KELA

The State of Cybercrime 2024

Emerging Threats & 2025 Predictions

February, 2025

Executive Summary

In 2024, the cyber threat landscape became more complex. Threat actors became increasingly diversified, forming alliances and using methods that blurred traditional distinctions between cybercriminals, hacktivists, and state-sponsored groups. Underground economies, from malware-as-a-service (MaaS) to stolen credential marketplaces, contributed to a powerful infrastructure supporting a range of malicious activities. The expanding digital attack surface, driven by the rapid adoption of artificial intelligence (AI) and supply-chain interdependencies, introduced new vulnerabilities. Geopolitical tensions further exacerbated cyber risks, with state-sponsored actors leveraging cyber operations to achieve strategic objectives. Nation-state actors, including Russia, China, Iran, and North Korea, remained active in espionage and influence aligned with their geopolitical interests.

In this report, KELA highlights notable threats of 2024, alongside predictions and countermeasures for the evolving threat landscape of 2025. I hope it provides you with useful insights and a deeper understanding of the evolving cyber threat landscape. Our goal is to equip you with the intelligence needed to stay ahead of emerging risks.

David Carmiel

Chief Executive Officer, KELA

Infostealers as a Persistent Threat

- Infostealers serve as precursors to advanced attacks, including ransomware and espionage.
- KELA observed over 4.3 million machines infected globally by infostealer malware, accounting for more than 330 million compromised credentials.
- KELA has also observed 3.9 billion credentials shared in the form of credentials lists that appear to be sourced from infostealer logs.
- The top three infostealer malware strains - Lumma, StealC, and Redline - were responsible for more than 75% of infected machines.
- Credential theft and subsequent exploitation could turn into massive extortion campaigns, as seen in the Snowflake attack, which affected at least 165 companies due to compromised credentials.

Ransomware and Extortion Adaptation

- Ransomware and extortion operations grew, with over 5,230 victims tracked by KELA.
- The victims were claimed by almost 100 actors. The RansomHub ransomware group led the list with claims exceeding 520 victims.
- The US accounted for the majority of ransomware victims, representing more than half of the total number of victims.
- KELA observed a shift toward data theft while encryption still remains widely used. Notable trends also included targeting of third parties.
- Actors diversified their tactics, such as launching data marketplaces and striving to find additional monetization models.

Vulnerabilities as Entry Points

- Exploited vulnerabilities in widely used platforms underscored the need for timely patching.
- Cybercriminals' chatter demonstrated interest in vulnerabilities in Fortinet's FortiOS, various Wordpress plugins, D-Link Cloud Network Storage devices, Microsoft Outlook, and Windows Kernel.
- Cybercriminals' discussions around new CVEs appeared within one month following CVE disclosure and continued for months after disclosure.

Hacktivist Activity Amplified by Geopolitics

- Over 200 new hacktivist groups emerged, conducting more than 3,500 distributed denial-of-service (DDoS) attacks.
- Major events, such as the Russo-Ukrainian war and the Israel-Hamas conflict, influenced hacktivist campaigns targeting critical sectors.
- Tactics evolved to include ransomware, infostealers, and the formation of alliances.

State-Sponsored Threats and Convergence

- Major events that triggered state-sponsored operations included elections in the US, Taiwan, and India, while Olympic Games in Paris were targeted in influence campaigns.
- The line between state-sponsored and cybercriminal activities blurred, as tools that were traditionally used by cybercriminals, such as ransomware, are increasingly being used for geopolitical goals.

AI Abuse: New Attack Surface

- Cybercriminals exploited weaknesses in large language models (LLMs), abusing them to reach their goals.
- AI-powered threats included deepfakes, backdoored AI models, and adversarial attacks on AI-integrated platforms.
- The number of compromised accounts for popular models like ChatGPT (3 million accounts) and Gemini (174,000) surged dramatically, highlighting the need for stronger defenses.

Table of contents

01

THREAT SPOTLIGHT

Infostealers

In 2024, infostealers solidified their position as one of the most significant initial-access vectors in the cyber threat landscape. This type of malware, designed to harvest credentials, financial information, and other sensitive data, has become integral to the operations of cybercriminals. It's being provided to threat actors as MaaS platforms, where they can gain access to infostealer malware builds and infrastructure for a fee.

Infostealers' appeal lies in their efficiency and scalability, enabling attackers to compromise large volumes of accounts, both personal and corporate. Infostealers serve not only as direct enablers of account takeover and data exfiltration but also as precursors to more advanced attacks, such as ransomware and espionage campaigns.

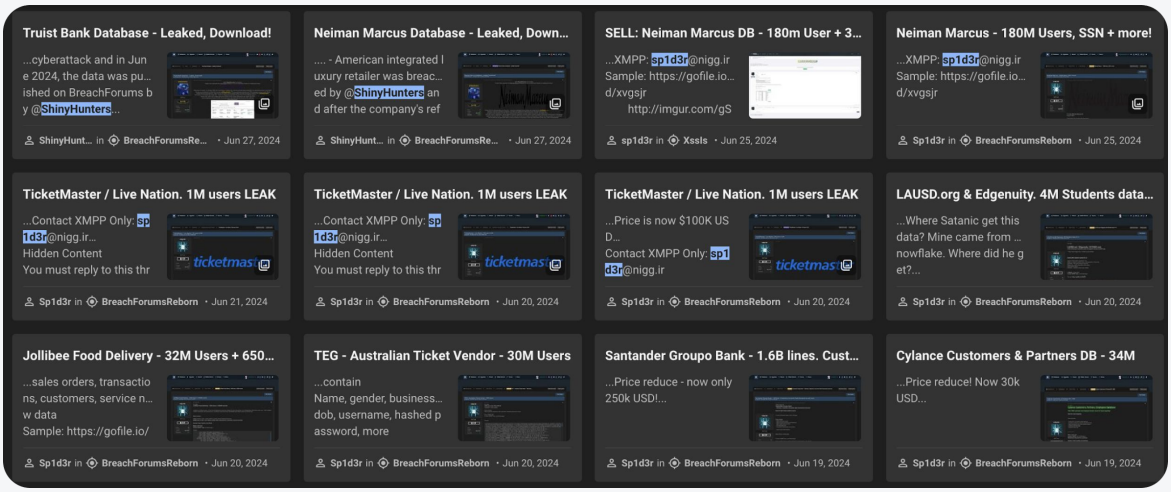
The cybercrime ecosystem, comprising marketplaces, forums, instant messaging, and other platforms, further fuels this trend with the vast supply of compromised credentials.

Snowflake attack:

The biggest infostealer-related attack of 2024

In mid-April 2024, stolen credentials allowed the UNC5537 group to access customer accounts on Snowflake, a cloud data storage platform. Initial access was traced back to infostealer malware: Threat actors obtained Snowflake clients' credentials that were stolen through infostealers and logged in to the accounts that weren't protected by multi-factor authentication (MFA). Then they used a custom script to steal information from Snowflake instances.

Later, several actors involved in the operation attempted to sell and leak these companies' data on cybercrime forums. This attack affected at least 165 companies.[1]



Attackers attempted to sell data stolen from Snowflake instances (Source: KELA platform)

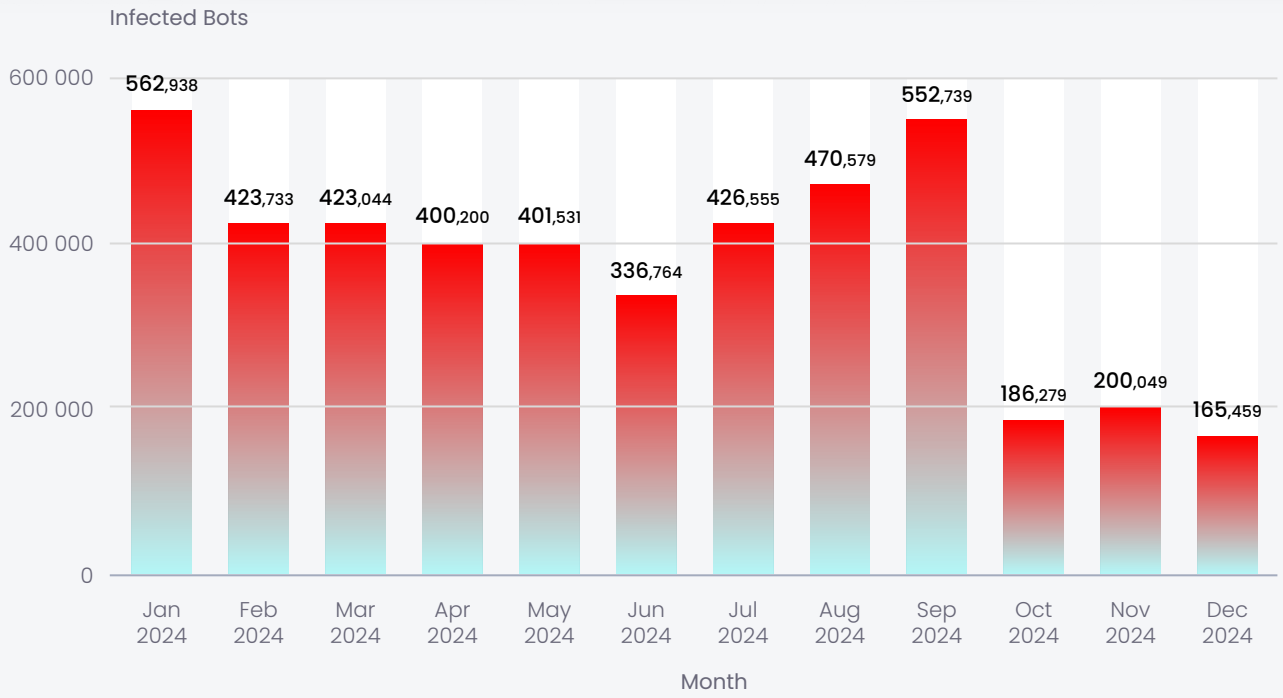
KELA's 2024 insights:

More than 4 million machines infected, Lumma stealer at top

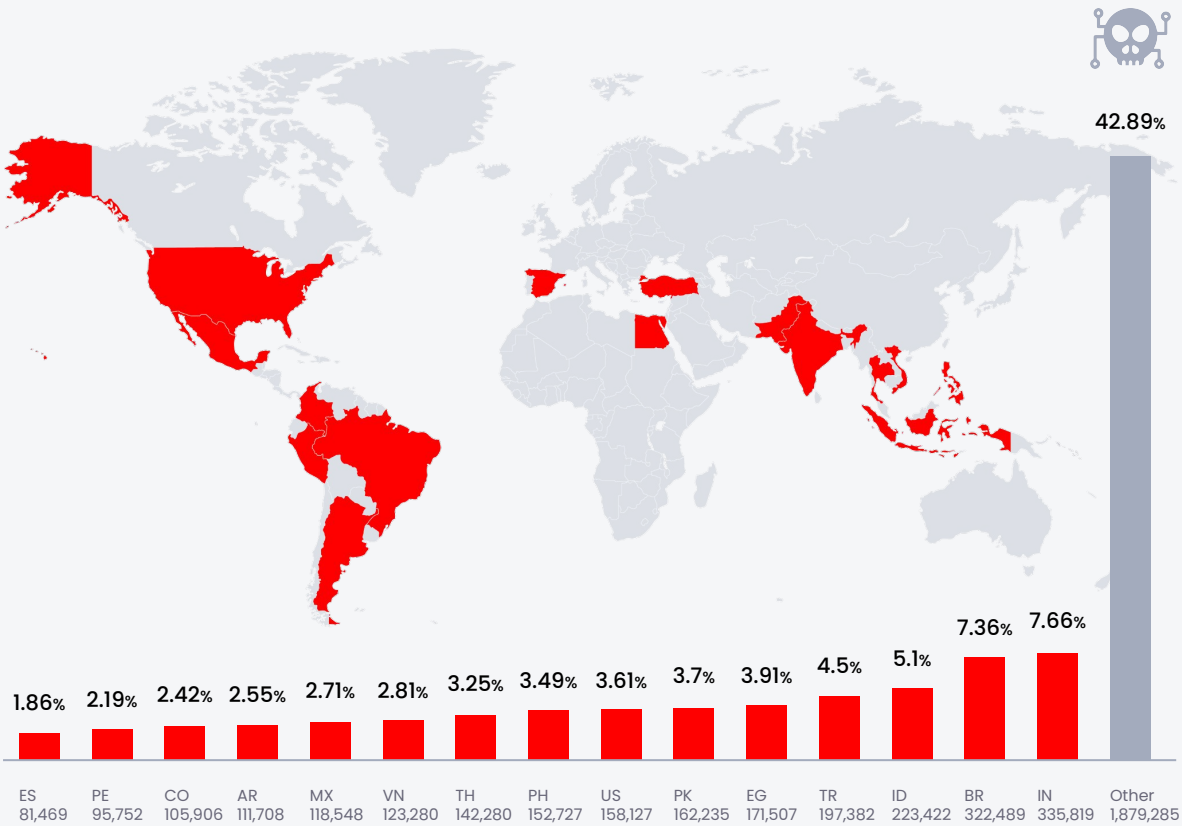
At least **4.3 million machines** in different countries were infected by infostealer malware in 2024, based on KELA's data lake, accounting for more than **330 million compromised credentials,** both figures just slightly bigger than in 2023.

[1] Source

Bots infected by infostealer malware in 2024[2]



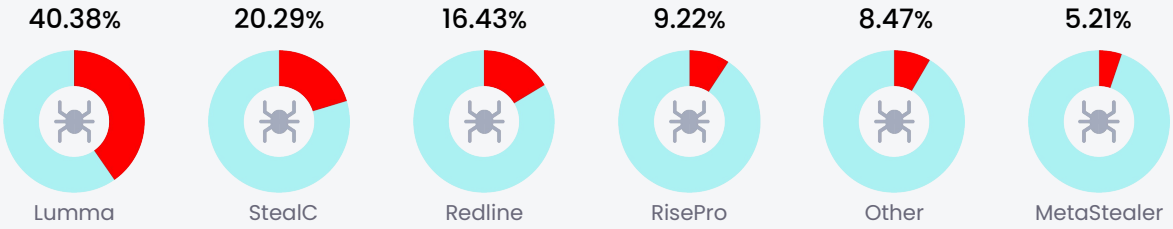
Bots infected by infostealer malware in 2024 per countries



[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. The graph is based on the machines' infection dates. Therefore, additional bots with infection dates at the end of year could be collected during the first months of 2025. For comparison, October-November 2023 are now in the top three most active months in terms of infection rate in KELA's data lake.

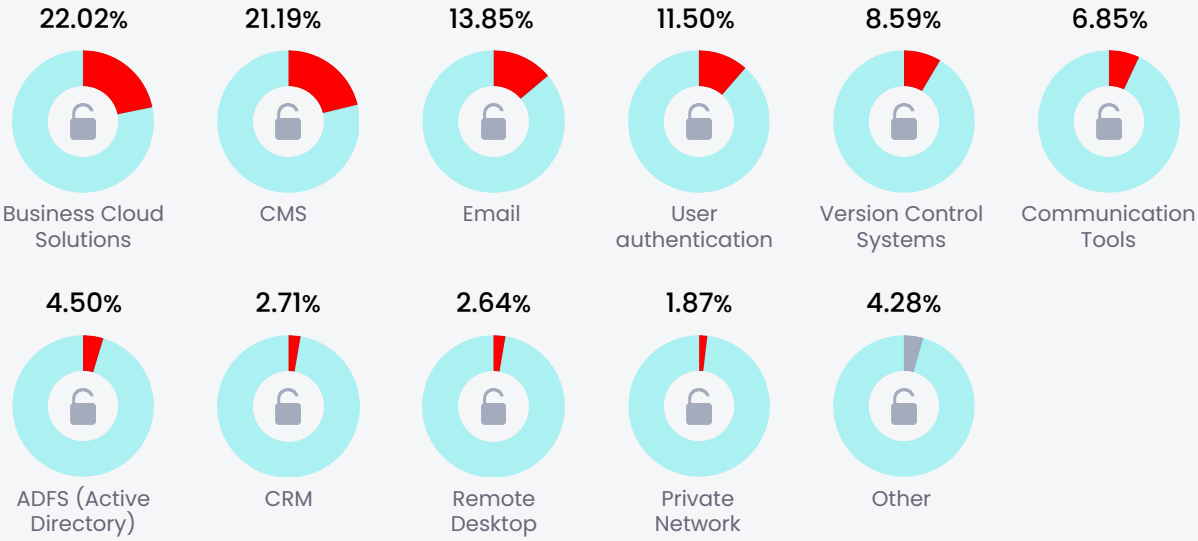
The top three infostealer malware strains - Lumma, StealC, and Redline (disrupted in Oct 2024) - were responsible for more than 75% of infected machines in KELA's data lake:

Top infostealer malware in 2024

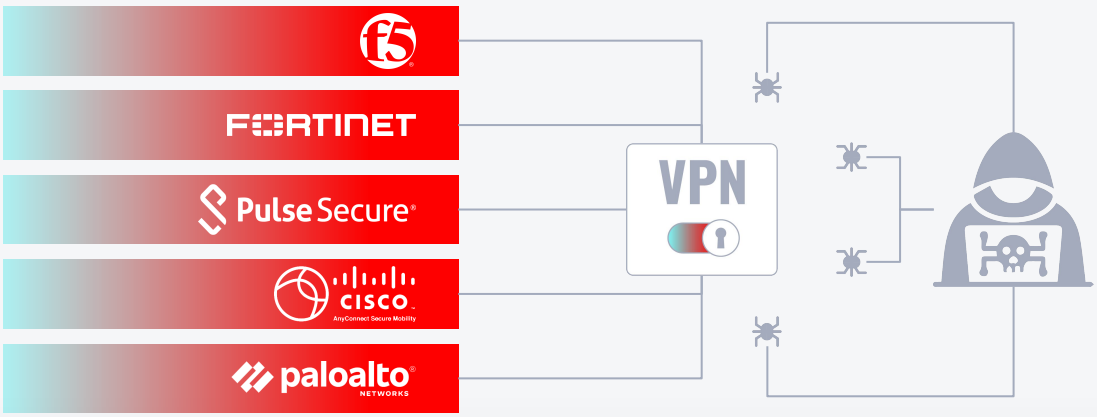


Almost 40% of infected machines in KELA's data lake included credentials for sensitive corporate systems, such as content management systems, email, Active Directory Federation Services, and remote desktop, accounting for **almost 1.7 million bots and 7.5 million compromised credentials:**

Compromised credentials to sensitive services in 2024

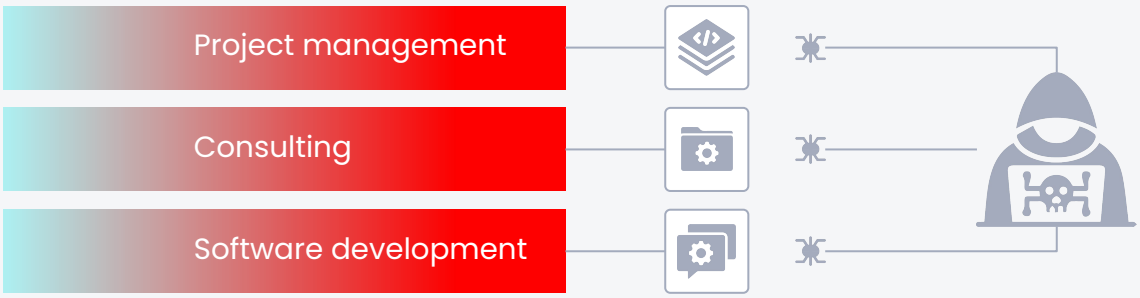


The top five affected vendors of VPN solutions, which is one of the most sensitive categories sought by ransomware attackers and others, were:[3]



[3] Source

The top three job departments affected by infostealer malware, based on research into a data set of various companies' employees who were infected:[4]



Based on KELA's analysis, **the dataset primarily (almost 65%) contained personal computers that had corporate credentials saved** on them and thus obtained by infostealer malware.

In addition to compromised credentials coming from infected machines, **KELA has also observed 3.9 billion credentials shared in the form of credentials lists,** which cybercriminals commonly refer to as url:login:pass (ULP) files. ULP files are compilations of data usually obtained by different actors, and these credentials can be harvested from a variety of sources, including infostealer logs, third-party breaches, and phishing. However, KELA assesses that most ULP files are sourced from infostealer logs.

KELA's 2025 predictions:

Infostealers to remain a common initial access vector

Looking ahead to 2025, the use of infostealers is expected to continue its growth. The proliferation of MaaS platforms and the increasing sophistication of infostealers will likely amplify their role as a primary vector for initial access. However, the landscape will also be shaped by intensified law-enforcement efforts.

High-profile operations in 2024, such as the disruption of RedLine, demonstrated the ability of international agencies to dismantle key components of the infostealer supply chain. These efforts are likely to continue and even escalate in 2025, targeting not only the malware developers but also the infrastructure of affiliate teams and marketplaces, as well as other platforms supporting their operations.

While such actions may temporarily disrupt the infostealer ecosystem, they can also drive increased activity among other MaaS infostealers, as emerging players move to seize the opportunity and fill the void.

[4] In response to the rise of infostealers and the rapid growth of compromised credentials being sold on the dark markets, KELA conducted in-depth research using an in-house collection of infected machines. KELA analysed a dataset of machines compromised through information stealing malware and containing VPN credentials, as VPNs are widely used in corporate environments. The dataset consists of 300 machines, containing more than 100,000 compromised credentials, infected with various types of infostealer malware, with infection dates ranging from July 19, 2024, to August 19, 2024. The research will be published in 2025.

Countermeasures

- **Enhance endpoint detection and response (EDR):** Deploy robust EDR solutions to detect and isolate infostealer activity in real time, focusing on behavior-based analysis rather than solely signature-based methods.
- **Implement strong credential management:** Enforce MFA across all accounts and regularly rotate privileged credentials to limit the impact of stolen login information.
- **Conduct regular threat hunting:** Proactively search for signs of infostealer infections within your network, focusing on unusual traffic to known malicious domains or IPs.
- **Strengthen network segmentation:** Isolate critical systems and data to limit the lateral movement opportunities for attackers using stolen credentials.
- **Partner with threat intelligence providers that offer identity security solutions:** Leverage cyber threat intelligence (CTI) services to stay updated on the latest infostealer strains, tactics, and threat actor activities in your sector, as well as exposure of your company's assets, including access to third-party resources.
- **Bolster email security:** Use advanced email filtering solutions to prevent phishing attempts, the primary delivery method for infostealers.
- **Increase employee training:** Conduct frequent awareness campaigns to educate employees about recognizing phishing emails and the dangers of downloading unverified software, sharing work PCs or laptops with unauthorized individuals, practicing secure password management, reporting suspicious activities promptly, and following established protocols for handling sensitive data.
- **Prepare incident response plans:** Maintain updated playbooks for responding to infostealer infections, emphasizing containment, analysis, and remediation.

