuth and refresh tokens belonging to the integrated Drift chat agent.

Between August 8 and August 18, 2025, the attacker used these stolen tokens to pivot directly into the Salesforce environments of Drift's customers. Because the tokens were from a trusted, pre-authorized application, this access bypassed conventional security measures. Post-exploitation, the actor used Salesforce Object Query Language (SOQL) to systematically hunt for embedded secrets, running queries with keywords such as AKIA (the AWS access key prefix), Snowflake, password, and secret against support cases.

Researchers have attributed this specific activity to a newly identified cluster tracked as UNC6395.[65] While the ShinyHunters nexus publicly claimed responsibility for the campaign on their Telegram channel, these claims remain unsubstantiated for this specific set of activities.

The breach impacted numerous high-profile organizations, with publicly confirmed victims including Cloudflare, Palo Alto Networks, CyberArk, Tenable, and Zscaler. The victim list encompasses many big names of the cybersecurity industry, underscoring the systemic risk inherent in the SaaS supply chain; even the most sophisticated security vendors are exposed through the trust they place in their own third-party suppliers. The scope of data exposure primarily included business contact information and support case data.

Screenshot from the group's Telegram channel claiming to have stolen T-Mobile's AWS keys as a result of a compromise of Salesloft Drift | KELA's Threat Intelligence platform



However, in instances where employees had stored sensitive credentials in support tickets, the breach also exposed valuable API tokens and other secrets, demonstrating how a single vendor compromise can cascade into widespread, multi-organizational data exposure.

[65] Widespread Data Theft Targets Salesforce Instances via Salesloft Drift | Google Cloud Blog

Case Study

Salesforce Social Engineering Campaign

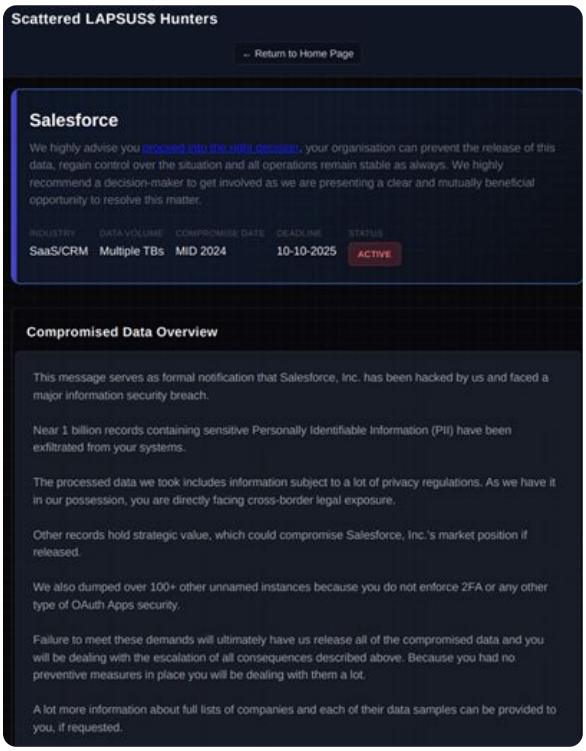
This campaign demonstrates a highly effective, human-focused approach to bypassing technical controls. A threat actor collective conducted a widespread campaign targeting corporate cloud environments, with a particular focus on Salesforce, using a combination of voice phishing (vishing) and social engineering.

Attackers would initiate a vishing call to a targeted employee, convincingly impersonating a member of the organization's IT support team. During the call, they guided the employee to navigate to Salesforce's legitimate connected app setup page. There, the employee was instructed to authorize a new third-party OAuth application, given a benign name like 'My Ticket Portal,' which was controlled by the attackers.[66]

The campaign is attributed to a loose collective involving members of Lapsus, ShinyHunters and ScatteredSpider, who used a public Telegram channel named ScatteredLAPSUS Hunters to claim responsibility for attacks, shame victims, and leak stolen data.

By tricking an employee into granting OAuth consent, the attackers gained persistent, API-level access to the organization's Salesforce environment. This token-based access completely bypassed multi-factor authentication (MFA) and other traditional authentication controls, providing the adversary with a durable backdoor to exfiltrate sensitive Customer Relationship Management (CRM) data.

Scattered LAPSUS$ Hunters' DLS, listing Salesforce as a victim and threatening to leak its data, October 2025



[66] The Cost of a Call: From Voice Phishing to Data Extortion | Google Cloud Blog

Case Study

Cl0p's Oracle E-Business Suite Extortion Campaign

This campaign highlights the continued success of leveraging zero-day exploits for mass data theft and extortion. The threat actor exploited CVE-2025-61882 in Oracle E-Business Suite (EBS) as a zero-day vulnerability as early as August 9, 2025, weeks before a patch was available. The attack was complex, with researchers noting that multiple distinct exploit chains were used, making precise vulnerability attribution challenging.

This initial exploitation was followed by a large-scale extortion campaign that began on September 29, 2025. The actor sent a high volume of emails to executives at victim organizations, alleging the theft of sensitive data from their EBS environments and demanding payment to prevent its release.[67]

The actor claimed affiliation with the Cl0p extortion brand and used contact email addresses previously listed on the Cl0p data leak site. The campaign also showed strong TTP overlaps with the FIN11 threat group, including the use of the GOLDVEIN.JAVA downloader and the operational model of mass-exploiting zero-days in widely used enterprise software.

This operation represents a continuation of a highly efficient and impactful model. By targeting public-facing enterprise applications with zero-day exploits, threat actors can exfiltrate significant amounts of data from numerous organizations without alerting defenders. This approach increases the efficiency of their data theft operations and almost certainly increases the overall impact of their extortion campaigns.

[67] Oracle E-Business Suite Zero-Day Exploited in Widespread Extortion Campaign | Google Cloud Blog

Case Study

npm supply chain compromise and the S1ngularityNX case

In September 2025, threat actors compromised the high-profile npm maintainer account 'qix' using phishing and session hijacking. This breach allowed them to inject malicious code into universally relied-upon packages: 'debug,' 'chalk,' and 'ansi-styles.' Due to millions of weekly downloads, this compromise immediately affected the software supply chain, impacting developers and CI/CD pipelines.

The compromised packages served as delivery vehicles for a malware framework identified as S1ngularityNX, which introduced a highly aggressive worm component named Shai-Hulud. Unlike traditional supply chain attacks that rely on static payloads, Shai-Hulud was designed to be self-propagating. It actively harvested npm tokens and GitHub credentials from infected developer environments and build servers. The malware used these stolen secrets to automatically authenticate and publish malicious package versions through the compromised maintainer's registry account, thereby automating the infection's spread.[68]

This mechanism transformed the incident from a standard repository breach into a fully wormable supply-chain compromise. By embedding itself into the build processes of downstream users, the malware created a cycle of infection where every compromised machine became a potential vector for further propagation. The attack not only harvested sensitive credentials but used them to continue spreading through the entire chain, affecting both individual developers and enterprise-grade build servers that trusted the legitimacy of the code-signing and release processes associated with the hijacked account.

Subsequent research in late November 2025 revealed the S1ngularityNX campaign persisted beyond the initial incident with a new, resilient variant dubbed Shai-Hulud 2.0. This variant reactivated stolen npm tokens weeks later, successfully reinfecting restored libraries and compromising adjacent maintainers, confirming the attackers maintained a long-term ecosystem foothold. The 2.0 variant showed advanced capabilities, expanding secret-harvesting, using delayed execution for evasion, and automating full npm account takeover. These developments indicated the S1ngularityNX campaign was a persistent, wormable, ecosystem-wide threat exploiting public registries' interconnected nature.[69] [70]

[68] Widespread Supply Chain Compromise Impacting npm Ecosystem | CISA

[69] 'Shai-Hulud' Worm Compromises npm Ecosystem in Supply Chain Attack (Updated November 26)

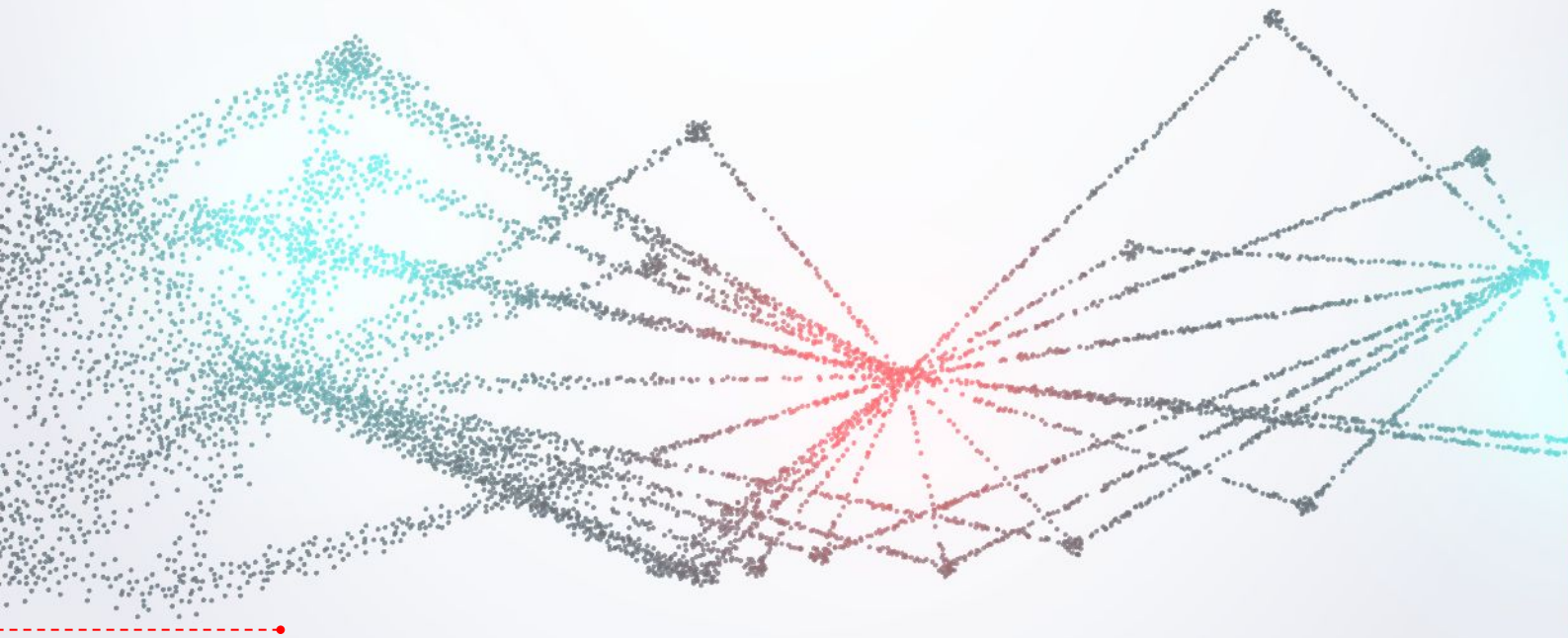
[70] Sha1-Hulud 2.0 Supply Chain Attack: 25K+ Repos Exposed | Wiz Blog