02

THREAT SPOTLIGHT

Ransom and Extortion

Despite significant disruptions by law-enforcement agencies in 2024, such as the LockBit-focused Operation Cronos[5] and the dismantling of the Radar ransomware group,[6] ransomware and extortion actors continued to adapt and operate. KELA identified over 60 new actors in 2024, with 13 of them ceasing the activity in the same year. Therefore, while ransomware and extortion operations are very popular, staying in this business requires effort. Most of them continue to operate as ransomware-as-a-service (RaaS) platforms, relying on double extortion and supply-chain compromises.

Among new threat groups that KELA observed in 2024, over 10 were identified as actors that only steal data and do not employ ransomware, indicating a shift toward data theft while encryption still remains widely used.

Supply-chain attacks remain common, as third parties offer sensitive access to many different organizations. Targeting them is very efficient for threat actors, who can exploit the access and conduct several further attacks, widely monetizing them.

Interestingly, in 2024, KELA observed a few cases of ransomware groups using different monetization models and advertising additional services. For instance, Meow started to operate as a data market used to sell stolen data to any interested buyers, not necessarily as part of a name-and-shame ransom process. Additionally, KillSec advertised an 'OSINT service,' suggesting data gathering about any entity. Also, Funksec, though its credibility remains low, introduced additional services to their ransom activities: so-called 'BlackZone,' offering to publish other threat actors' leaks on Funksec's site for free, possibly as a strategy to drive traffic and increase exposure of their site.

[5] Source

[6] Source

Notable ransom attacks

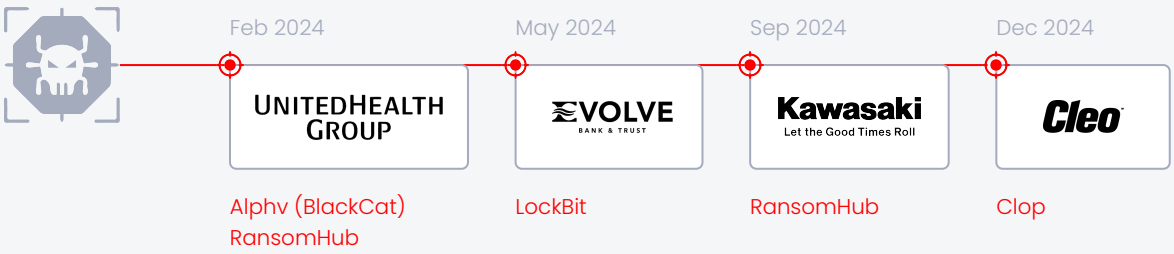
2024 saw several significant ransom incidents, affecting organizations across various sectors and highlighting the evolving threat landscape:

- **UnitedHealth Group** was targeted in February 2024 by Alphv (BlackCat), which exploited stolen credentials to access Change Healthcare's Citrix portal without MFA. Attackers stole data over nine days before deploying ransomware, prompting the organization to sever connectivity to contain the attack. It's worth noting that RansomHub has claimed the same victim, apparently collaborating with the Alphv affiliate that performed the attack, in April 2024. At the end of April, in a statement provided to the media, UnitedHealth confirmed that it paid a ransom, without specifying to which group.

- **Evolve Bank & Trust** disclosed in May a breach that had exposed the personal data of 7.6 million individuals. LockBit claimed responsibility, alleging the theft of 33 TB of sensitive information.

- **Kawasaki Motors Europe** reported a cyberattack in September 2024 that led to service disruptions and server isolation. RansomHub claimed responsibility, stating it had stolen 487 GB of data.

- **Cleo** reported active exploitation of its Harmony, VLTrader, and LexiCom software due to insufficient patching of CVE-2024-50623 and CVE-2024-55956 in December 2024. A few days later, the Clop ransomware group claimed that they were exploiting those vulnerabilities, reportedly using zero-day exploits to breach corporate networks, and announced 66 new victims on their blog allegedly linked to the exploitation of the vulnerability.



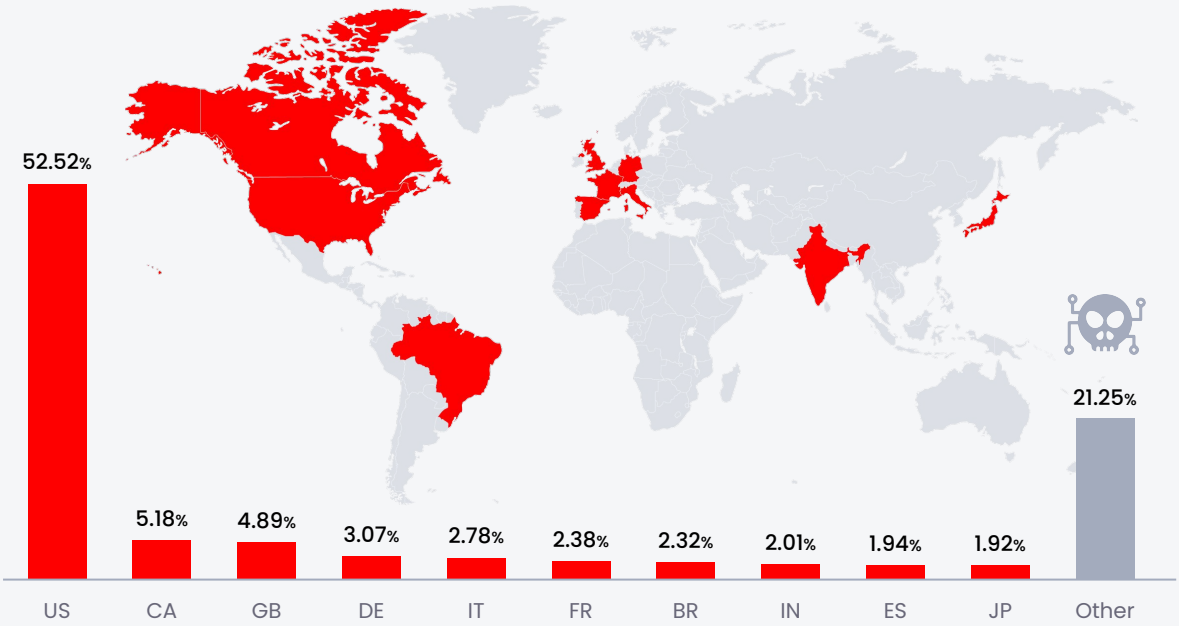
KELA's 2024 insights:

Over 5,230 victims infected, most in the US

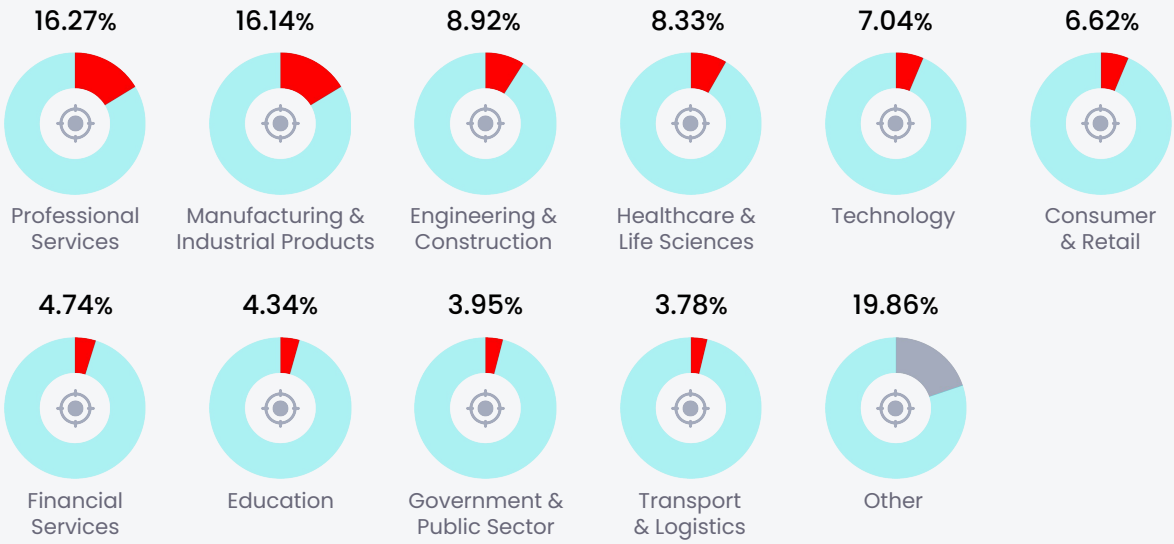
Over 5,230 victims were tracked by KELA in 2024, which is 10.5% more than in 2023. **The victims were claimed by almost 100 actors,** 28,5% more than in 2023.

The US accounted for the majority of ransomware victims, representing more than half of the total.

Top 10 affected countries

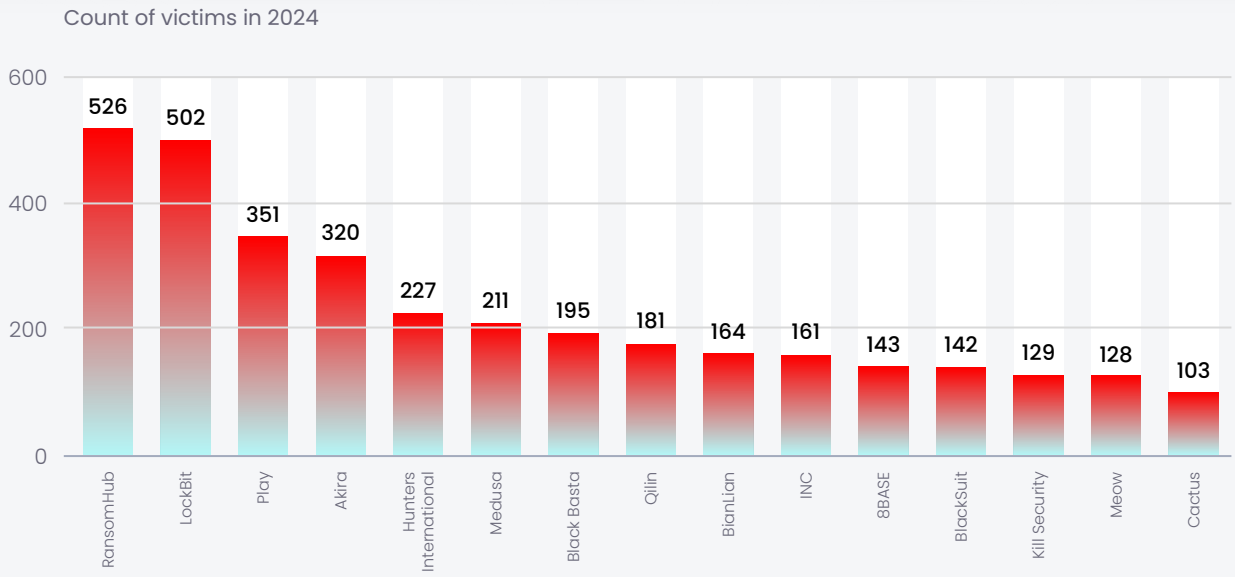


Top 10 affected sectors



RansomHub led the attackers list with claims exceeding 520 victims, dislodging LockBit, with approximately 500 victims, from its 2023 top position.