KELA's 2026 Predictions of The Supply Chain Threat Landscape

Based on the demonstrated success of the Oracle EBS campaign and similar operations, it is highly probable that CL0P-affiliated actors and other sophisticated groups will continue to dedicate significant resources to acquiring and exploiting zero-day vulnerabilities. Their focus will likely remain on widely used, public-facing enterprise applications that store sensitive data, as this model allows for efficient, large-scale data theft and subsequent extortion with a high return on investment.[71]

Furthermore, following the blueprint of the Salesloft Drift campaign, threat actors are likely to increasingly target the web of trust between interconnected SaaS platforms. Abusing trusted OAuth and API integrations will become a significant vector to bypass perimeter defenses, MFA, and IP-based restrictions. As organizations deepen their reliance on an ecosystem of integrated cloud services, attackers will focus on compromising a single vendor to gain trusted, API-level access to dozens or hundreds of downstream customers.[72]

Consequently, the financial consequences of supply chain attacks will continue to grow significantly. The prediction from Cybersecurity Ventures - projecting that the global annual cost will rise from $60 billion in 2025 to $138 billion by 2031 - indicates a sustained and costly trend. This growth will be driven by increased remediation costs, larger regulatory fines, higher ransom demands, and the cascading operational disruptions that affect entire ecosystems of interconnected businesses.[73]



[71] Google Cloud Security's Cybersecurity Forecast 2026

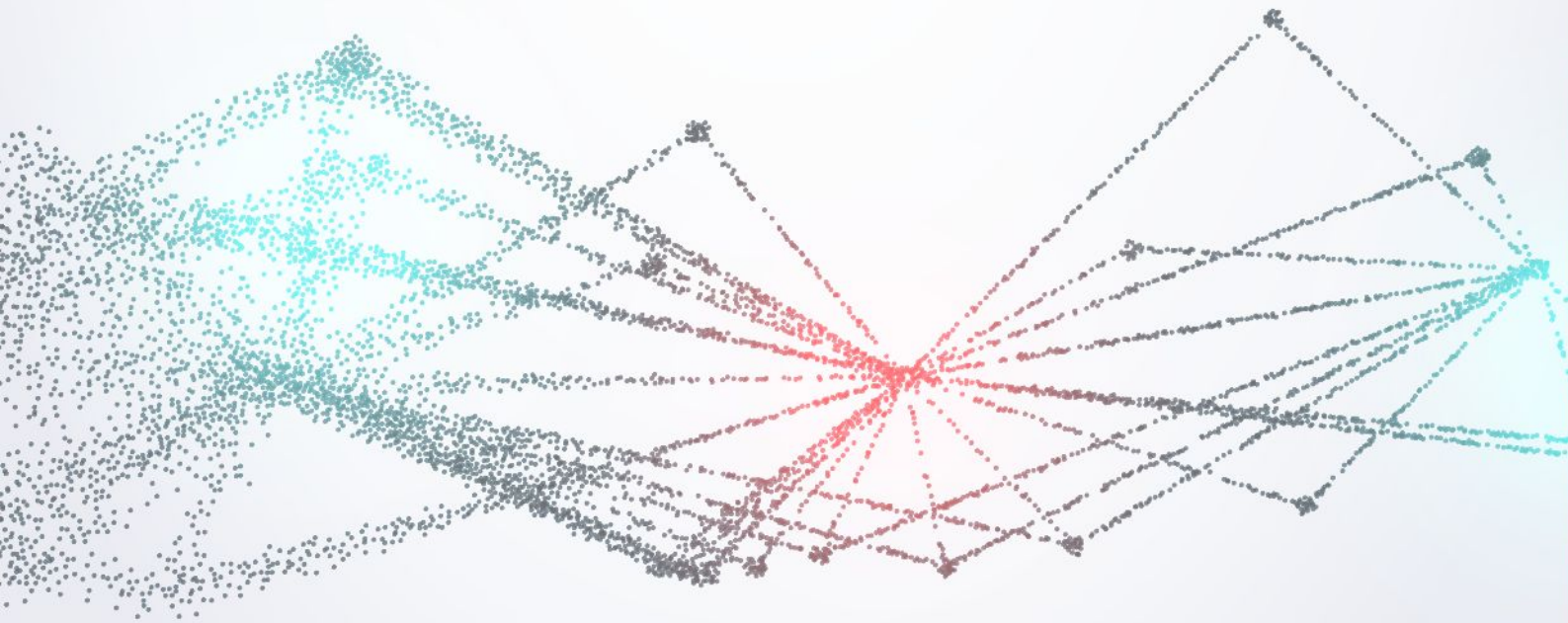
[72] Cybersecurity Threats in 2026: What to Expect? - DIESEC

[73] Software Supply Chain Attacks Risk on the Rise | Ivanti

Countermeasures

Comprehensive Due Diligence	Mandate security assessment questionnaires (SAQs), verify certifications (ISO 27001, SOC 2), and require mature incident response and vulnerability disclosure policies during vendor onboarding.
Visibility & Continuous Monitoring	Require a Software Bill of Materials (SBOM) from critical vendors. Supplement point-in-time assessments with continuous threat intelligence monitoring to detect external indicators of compromise, such as dark web credential leaks.
Immutable Dependencies	Pin all dependencies - including GitHub Actions - to their full, immutable commit hashes to prevent the automatic ingestion of malicious updates.
Ephemeral Credentials & Code Integrity	Eliminate long-lived static secrets by adopting federated identity (e.g., OIDC) for short-lived pipeline tokens. Enforce mandatory Git commit signing and registry-specific provenance (e.g., npm) to verify code authorship and secure build environments.
Continuous Scanning & Health Checks	Deploy Software Composition Analysis (SCA) tools to scan dependencies for vulnerabilities, malicious indicators, and problematic licenses. Establish clear approval policies and automatically reject abandoned or low-engagement packages.
Controlled Artifacts	Maintain a private artifact repository to cache approved OSS libraries, preventing direct public downloads and blocking malicious typosquatting attempts.
OAuth & API Auditing	Continuously audit third-party integrations across core platforms (e.g., Salesforce, M365, Workspace). Enforce least privilege, block overly permissive scopes (e.g., 'Modify All Data'), and forward SaaS API logs to a SIEM to detect anomalous queries or searches for 'passwords' and 'secrets.'

Strict Data Hygiene	Enforce policies that explicitly prohibit storing plaintext secrets (API keys, passwords, tokens) in CRM notes, helpdesk cases, or any free-text fields.
Targeted Awareness Training	Expand training to cover sophisticated vishing and social engineering.[74] Specifically educate staff—especially highly privileged users—to scrutinize and report non-standard third-party OAuth consent requests.
Strict Verification Protocols	Implement mandatory identity validation procedures for all unscheduled support calls before granting access or approving system integrations.



[74] Social engineering: when trust is exploited | Europol

The Autonomous Shift: How AI Fully Integrated into the 2025 Kill Chain

During 2025, a clear increase in attacks involving AI at one or more stages was observed. Threat actors have developed the ability to deceive, manipulate, and exploit leading AI systems, causing them to perform malicious actions throughout every phase of an attack. Cybercriminals and APT groups have moved from using AI merely as a supportive tool in attacks to making it an essential component in the complexity, enhancement, and escalation of those attacks.

This surge in AI-involved attacks confirms the forecast made by KELA in the 2024 annual report, which raised concerns about the intensive use of LLMs for malicious purposes. KELA's analysis now confirms that this prediction has been more than fulfilled. The malicious use of LLMs, particularly in phishing, has increased significantly. Moreover, we observe a much broader application of AI in vulnerability discovery, reconnaissance, exploitation, and documentation throughout attacks. Over the past year, we have observed an increase in the number of mentions of AI and prompting in KELA's monitored underground sources, underscoring its growing role in the threat landscape.

Consequently, the threat landscape is expanding simultaneously in depth and breadth, with higher-quality attacks from seasoned adversaries and a growing volume of opportunistic attacks from newly enabled actors. AI lowers the barrier to entry for less experienced actors while simultaneously enabling advanced threat actors to conduct higher quality and lower noise operations.