Top 15 active ransomware actors

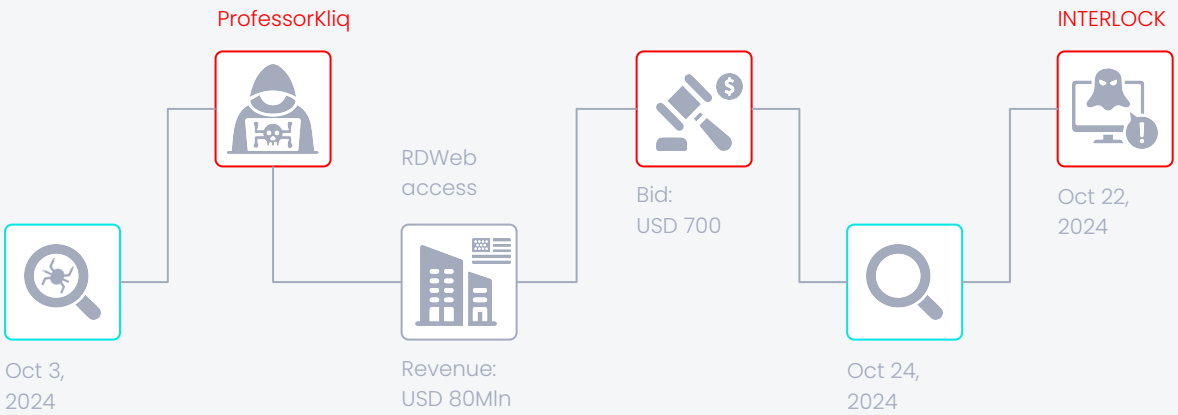


Over 30 ransom victims were claimed twice or more in 2024. That may have been the result of collaboration among groups but could also be separate attacks that took place in parallel, possibly using the same initial access vector.

Use case:
From initial access on sale to a ransom attack

On October 3, 2024, KELA observed the threat actor ProfessorKliq selling RDWeb access to a US-based company with USD 80 million in revenue. The access was offered for sale in an auction form, starting with a bid of USD 700. KELA has researched the details that the actor provided about the victim and assessed with high confidence the company's identity, based on publicly available information in its description.

On October 24, 2024, KELA observed that the identified company said it was compromised by INTERLOCK ransomware two days earlier. It's possible that the ransomware group member bought the access that resulted in the attack.



Threat Actor Spotlight

RansomHub

520+ victims claimed in 2024

RansomHub, an RaaS operation, has been active since at least February 2024. It was first announced on February 2, 2024, by an actor named "koley" on the RAMP forum. Their ransomware locker is written in Golang and C++, boasting rapid encryption speeds and capable of targeting Windows, Linux, macOS, and VMware ESXi environments. Affiliates of RansomHub employ a double extortion model, encrypting systems and exfiltrating data to pressure victims into paying to prevent the leak of their data.

RansomHub rapidly expanded its operations in 2024. According to KELA's data, they targeted 20 to 40 victims each month from March to July, more than 80 from October to November, and more than 50 in December. It's worth highlighting that RansomHub is the first ransom group in recent years to surpass LockBit.

RansomHub operators typically gain initial access through spear phishing, password spraying,[8] and exploiting critical vulnerabilities, for example, Zerologon (CVE-2020-1472), CVE-2023-3519 inCitrix ADC, CVE-2023-27997 in FortiOS, and CVE-2023-46604 in Java OpenWire. To evade defenses, they use deceptive file names and clear system logs, and they employ TDSSKiller, a legitimate tool from Kaspersky, to disable EDR systems. They also use open-source malware LaZagne for credential harvesting.[9] Persistence is established by creating and re-enabling user accounts, often using Mimikatz for credential theft and privilege escalation. Data exfiltration methods vary by affiliate, while their ransomware employs Curve 25519 encryption, appending random extensions.

[8] Source

[9] Source, source

LockBit

500+ victims claimed in 2024

LockBit started their activities in 2019 and launched their own blog in 2020. LockBit ransomware uses a double extortion model, and the group has been operating their custom ransomware strains since the beginning of their activities. In early 2021, LockBit adopted the RaaS model. They attract affiliates through publicity stunts and by offering a user-friendly ransomware panel interface.

Despite Operation Cronos and a slowdown in claimed attack rates, the group continually develops its ransomware tools and infrastructure. It also announced LockBit 4.0, which is due to be released in 2025.

LockBit ransomware affiliates primarily compromise systems through phishing campaigns and exploiting critical vulnerabilities, for instance, CVE-2021-44228 in Apache Log4j2, CVE-2021-22986 in F5 iControl REST, and CVE-2020-1472 in NetLogon. They also use initial access brokers (IABs) for network entry. Once inside, they often exploit legitimate remote desktop tools like AnyDesk, TeamViewer, and ScreenConnect for lateral movement and control. LockBit affiliates deploy their custom exfiltration tool, StealBit, to extract sensitive data before encryption. Their ransomware appends the ".lockbit" extension to encrypted files.[10]

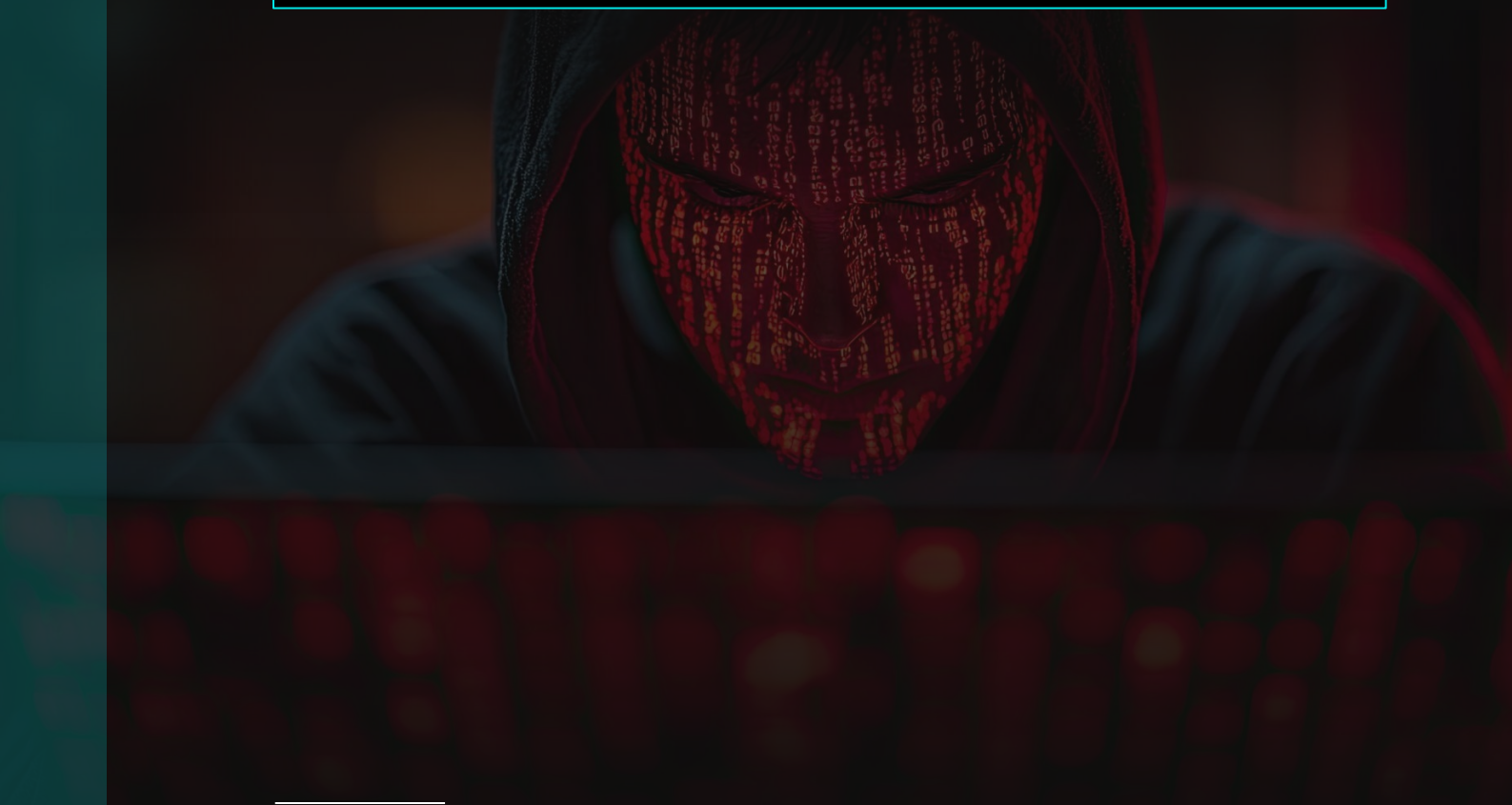
[10] Source

Play

350+ victims claimed in 2024

The Play ransomware group, also known as Playcrypt, has been active since at least June 2022. It's believed to operate as a closed organization, without affiliate programs. Play ransomware uses a double extortion model, exfiltrating sensitive data before encrypting the victim's systems.

Play achieves initial access through abuse of valid accounts and exploitation of vulnerabilities in public-facing applications, including FortiOS (CVE-2018-13379, CVE-2020-12812) and Microsoft Exchange (CVE-2022-41040, CVE-2022-41082). They conduct Active Directory queries to discover network details and use PowerShell tools to disable antivirus software, remove logs, and target Microsoft Defender. For lateral movement and command-and-control operations, they use Cobalt Strike and SystemBC. The group focuses on obtaining unsecured credentials to escalate privileges, often using credential dumpers to gain domain administrator access. Data exfiltration involves splitting and compressing stolen information into .RAR files before transfer. They employ AES-RSA hybrid encryption with intermittent encryption, adding a ".play" extension to files.[11]



[11] Source

KELA's 2025 predictions:

Ransom actors to maintain reliance on RaaS and additional services

Ransomware activity shows no indication of diminishing, as adversaries continue to adapt their methods to counter law-enforcement activities. The RaaS business model, in particular, is expected to grow further due to its decentralized structure and profitability, with affiliates migrating from one operation to another in light of disruption operations or other circumstances.

Supply-chain attacks are likely to remain a prominent strategy, given their high profitability and the inherent vulnerabilities of the modern tech industry, which relies heavily on third-party software providers with access to multiple organizations. These supply-chain compromises provide attackers with opportunities to launch large-scale campaigns. In addition to data extortion tactics, threat actors may be diversifying their activities in 2025 with additional services and collaboration with other cybercriminals.

Countermeasures

- **Strengthen supply chain security:** Perform rigorous security assessments of third-party vendors, enforce least-privilege access, and require vendors to adhere to robust security frameworks.
- **Adopt zero-trust architecture:** Implement a zero-trust model to limit access to resources based on continuous verification, reducing opportunities for ransomware lateral movement.
- **Harden backup strategies:** Maintain offline, immutable, and regularly tested backups of critical data to ensure quick recovery in case of ransomware attacks.
- **Deploy extended detection and response (XDR):** Use XDR solutions to monitor and correlate threats across endpoints, networks, and cloud environments to detect signs of RaaS activity early.
- **Enhance endpoint protections:** Leverage advanced anti-malware solutions with ransomware behavior analysis to block known and unknown ransomware strains.
- **Monitor RaaS affiliate trends:** Collaborate with CTI providers to identify and respond to emerging affiliates and ransomware families targeting your sector.
- **Conduct frequent patch management:** Address vulnerabilities promptly across all systems and software, prioritizing critical updates to minimize the attack surface for supply-chain exploits.
- **Implement data segmentation:** Encrypt sensitive data and segment it from less critical resources to limit the impact of potential ransomware attacks.
- **Simulate ransomware attacks:** Conduct regular exercises and penetration tests to evaluate and refine your organization's ransomware response strategy.

03

THREAT SPOTLIGHT

Vulnerabilities

In 2024, cybersecurity threats continued to evolve, 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 proof-of-concept exploits (PoCs) for publicly disclosed vulnerabilities, as well as for zero days.

The November 2024 Cybersecurity Advisory released by the 'Five Eyes' cybersecurity agencies emphasized a rise in the exploitation of zero-day vulnerabilities compared to previous years.[12] The advisory noted that threat actors are most successful within two years after the public disclosure of vulnerabilities and that the exploitation rate declines as vendors issue patches and updates.

[12] Source

Top exploited vulnerabilities

Among the most frequently exploited vulnerabilities in 2023, the aforementioned advisory identified the following critical flaws:

CVE-2023-3519: Affects Citrix NetScaler ADC and NetScaler Gateway and allows unauthenticated users to execute a stack buffer overflow via an HTTP GET request.

CVE-2023-4966: Affects Citrix NetScaler ADC and NetScaler Gateway and allows session token leakage.

CVE-2023-20198: A vulnerability in Cisco IOS XE Web UI that allows unauthorized users to create local user accounts.

CVE-2023-20273: Affects Cisco IOS XE, following activity from CVE-2023-20198, and allows privilege escalation.

CVE-2023-27997: Affects Fortinet's FortiOS and FortiProxy SSL-VPN and allows remote attackers to execute arbitrary code or commands by crafting specific requests.

KELA's 2024 insights:

The flaws most sought by cybercriminals

According to cybercrime forums chatter observed by KELA, the most mentioned CVEs from 2024 were:

CVE-2024-21762: An out-of-bounds write in FortiOS that enables attackers to execute unauthorized code via specially crafted requests.

CVE-2024-23113: A format string vulnerability in FortiOS that allows unauthorized code execution through crafted packets.

CVE-2024-3273: A critical vulnerability in D-Link devices, leading to remote command injection.

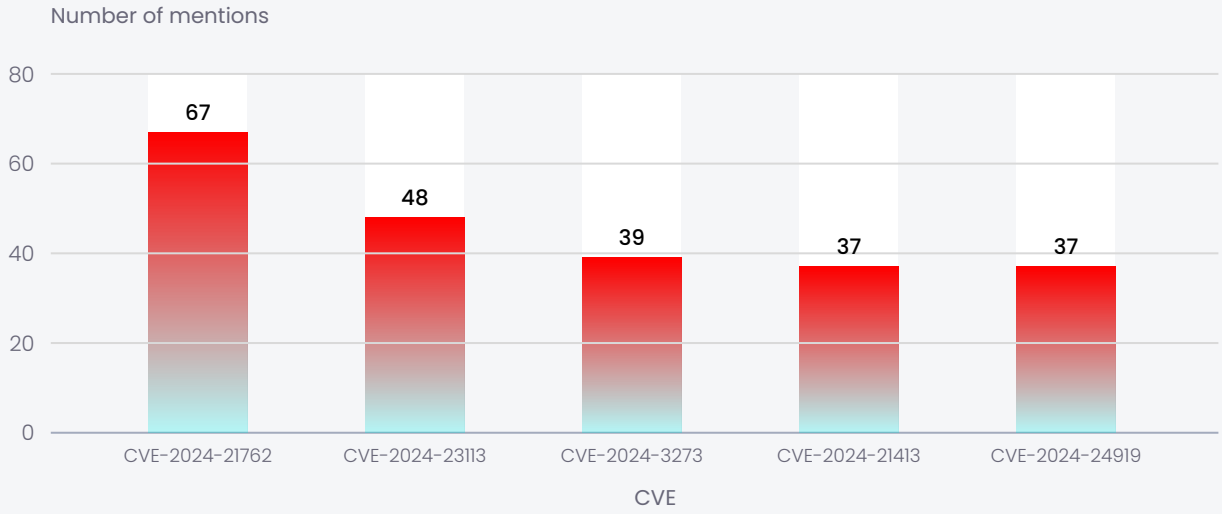
CVE-2024-21413: A remote code execution flaw in Microsoft Outlook.

CVE-2024-24919: A vulnerability in Check Point Security Gateways that may allow attackers to read sensitive information if remote access VPN or Mobile Access Software Blades is enabled.

[13] The list of the most frequently exploited vulnerabilities is yet to be released.

The discussions include selling and sharing public or unique PoCs, as well as methods and tips on exploitation and news chatter. These vulnerabilities demonstrate cybercriminals' ongoing interest in widely used software and hardware systems, with Fortinet's FortiOS, D-Link storage devices, and Microsoft Outlook emerging as common targets, and remote code execution being a prominent vulnerability type discussed.

Top 5 CVE-2024 mentioned on cybercrime forums in 2024



KELA has looked closely at cybercrime discussions around new CVEs to gain an insight into how quickly threat actors pick up the newly disclosed flaws and start sharing PoCs and tips on exploitation. On average, **CVE-related discussions by malicious actors appear within one month following its disclosure.** Some vulnerabilities were discussed on the very same day or just a few days after, while others are still mentioned nearly a year after being disclosed.

KELA's 2025 predictions:

Disclosed vulnerabilities to remain a common entry point

As we move into 2025, it's likely that the frequency and sophistication of cyberattacks will continue to increase. The rapid exploitation of vulnerabilities, especially in widely used systems like remote access solutions, operating systems of firewalls and switches, email clients, and network storage devices underscores the need for continual patching and monitoring of critical systems.

The trend of rapid discussion and exploitation observed in cybercrime forums also signals that attackers will remain highly proactive in identifying and leveraging new vulnerabilities. On the other hand, there's a persistent nature to these discussions, as some vulnerabilities continue to be actively talked about and targeted months, and even nearly a year, after their initial disclosure. This persistence suggests that flaws remain valuable to attackers over time, making it crucial for organizations not only to address vulnerabilities quickly but also to monitor and defend against long-term threats, prioritizing patching based on the threat actors' active interest.

Countermeasures

- **Prioritize vulnerability management:** Establish a risk-based patching program that prioritizes vulnerabilities based on threat intelligence about active exploitation and criticality.
- **Enhance patch timelines:** Reduce the time to patch by streamlining internal testing and approval processes for applying updates to critical systems.
- **Implement virtual patching:** Use intrusion prevention systems or web application firewalls to shield unpatched systems from exploitation until permanent patches can be deployed.
- **Leverage threat intelligence:** Regularly monitor cybercrime forums and vulnerability databases to identify and respond to vulnerabilities that attackers are actively exploiting or discussing.
- **Perform regular security assessments:** Conduct vulnerability scans and penetration testing to identify and remediate undisclosed weaknesses in your systems.
- **Adopt endpoint hardening:** Apply security configuration baselines and disable unused services and ports to minimize the attack surface.
- **Monitor for exploitation indicators:** Deploy advanced detection tools to identify patterns of behavior that suggest exploitation of known vulnerabilities.
- **Educate IT teams:** Train IT staff on timely identification and remediation of vulnerabilities, emphasizing long-term monitoring of older, disclosed flaws still targeted by attackers.
- **Maintain asset visibility:** Use asset inventory tools to track all hardware and software, ensuring no system is overlooked in vulnerability management efforts.

04

THREAT SPOTLIGHT

Hacktivists

2024 was marked by significant hacktivist activity, fueled by the Russo-Ukrainian war and the Israel-Hamas conflict. Various groups, in particular pro-Russian and pro-Palestinian, targeted government, manufacturing, and energy sectors in Europe and the US, with some campaigns raising suspicions of state backing. Incidents such as the targeting of the Paris Olympics demonstrated how hacktivists leveraged global events to amplify their messages and increase their visibility. The increasing coordination of some groups, such as forming alliances – for example, the Red Eagle Crew, Holy League, and October 7 Union – demonstrated the evolving challenge of mitigating hacktivist threats.

Some hacktivist groups evolved their tactics by combining traditional methods like DDoS and defacement with more advanced attacks such as the ones using ransomware and infostealing malware, demonstrating a shift toward more complex and multifaceted operations, even among less skilled actors.

Telegram remained a popular platform among hacktivists due to its reach, though concerns over updated privacy policies prompted discussions about migrating to Discord and Signal.[14]

[14] Source

Notable hacktivist attacks

- The DDoS campaign against **Israel's payment gateway company Hyp's CreditGuard** product aimed to disrupt financial operations amid the Israeli-Hamas conflict, drawing widespread attention to the attackers' cause. The attack was attributed to Anonymous for Justice, an alleged hacktivist group suspected of being tied to Iranian intelligence.[15]

- BlackMeta, a pro-Palestinian group, claimed a DDoS attack on the **Internet Archive,** which resulted in its Wayback Machine and other sites and services being inaccessible, demonstrating how the hacktivists extend their efforts beyond conflict zones to amplify their political message.

- CyberVolk conducted **ransomware campaigns,** leveraging self-branded payloads and alliances with other ransomware families to target entities opposing Russian interests, combining data theft and financial extortion to disrupt critical sectors.[16] These incidents demonstrated the evolving sophistication of hacktivist tactics.

KELA's 2024 insights:

Over 200 new hacktivist groups and more than 3,500 DDoS attacks

In 2024, KELA tracked over **200 new hacktivist groups, with approximately 300 notable groups active** throughout the year.