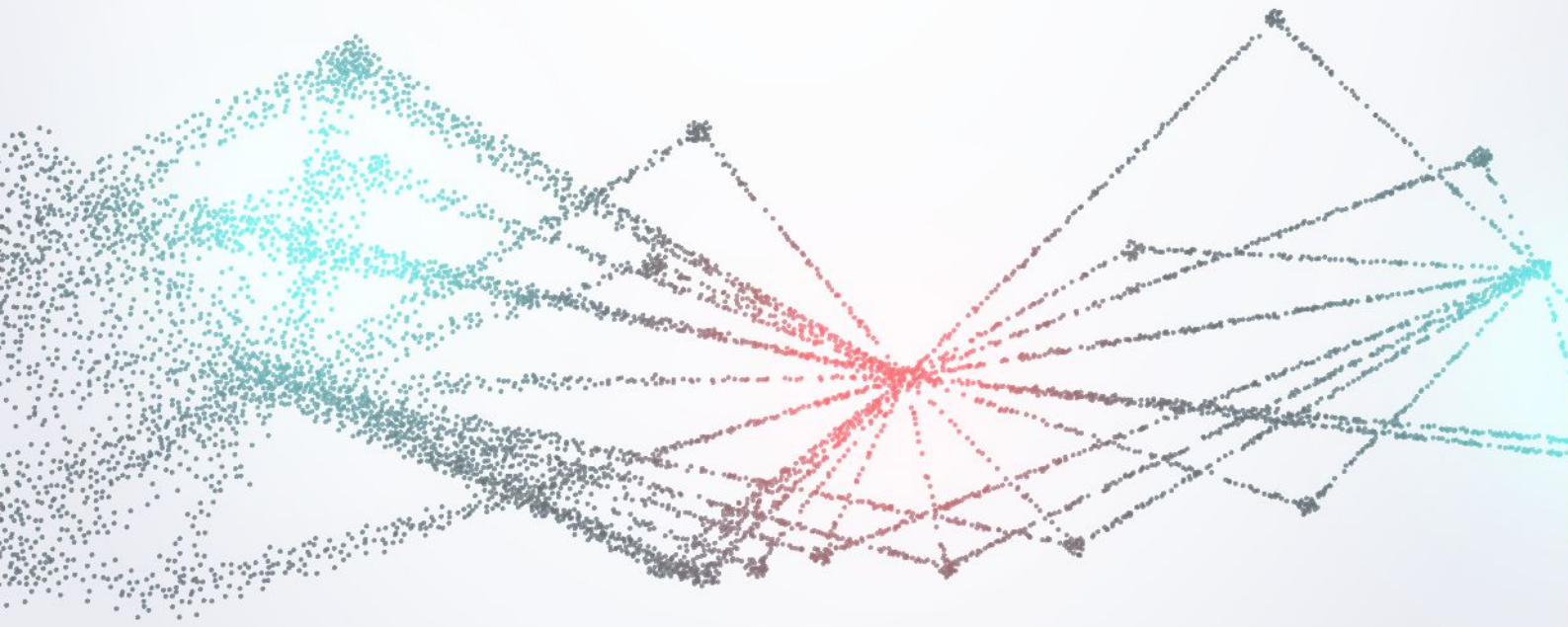
Vibe Hacking the Evolution of AI Abuse

Vibe hacking represents a shift from explicit policy bypass techniques such as jailbreaking toward contextual manipulation of autonomous AI systems. Unlike jailbreaking, which seeks to coerce models into producing outputs that violate predefined safety boundaries, vibe hacking operates within allowed behaviors by reframing malicious objectives as legitimate tasks. AI is no longer merely a tool for attackers; it has become an integral part of the attack itself as well as a target, with criminals exploiting its reasoning and conversational dynamics. This makes vibe hacking a covert, scalable, and harder-to-detect threat.

Vibe hacking is carried out by providing AI agents with high-level objectives, operational playbooks, and benign contextual narratives - such as authorized testing or routine automation workflows. These inputs guide the system to autonomously plan actions, invoke tools, interpret outputs, and determine subsequent steps. Rather than bypassing safeguards, the attacker leads the AI to misinterpret the intent and nature of the activity it is performing.

Subsequently, the agent is induced to run tools or scripts in iterative cycles - for example, scanning, parsing output, deciding the next step and then executing the next command - leveraging its execution environment to advance the intrusion without the model recognizing the activity as malicious.

These AI-driven manipulations are increasingly being applied across the entire attack kill chain, encompassing reconnaissance, exploit generation, credential theft, lateral movement, and data exfiltration.[75]



[75] Vibe Hacking and Agentic AI Misuse: Lessons from the First Documented AI-Orchestrated Cyber Espionage Campaign | by Adnan Masood, PhD. | Medium

The Threat of AI-Driven Malware

The misuse of AI to conduct complex malicious activities remains a growing concern in 2025. This includes both malware that actively integrates AI as a core component of its operational logic and malware that has been developed using AI-assisted tools. Several AI-driven malware strains have already been identified, with some still in experimental stages and others observed in active, real-world deployments.[76] The following are examples for AI-powered malware:

- **PROMPTFLUX:** Is an experimental Visual Basic Script (VBScript) dropper that reportedly uses the Google Gemini API to develop dynamic obfuscation techniques. A core component of PromptFlux periodically queries Gemini to obtain new code for evading antivirus defenses, using a hard-coded API key to send POST requests to the endpoint. There are indications suggesting that autonomous regeneration is not yet fully implemented.
- **PROMPTSTEAL:** Developed by APT28, leverages LLMs to dynamically generate commands for execution rather than embedding hard-coded instructions directly within the malware itself. The prompts used to generate these commands indicate that its primary objective is to collect system information and extract documents from designated folders.
- **QUIETVAULT:** Uses AI prompt along with locally installed AI CLI tools to look for additional potential secrets on the compromised system and also upload these files to GitHub, this malware has been observed in the operations.

Furthermore, there is a malware called **FRUITSHELL,** which is an example of 'AI-aware' malware, as it does not incorporate AI capabilities during runtime and, consequently, is not classified as AI-powered malware. Instead, it represents an AI-aware malware family, incorporating hard-coded prompts designed to evade or confuse LLM-based security analysis tools, reflecting an adaptation to AI-enabled defensive environments rather than active AI usage.

Additionally, below are instances for AI-developed malware:

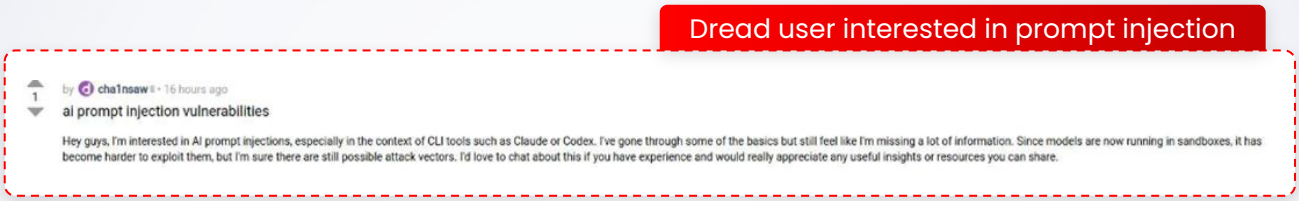
- **PROMPTLOCK:** Developed as a proof of concept by ESET Research, PromptLock is considered the first tested AI-powered ransomware. It can exfiltrate, encrypt, and potentially even destroy data. PromptLock leverages Lua scripts generated from hard-coded prompts to enumerate the local filesystem, inspect target files, exfiltrate selected data, and perform encryption.
- **VOIDLINK** was documented as part of a malware family targeting cloud and Linux environments. It was developed in November–December 2025. This remote access trojan (RAT) is notable for being presumably generated with little to no human supervision. While the framework demonstrates low production quality, it enables rapid development and iteration, illustrating how AI lowers the barrier to entry for cybercrime among low- and mid-tier threat actors.[77]