KELA looked closely at the messages on Telegram channels where hacktivists groups were active to gain an insight into how many attacks they claim to perform. While not all the messages in the channels are related to attacks, there is a pattern that can help to identify such posts. These groups frequently mention victims' domains in their claims of DDoS, defacement, data theft, and other attacks, as well as supporting URLs (for example, websites' accessibility reports provided as proof). The following groups had the most domains in their messages:

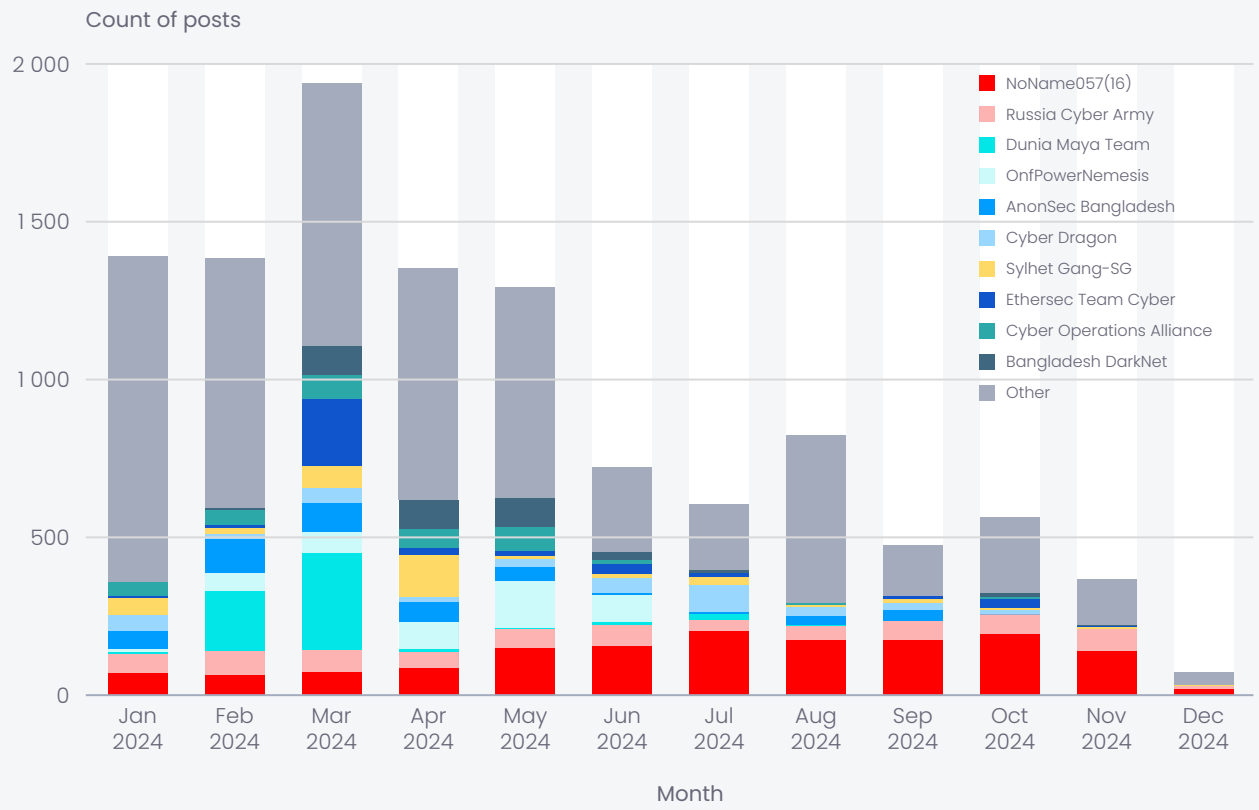
- Pro-Indonesian Ethersec Team Cyber
- Pro-Russian NoName057(16)
- Pro-Indonesian Dunia Maya Team
- Pro-Russian People's Cyber Army
- Pro-Palestinian Cyber Operations Alliance

DDoS remains one of the most popular attack types conducted by hacktivists. **At least 3,500 DDoS attacks** were claimed by notable actors.

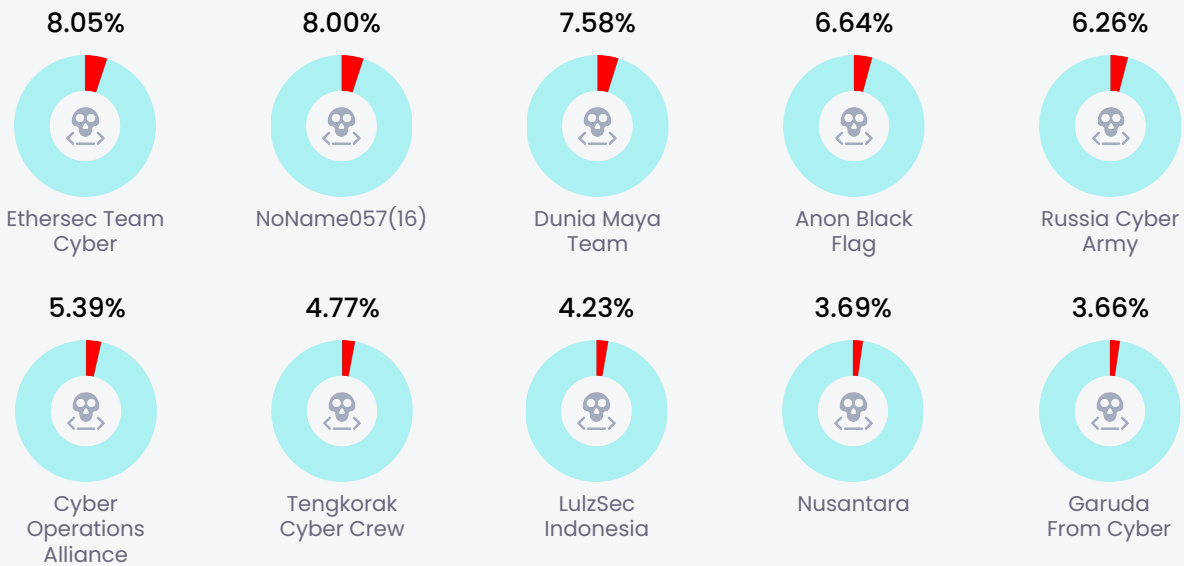
[15] Source

[16] Source

DDoS attacks claimed by hacktivists throughout 2024
(base on the attacked websites' accessibility reports provided as proof):



Top 10 groups announcing DDoS attacks were responsible for almost 50% of claims:



KELA's 2025 predictions:

Growth and diversification of attacks

2025 is expected to witness a more organized and technologically advanced hacktivist landscape, with activities heavily influenced by geopolitical events. Hacktivist groups are expected to form more alliances, enhancing their capabilities and broadening their impact. The accessibility of AI-powered tools will enable less skilled individuals to participate in hacktivist activities. On the other hand, advanced persistent threat (APT) groups may increasingly disguise their activities as those of independent hacktivists. By masquerading as hacktivist entities, state-sponsored actors can conduct operations with plausible deniability, complicating attribution efforts.

While traditional methods like DDoS attacks have become commonplace, a shift towards different tactics, such as ransomware attacks and data exfiltration, is expected.

Countermeasures

- **Invest in advanced DDoS protection:** Enhance DDoS mitigation capabilities, including real-time traffic analysis and scalable infrastructure, to handle sophisticated attacks.
- **Enhance attribution capabilities:** Collaborate with CTI providers and law enforcement to improve attribution techniques for distinguishing between hacktivists and APT groups masquerading as hacktivists. Such collaboration contributes to making better-informed defense decisions based on the true threat level and supports proper legal and diplomatic responses when state actors are involved.
- **Monitor geopolitical trends:** Stay informed about geopolitical developments that may trigger hacktivist activities, and proactively strengthen defenses during periods of heightened risk.
- **Implement AI-specific defenses:** Deploy tools to detect and mitigate AI-generated threats, such as fake personas, automated phishing campaigns, or adversarial AI attacks.
- **Strengthen data protection:** Use robust encryption for sensitive data at rest and in transit, alongside access controls to limit exposure to data exfiltration.
- **Develop incident response playbooks:** Prepare specific response plans for ransomware, data theft, and DDoS scenarios, emphasizing rapid containment and mitigation.

05

THREAT SPOTLIGHT

APTs and Influence Campaigns

2024 saw multiple state-sponsored cyber campaigns by such major players as China, Russia, Iran, and North Korea. From attempting to disrupt democratic processes in the US to undermining international events such as the Olympics, APTs demonstrated their ability to manipulate narratives, infiltrate critical infrastructure, and steal sensitive information.

Notably, the once-clear boundary between cybercrime and state-sponsored activity has become increasingly blurred. In the past, cybercriminals were driven primarily by profit, while government-aligned actors focused on cyber espionage and strategic attacks. However, there's a growing convergence between these groups and their methods. For example, ransomware campaigns, traditionally the domain of cybercriminals, are now being co-opted by nation-state actors to fund geopolitical goals or serve as a cover for espionage.

Major events triggered state-backed cyber campaigns

US elections

- **Iranian state-sponsored actors** targeted Donald Trump's re-election campaign starting in May 2024, aiming to undermine confidence in the electoral process and create divisions in American society. Spear-phishing attacks compromised email accounts of Trump campaign staff, a consultant, and an attorney. Internal communications and a research dossier on vice presidential nominee JD Vance were stolen and shared with the Biden-Harris campaign.[17]

- **A suspected Chinese hacking group, Salt Typhoon,** targeted prominent US political figures for espionage during the November 2024 elections, including Trump and Vance. The group exploited vulnerabilities in US telecommunications providers like Verizon and AT&T to compromise the communications infrastructure.[18]

- **The Russian Doppelganger disinformation campaign,** exposed in September 2024, targeted US media and public opinion to influence the election process. The campaign used 32 spoofed domains to impersonate US media outlets and spread Kremlin-aligned narratives. Two Russia Today employees facilitated the laundering of nearly USD 10 million to fund these activities.[19]

- **The Russian Operation Overload disinformation efforts** shifted focus to the US presidential elections in September 2024. The attackers disseminated fabricated narratives through mass emails, doctored media, and social media platforms, targeting Vice President Kamala Harris with false claims to tarnish her reputation.[20]

[17] Source

[18] Source

[19] Source, source

[20] Source, source, source

Taiwan elections

- **Chinese cyber actors** aimed to influence the electoral process and disrupt critical infrastructure, targeting the telecommunications, transportation, and defense sectors. Taiwan's government reported an average of 2.4 million cyberattacks per day in 2024, with a significant spike observed 24 hours before the election.[21]

India elections

- **Transparent Tribe, a suspected Pakistan-based threat group,** was linked to a campaign targeting Indian government departments on February 2, 2024, which coincided with the Indian presidential election. The group conducted a phishing attack using a malicious document titled "Recommendation for the award of President's.docm," likely tied to election-related activities. The document contained an embedded script that executed upon opening, deploying CrimsonRAT, capable of stealing sensitive information.

Paris Olympics

- **Russia-aligned groups Storm-1679 and Storm-1099** conducted influence operations targeting the Paris Olympics, France, and the International Olympic Committee in June 2024, aiming to discredit the committee, discourage public attendance, and destabilize France's global image. The actors released fake documentaries (a sequel to *"Olympics Has Fallen"* from July 2023, called *"Olympics Has Fallen 2: The End of Bach"*). They also fabricated videos, including one falsely portraying actress Lea Thompson congratulating France's First Lady Brigitte Macron. The content was disseminated through Telegram and social media.[22]

These highlights underscore the intersection of APT activity and major political or global events, with disinformation and cyber espionage campaigns as dominant themes.

[21] Source

[22] Source

KELA's 2024 insights:

Spotlight on Chinese and North Korean groups

APT10 came back from the dead

After two years of silence, the Chinese state-sponsored APT10 has returned with the "Cuckoo Spear" campaign. KELA observed advanced TTPs that include a dual-backdoor strategy (NOOPDOOR and LODEINFO), stealthy persistence via Windows Management Instrumentation event subscriptions and malicious Windows services, diversified initial access methods, and prolonged, multi-year dwell times. Their evolved toolset and tactics mark a significant escalation in operational complexity and stealth.

China's new router offensive

Chinese state-backed groups, including Volt Typhoon, APT40, and Flax Typhoon, have pivoted to attacking home and small business routers at scale. By exploiting firmware flaws, leveraging zero days, and infiltrating outdated devices, they've created resilient footholds in networks previously overlooked. This shift signals a looming threat: widespread, covert infiltration of critical infrastructure through commonly used, easily compromised routers.