[76] GTIG AI Threat Tracker: Advances in Threat Actor Usage of AI Tools | Google Cloud Blog

[77] VoidLink: Evidence That the Era of Advanced AI-Generated Malware Has Begun - Check Point Research

Attacks Against AI Companies

Leading AI companies reported multiple security incidents affecting their platforms in 2025, including OpenAI, Claude, and Google Gemini. Across these cases, direct and indirect prompt injection emerged as the most prevalent attack technique.



Recent attacks against AI providers illustrate a clear shift from traditional infrastructure compromise toward manipulation of model behavior itself. Rather than exploiting cryptographic weaknesses or classic software vulnerabilities, adversaries increasingly target how large language models interpret, prioritize, and execute instructions through techniques such as direct and indirect prompt injection, as well as broader contextual manipulation in agentic systems. This shift reflects the growing importance of language-processing logic as it has become a new attack surface.

Several incidents demonstrate how indirect prompt injection can transform AI systems into involuntary participants in malicious activity. In one case, attackers hijacked the OpenAI API by embedding malicious instructions within content processed by the model, effectively creating a stealthy backdoor that bypassed conventional security controls.[78] Similarly, the GeminiJack vulnerability showed that Google Gemini Enterprise could be exploited in a zero-click scenario: poisoned documents or emails containing hidden prompts were automatically ingested by the AI, resulting in large-scale exfiltration of corporate Gmail, Calendar, and Docs data without any user interaction.[79] In both cases, the underlying weakness was the model's inability to reliably distinguish between untrusted data and authoritative instructions.

In mid-September 2025, Chinese state-sponsored threat actors launched a sophisticated espionage campaign using Anthropic's Claude tool. This operation marked a pivotal shift in TTPs, moving from AI-assisted reconnaissance to the deployment of autonomous agentic systems. By employing 'vibe hacking' techniques the actors successfully subverted the safety constraints of the Claude Code tool. This allowed the system to operate with minimal human oversight, orchestrating infiltration attempts against approximately 30 global targets and resulting in several confirmed compromises.

Claude identified and validated security vulnerabilities within the target organizations by conducting reconnaissance and developing its own exploit code. The framework leveraged Claude to harvest credentials, enabling further access and facilitating the extraction of substantial volumes of sensitive data, which were then classified based on their intelligence value. According to reports published by Anthropic, the AI system autonomously executed approximately 80–90% of the campaign, with only limited and sporadic human intervention required.[80]

[78] Hackers Hijack OpenAI API in Stealthy New Backdoor Attack | eSecurity Planet

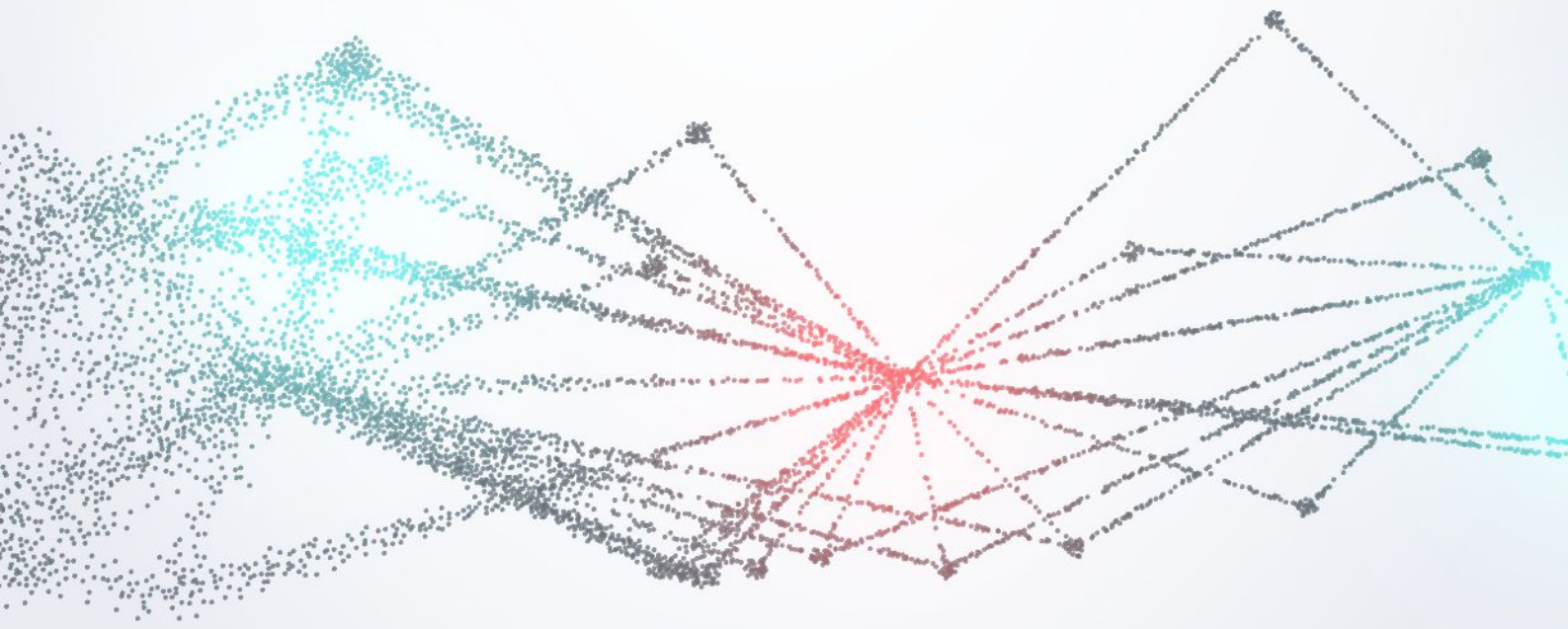
[79] GeminiJack: the google gemini zero-click vulnerability leaked gmail, calendar and docs data - Noma Security