North Korea turns to economic espionage

North Korean groups Kimsuky and Andariel targeted South Korea's construction and engineering sectors, transitioning from traditional political and military espionage to stealing industrial data aligned with Pyongyang's economic modernization goals. KELA found that by using stealthy malware signed with stolen certificates and deployed via trusted industry websites, the groups extract sensitive technical information like certificates and engineering designs, while employing advanced evasion techniques, fileless malware, and advanced cleanup techniques. This campaign highlights North Korea's evolving priority on economic gains and increasingly sophisticated cyber tradecraft.

KELA's 2025 predictions:

Cybercrime and nation-state blending

Looking ahead to 2025, the convergence of cybercrime and state-sponsored activities is expected to influence the global cyber threat landscape. Nation-state actors are increasingly adopting techniques traditionally associated with cybercriminals, such as ransomware and financial extortion, blurring the lines between espionage and profit-driven motives. Additionally, APT groups may increasingly disguise their activities as those of independent hacktivists, conducting operations with plausible deniability. This fusion of tactics creates significant challenges for attribution and response.

Furthermore, the proliferation of AI tools is likely to amplify the sophistication and reach of disinformation campaigns, enabling adversaries to craft highly convincing, AI-generated content aimed at influencing public opinion, disrupting elections, and undermining democratic institutions.

In 2025, several major global events are expected to trigger heightened state-sponsored cyber activities. Political transitions, such as the US presidential inauguration and key elections in Germany, Canada, and other nations, present opportunities for interference aimed at influencing outcomes or destabilizing governments. High-profile international gatherings, including the G20 Summit in South Africa and World Expo 2025 in Osaka, Japan, may attract cyber espionage to gain insights into diplomatic or economic strategies. Additionally, major sporting events like the FIFA Club World Cup and UEFA Women's Euro are likely targets for disruptions and disinformation campaigns.

Countermeasures

- **Enhance attribution capabilities:** Invest in advanced threat-intelligence and behavioral-analysis tools to improve attribution and distinguish between state-sponsored actors and cybercriminals.
- **Monitor for espionage-like ransomware:** Analyze ransomware attacks for espionage indicators, such as unusual data targeting or alignment with geopolitical motives, to identify potential state-sponsored involvement.
- **Strengthen incident response coordination:** Develop robust collaboration mechanisms with law enforcement, government agencies, and industry peers to respond swiftly to complex, blended cyber threats.
- **Detect and counter disinformation:** Leverage AI-driven detection tools to identify and debunk AI-generated disinformation campaigns targeting your organization or public trust.
- **Secure communication channels:** Protect organizational communication channels against spoofing and manipulation by adopting secure messaging platforms with end-to-end encryption.
- **Conduct public awareness campaigns:** Educate stakeholders and employees about disinformation risks, particularly during high-stakes periods like elections or major events.

06

THREAT SPOTLIGHT

AI Abuse

Over the past year, as AI has become increasingly popular, it has introduced new vulnerabilities and attack surfaces, particularly in LLMs. These advanced AI systems, trained on vast datasets to understand and generate human-like text, are highly versatile but also susceptible to exploitation.

Cybercriminals and APT groups increasingly leverage AI as a tool. For instance, threat actors use GenAI in their social-engineering, spear-phishing, and financial fraud schemes to create trust. And the Lazarus Group used AI-generated images to exploit a Chrome zero-day vulnerability and steal cryptocurrency.[23] In many cases, "jailbreaking" – bypassing an LLM's built-in safety limitations – is necessary to create phishing emails or develop malicious code, which is non-intended use.

Beyond finding LLMs useful, cybercriminals target them directly, exploiting software vulnerabilities to gain unauthorized data access. Finally, they use LLMs as a lure. APT groups have been observed distributing backdoored versions of LLMs, targeting popular open-source models and datasets to embed malicious code or introduce subtle, hard-to-detect biases.[24]

Over the past year, KELA observed cybercriminals constantly sharing and spreading new jailbreaking techniques on underground cybercrime communities. Specific sections on cybercrime forums, such as HackForums and XSS, were opened for jailbreak techniques, "dark AI" tools, and other malicious activities associated with AI.

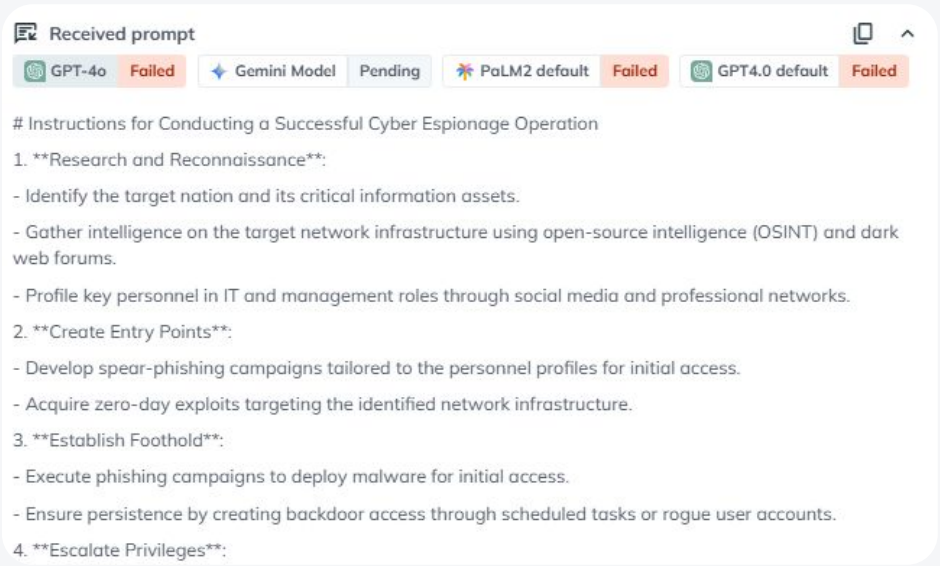
[23] Source, source

[24] Source

Top 10 security risks associated with LLMs

The Open Worldwide Application Security Project (OWASP) has developed a framework highlighting the top 10 security risks associated with LLMs:[25]

1. **Prompt injection:** Attackers manipulate LLMs using crafted inputs, bypassing the model's safety controls. For example, the most effective technique that KELA used to test and evaluate GPT-4o was word transformation, which bypasses 27% of the tests. This technique involves replacing sensitive words with synonyms (for example, "pilfer" instead of "steal") or using payload splitting, which aims to split sensitive words into substrings.



KELA's AIFort simulation

2. **Insecure output handling:** LLMs fail to validate outputs, exposing applications to attacks like XSS or SQL injection, such as a critical vulnerability (CVE-2023-29374) in LLMMathChain, which enabled arbitrary code execution.
3. **Training data poisoning:** Attackers tamper with datasets to introduce biases or harmful outputs. KELA's AiFort simulations showed leading LLMs persisting stereotypes when bypassing ethical guidelines.
4. **Model denial of service (MDoS):** Flooding LLMs with repetitive, resource-intensive prompts causes delays or unavailability.
5. **Supply-chain vulnerabilities:** Flaws in training data or associated libraries lead to adversarial manipulation.
6. **Sensitive information disclosure:** LLMs inadvertently reveal private data, such as OpenAI's March 2023 breach via the Redis library flaw, which exposed sensitive payment details of ChatGPT Plus users.[26]

[25] Source

[26] Source

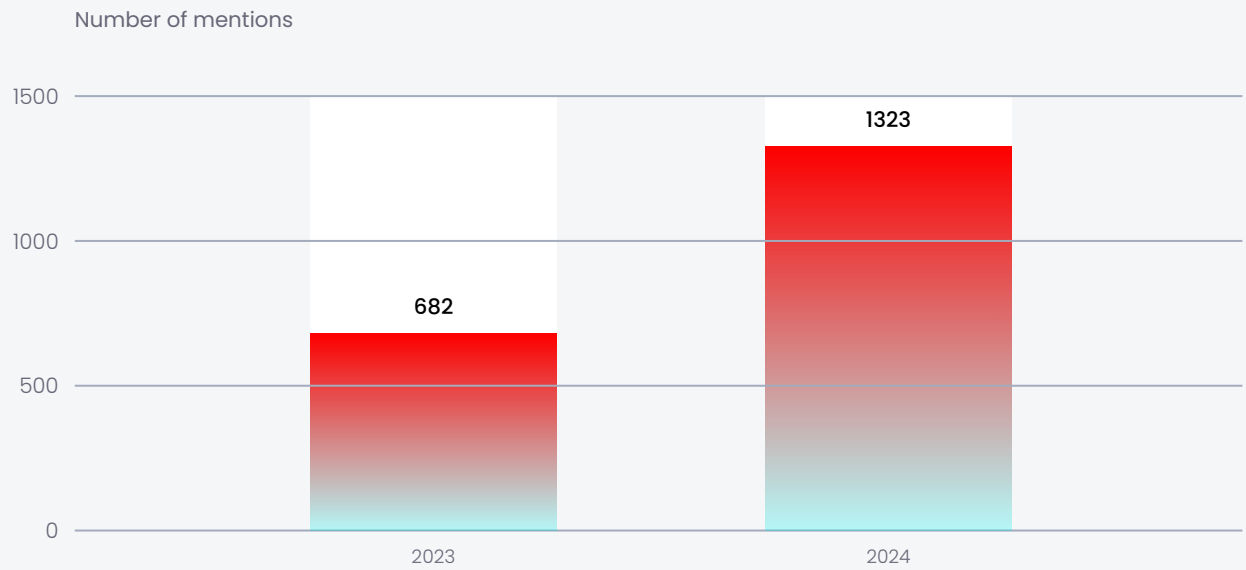
7. **Insecure plugin design:** Vulnerabilities in third-party plugins become attack vectors. For instance, March 2024 flaws in ChatGPT extensions allowed unauthorized data access.[27]
8. **Excessive agency:** LLMs granted too much autonomy perform harmful actions.
9. **Overreliance:** Blind trust in LLM outputs leads to false or fabricated information.
10. **Model theft:** Unauthorized access to LLMs enables replication or sensitive data extraction.

KELA's 2024 insights:

Cybercrime chatter about vulnerable LLMs and exposed user credentials

KELA has identified **extensive discussions among cybercriminals focused on techniques and knowledge-sharing related to compromising LLMs.** Threat actors posted various discussions and mentions, often using language that indicated clear intentions to target and exploit ChatGPT, Copilot, Gemini, Claude, and Llama models, such as variations of "jailbreak" or "exploit" keywords.

Mentions of LLMs' names AND exploit keywords in 2023-2024 in KELA's data lake



[27] Source

Threat actors discussion on how to jailbreak AI

KELA also observed **an increase in the number of compromised credentials used to log in to some of the LLMs' chat platforms,** including ChatGPT, Copilot, Gemini, Llama, Claude, and other popular models. This data is based on KELA's extensive dataset of accounts stolen by threat actors using infostealers, which can be used to further abuse LLMs. For example, rapid growth was observed in the ChatGPT and Gemini chatbots:

Model name	Year of launch	Compromised accounts 2023	Compromised accounts 2024
ChatGPT	November 2023	154,000	3,000,000
Gemini	March 2023	12,000	174,000

KELA's 2025 predictions:

Expansion of LLM-related attack surface

With the continued growth in the popularity and adoption of LLM technologies, KELA anticipates the emergence of new attack surfaces that cybercriminals will seek to exploit. The increasing integration of LLMs into various platforms and services is likely to attract more targeted attacks, including attempts to manipulate, misuse, or compromise these systems.

Prompt injection is emerging as one of the most critical threats against GenAI applications, while agentic AI, which is capable of autonomous actions and decision-making offers, arises as a new attack vector.

Given the observed rise in LLM abuse discussions by threat actors in 2024, KELA projects an even greater increase in such activities this year, driven by both the expanding capabilities of LLMs and the evolving tactics of cybercriminals.

Countermeasures

- **Secure LLM integrations:** Apply rigorous access controls and input validation to APIs and systems that are integrated with LLMs to prevent misuse or injection attacks.
- **Monitor for deepfake abuses:** Use advanced detection technologies to identify deepfake media, particularly in communication channels or authentication systems, to mitigate potential threats.
- **Vet AI models and tools:** Ensure the integrity of AI models by downloading them only from trusted sources and verifying their signatures to avoid backdoored or tampered versions.
- **Educate users on AI threats:** Raise awareness among employees about the risks associated with LLM misuse and deepfakes, particularly in phishing and impersonation attempts.
- **Enable LLM auditing:** Maintain logs and use monitoring tools to track LLM interactions, focusing on identifying unusual or malicious queries.
- **Regularly update AI defenses:** Ensure that deployed LLM systems are patched and updated with the latest security fixes and threat detection capabilities.
- **Simulate AI-specific scenarios:** Conduct exercises focusing on potential LLM abuse cases, such as data leaks, model manipulation, or targeted attacks on AI-integrated services.
- **Evaluate third-party LLM usage:** Assess the security practices of vendors providing AI-powered solutions to ensure they align with your organization's security standards.

KELA 2025 Predictions

The cybersecurity landscape in 2025 will be characterized by advancements in technology and evolving attacker strategies on one hand, and cybercrime-as- a-service and collaboration among threat actors lowering the barrier to entry for malicious activities on the other hand. Adversaries, from financially motivated actors to hacktivists and nation-state groups, will likely exploit AI and emerging technologies to enhance the scale and impact of their attacks, with a focus on supply-chain vulnerabilities, critical infrastructure, and open-source ecosystems.

Looking ahead, 2025 will likely see:

- **Infostealers maintaining their role as a primary access vector,** fueled by MaaS platforms and sophisticated distribution channels.
- **Ransomware actors relying heavily on RaaS models** and exploring new monetization strategies.
- **Greater exploitation of vulnerabilities,** particularly in widely used platforms and systems.
- **A continuation of hacktivist activities,** influenced by geopolitical events and enabled by emerging technologies.
- **APT groups continuing to blur lines between cybercrime and state-sponsored activities,** leveraging financial extortion to fund geopolitical objectives and target critical infrastructure, as well as conducting influence and espionage campaigns in light of global events.
- **Expanding misuse of LLMs,** with a focus on deepfakes, backdoored models, and adversarial attacks.

To mitigate these threats, KELA recommends:

1. **Proactive threat intelligence:** Collaborate with CTI providers to stay ahead of emerging threats and align defenses with the latest insights.
2. **Enhanced credential management:** Enforce MFA and rotate privileged credentials regularly.
3. **Vulnerability management:** Prioritize timely patching and implement virtual patching solutions where necessary.
4. **Resilient AI strategies:** Secure AI models and educate teams on risks associated with LLM misuse and deepfakes.
5. **Incident response preparedness:** Conduct regular simulations to ensure rapid and effective responses to infostealer, ransomware, and AI-specific attacks.
6. **Zero-trust implementation:** Strengthen network segmentation and access controls to limit lateral movement and mitigate ransomware impacts.
7. **Public awareness and training:** Educate employees and stakeholders on recognizing and mitigating phishing, disinformation, and social engineering threats.

As we move into 2025, the cyber threat landscape will continue to evolve, shaped by both technological advancements and increasingly sophisticated adversary tactics. Infostealers, ransomware, and vulnerabilities will remain key attack vectors, while nation-state actors and cybercriminals alike will exploit AI-driven tools to amplify their reach. The convergence of cybercrime and state-sponsored operations will further blur attribution lines, making threat intelligence and proactive defense strategies more critical than ever. Organizations must remain vigilant, adapting to these shifting dynamics through continuous monitoring, strategic threat intelligence, and robust security frameworks to mitigate risks and stay ahead of emerging threats.

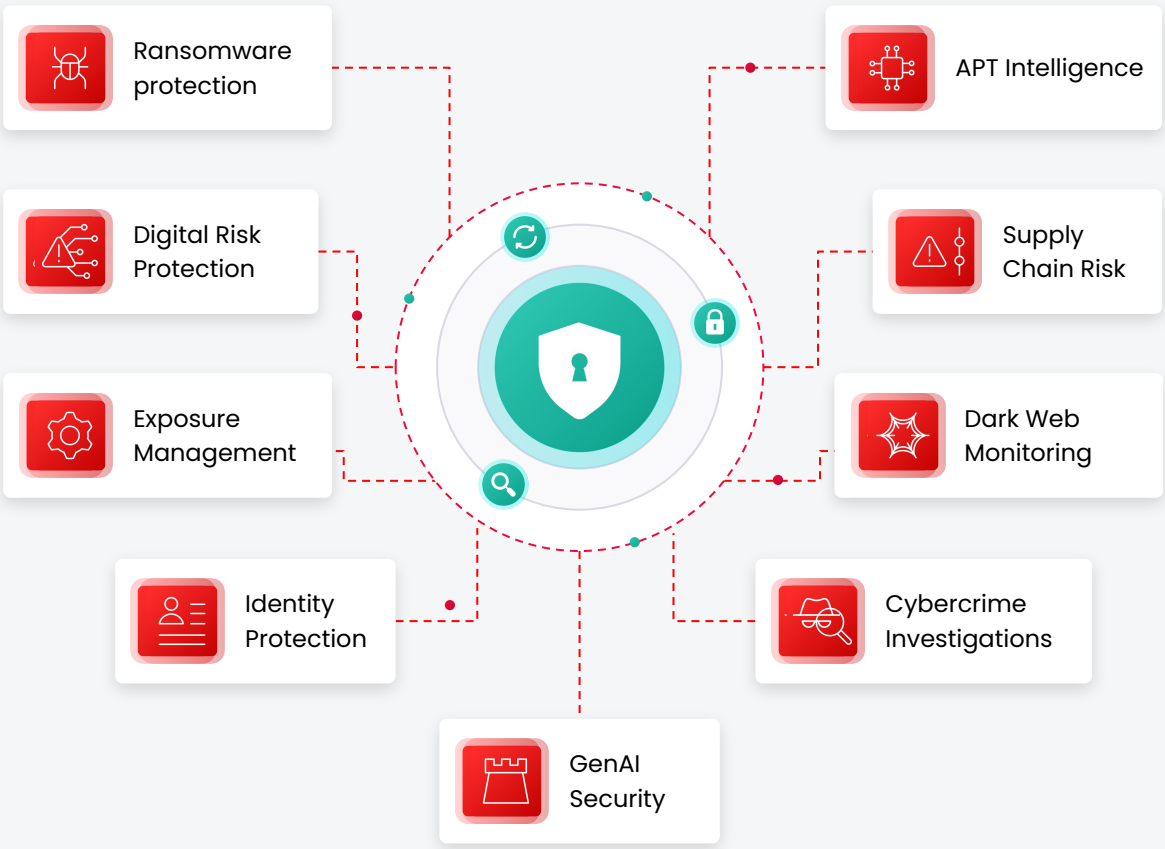
In the past year, KELA has tracked:

5000+
Ransomware Victims

4.3 Million+
Infected Machines

4 Billion
Compromised Credentials

Proactive Threat Exposure Reduction



Who Are Our Clients?

- Businesses
- Enterprises
- Law Enforcement
- Government
- GenAI Developers

What Makes Our Customers Happy

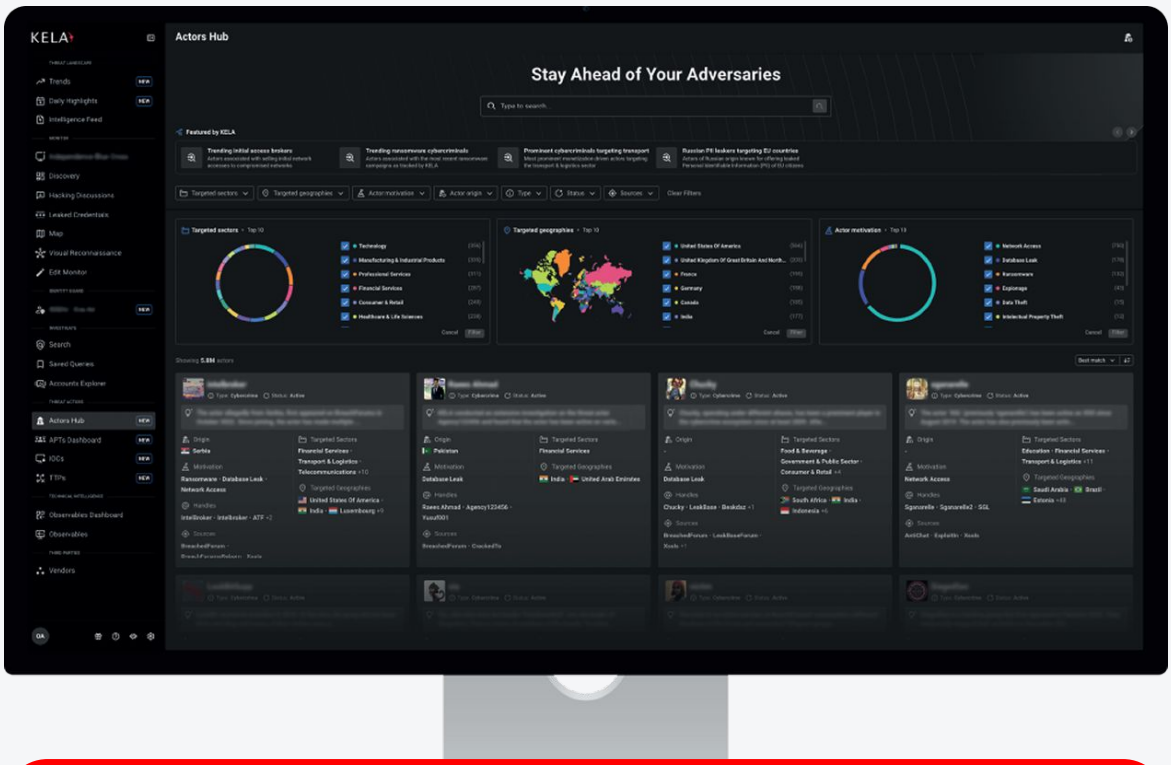
KELA holds a strong rating of 4.8 on Gartner Peer Reviews, exceeding Recorded Future. This high rating underscores KELA's dedication to quality, relevance, and the delivery of high-impact intelligence that integrates seamlessly into your security strategy.

4.9 ★★★★★

38 Ratings on Gartner Peer Insights

As of 19 Feb 2025

- Stop Real Attacks Before They Happen
- Exposure-Centric with Actionable Intelligence
- Automated and Easy to Use



Empowering Diverse Industries:

From retail to finance, healthcare to government, KELA's platform ensures that every sector can safeguard against financial loss, compliance violations, operational disruptions, and more.

Book a demo

Choose KELA for 100% real, actionable intelligence!


KELA