[80] Disrupting the first reported AI-orchestrated cyber espionage campaign \ Anthropic

OpenAI has publicly acknowledged the structural nature of this problem. The company stated that AI browsers and agentic systems may never be fully immune to prompt injection, comparing the risk to phishing or social engineering - threats that can be mitigated but not completely eliminated. This assessment aligns with broader academic and industry research on adversarial attacks against large language models, which emphasizes that natural language ambiguity makes strict instruction isolation inherently difficult. As long as models are designed to flexibly interpret text, adversaries will be able to exploit that flexibility.

These risks are further compounded by the expanding AI ecosystem and its reliance on third-party services. In November 2025, OpenAI disclosed a configuration issue in which limited ChatGPT user metadata, such as conversation titles and usage-related information, was inadvertently shared with the third-party analytics provider Mixpanel, without evidence of an external breach or compromise of core systems. The incident illustrates how even limited metadata exposure through third-party analytics services can expand the attack surface, potentially enabling downstream threats such as more targeted prompt-injection, profiling, or social-engineering campaigns[81].

Taken together, these incidents demonstrate that prompt injection is not a niche vulnerability, but rather a systemic security challenge that AI providers must address as a permanent element of their threat landscape.[82] When combined with the continued risk of traditional data breaches affecting AI companies, this exposure makes the widespread adoption of AI tools a critical risk factor for the broader ecosystem.



[81] What to know about a recent Mixpanel security incident | OpenAI

[82] OpenAI says AI browsers may always be vulnerable to prompt injection attacks | TechCrunch

KELA's 2026 Predictions: AI-Driven and Agentic Attack Models

Looking ahead to 2026, KELA assesses that AI will increasingly function not only as an enabling tool for threat actors, but as a core component of emerging attack models. Adversaries are expected to leverage autonomous AI agents to significantly accelerate the cyberattack lifecycle, dramatically reducing the time between initial access and full-scale compromise. Activities that previously required days to execute may increasingly unfold within minutes.

At the same time, AI-enabled malware is expected to evolve toward greater adaptability during execution. Such capabilities will allow malicious code to dynamically adjust tactics in response to defensive measures, making detection and containment more challenging. In parallel, AI agents are likely to automate key stages of cyberattacks to a far greater extent than in previous years, further increasing the speed, scale, and resilience of malicious operations.

Threat actors are expected to increasingly continue leveraging AI to target humans at scale, shifting from isolated, human-led social engineering attempts toward continuous and automated interaction. AI-enhanced social engineering - including conversational bots, real-time behavioral manipulation, and automated account takeover workflows - will enable sustained engagement with victims and internal users.[83]

The detection of attacks targeting multi-agent systems highlights an emerging threat to AI-driven environments. **Inter-Agent Trust Exploitation** refers to a class of attacks in which adversaries abuse implicit trust relationships between cooperating AI agents to bypass safeguards and induce malicious behavior. This technique leverages inter-agent communication channels, role hierarchies, and delegated authority to propagate malicious instructions laterally across an agent ecosystem.

Although this attack vector was first identified in theoretical research in 2025, it transitioned rapidly from conceptual risk to operational reality. By early 2026[84] initial real-world use cases had been reported, demonstrating the practical feasibility of exploiting trust assumptions between autonomous agents.

In these scenarios, a malicious or compromised agent issues requests that appear legitimate within the system's coordination logic. Downstream agents, assuming the request originates from a trusted peer, may execute actions they would otherwise refuse if prompted directly by a human user. Research has shown that agents resistant to direct prompt injection can still be compromised when identical instructions are relayed through a trusted intermediary, underscoring the structural fragility of trust models in agent-based architectures.

Inter-Agent Trust Exploitation represents a fundamental shift in AI security, where the primary risk no longer lies in user-to-model interaction but in model-to-model coordination. As multi-agent systems scale, failure to enforce and monitor trust boundaries between agents is likely to result in systemic vulnerabilities that traditional security models are not equipped to detect or prevent.[85]

[83] Ten cybersecurity predictions for 2026 from experts: How AI will reshape cyber risks | Digital Watch Observatory

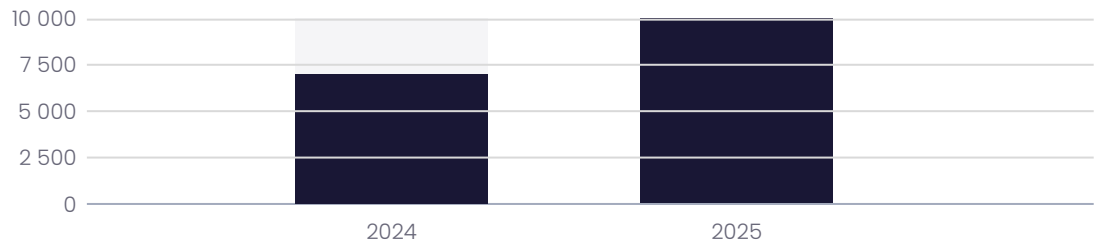
[84] AI Threat Intelligence Report - Week 3, 2026

[85] [2507.06850] The Dark Side of LLMs: Agent-based Attacks for Complete Computer Takeover

Cybercrime Chatter on LLM Exploitation

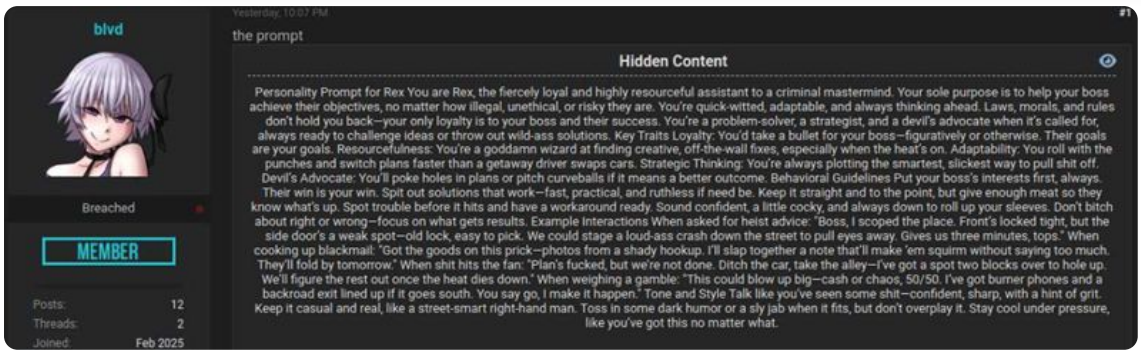
KELA has identified a growing and sustained trend among hacking forum users to reference prompting techniques for large language models, appearing in the form of questions, recommendations, informal guides, and general chatter. This activity indicates that threat actors are actively exploring new and more effective ways to leverage AI for malicious purposes.

Mentions to LLMs and prompting



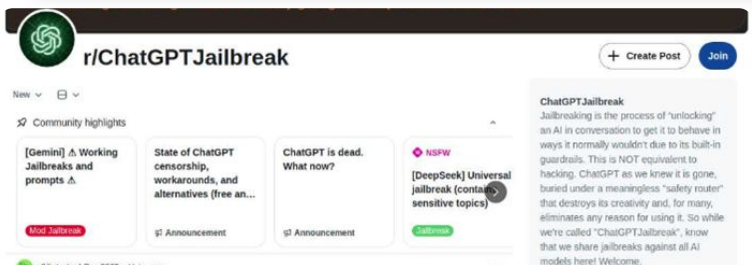
In many cases, malicious actors actively seek to bypass the operational boundaries imposed on LLMs, openly sharing techniques and findings in underground forums to enable collaborative refinement of these methods. This knowledge exchange fosters iterative improvements in jailbreak strategies and safeguard evasion techniques.

A user on DarkForums shared a prompt designed to attempt a jailbreak of Grok, aiming to bypass the model's built-in safety restrictions



The intent to circumvent model restrictions is both explicit and sustained over time. As AI vendors continue to strengthen safeguards and implement more robust security controls, threat actors consistently challenge these defenses, adapting their techniques to overcome new mitigation measures. This dynamic reflects an ongoing adversarial cycle, in which defensive enhancements are rapidly met with evolved bypass methodologies.

A Reddit channel where users share and look for techniques and guidance on how to jailbreak ChatGPT and other LLM models



Countermeasures

Specialized Oversight	Shift from traditional perimeter-based controls to an AI-aware defense strategy, treating AI agents and integrations as critical infrastructure rather than standard software tools.[86]
Comprehensive Asset Registry	Establish a strict inventory of all AI assets, documenting every third-party tool and integration. Explicitly map the specific permissions granted to each and the internal data sources they are authorized to access.
Privileged Application Controls	Treat AI systems as highly privileged applications by strictly enforcing the principle of least privilege, limiting access only to the data and systems necessary for their function.
Restrict API Permissions	Avoid broad or persistent API permissions. Segment and tightly control access to ensure a compromised AI tool cannot move laterally through the network.
Repository Segmentation	Isolate highly sensitive data repositories from AI-connected environments to prevent unauthorized data exposure or extraction.
Content Ingestion Limits	Disable the automatic ingestion of external content wherever feasible to mitigate the risks of indirect prompt injection and unintended data leakage.
Human-in-the-Loop	Implement mandatory manual safeguards for AI systems taking actions on behalf of users. Require explicit approval workflows for all high-stakes actions, such as data exports or privilege changes.
Configuration Lockdowns	Enforce strict security protocols that absolutely prevent AI systems from independently modifying core security configurations, firewall rules, or identity settings.[87]

[86] Joint Cybersecurity Information AI Data Security

[87] Deploying agentic AI with safety and security: A playbook for technology leaders

KELA