IT ISAC

CELEBRATING 25 YEARS OF THREAT INTELLIGENCE SHARING

NEW

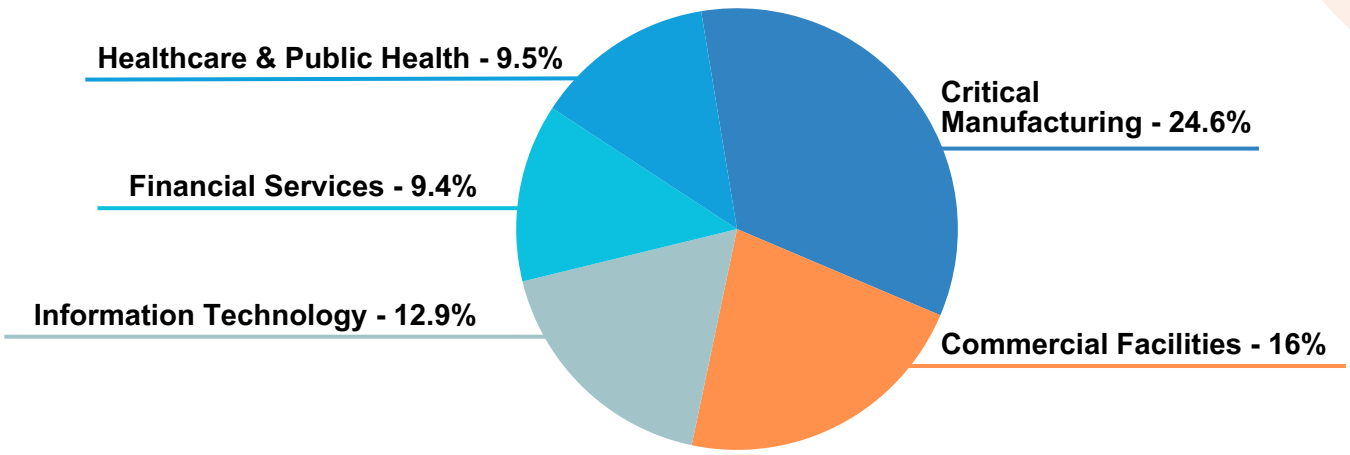
Quarterly IT Sector Ransomware Analysis

Q3 2025, July - September

Q3 2025 Analysis
July - September

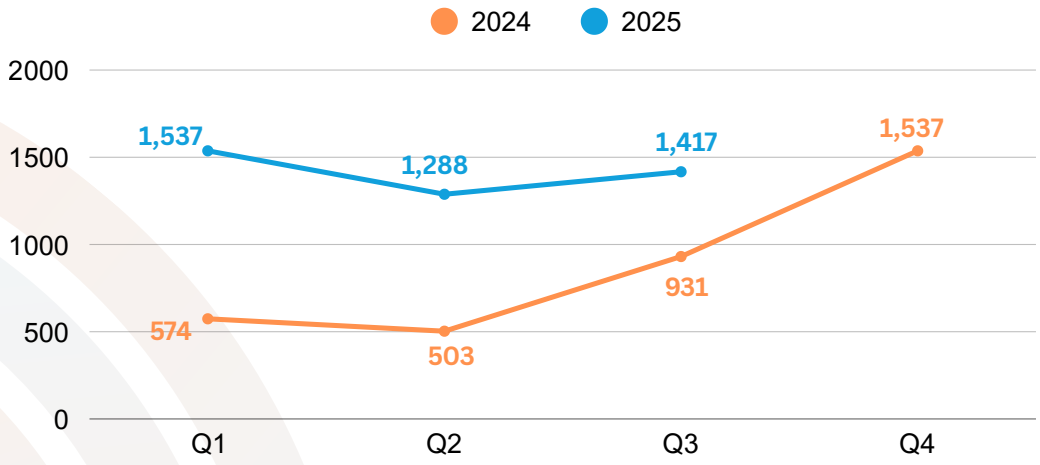
In Q3 2025, the Information Technology - Information Sharing and Analysis Center (IT-ISAC) recorded a total of 1,417 ransomware attacks, with the Critical Manufacturing, Commercial Facilities, and Information Technology sectors being the most frequent victims.

Q3 2025 Top Targeted Critical Sectors



In 2024, ransomware attacks saw a substantial increase towards the second half of the year, climbing from 503 in Q2 to 931 in Q3, and peaking at 1,537 in Q4. Based on metrics collected for Q3 2025, a similar pattern is unfolding. While the first two quarters of 2025 saw a decline from 1,537 (Q1) to 1,288 (Q2), Q3 2025 reversed that trend with an increase to 1,417 attacks. This suggests that ransomware activity is once again gaining momentum in the latter half of the year.

Yearly Ransomware Attacks 2024 vs. 2025

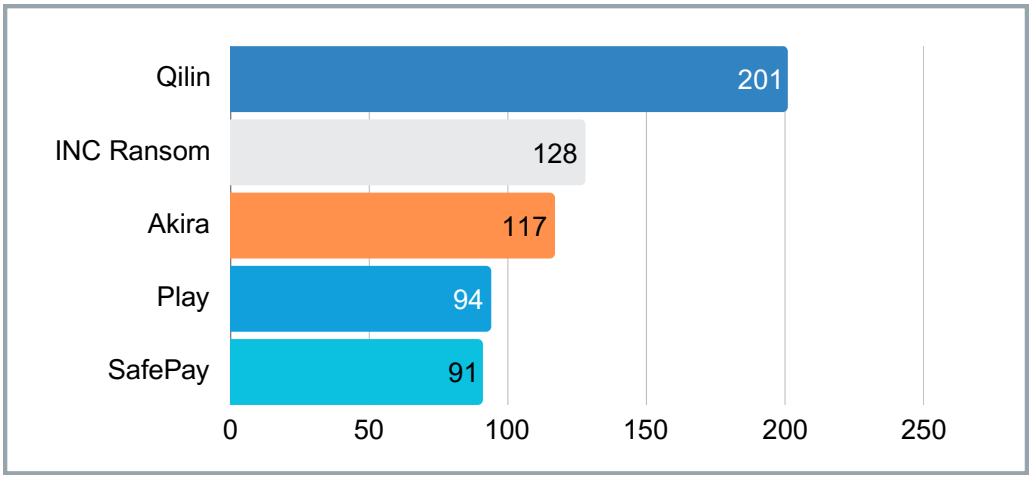


Q3 2025 Analysis
July - September

Qilin, INC Ransom, Akira, Play, and SafePay ransomware were the most active groups in Q3 2025, accounting for 44% of all ransomware attacks tracked during the quarter. While this lineup remains unchanged from Q2 of this year, the IT-ISAC observed a surge in activity from Inc. Ransom, with attacks from this group more than doubling from 52 observed attacks in Q2 2025 to 128 observed in Q3 2025. Of their observed Q3 2025 victims, 73 were based in the United States, followed by 12 in Germany and 10 in Canada.

This group typically gains initial access via spearphishing and the exploitation of known vulnerabilities (e.g. CVE-2023-3519), highlighting the need for organizations to apply system patches on a timely basis and to be cautious when interacting with emails or messages from unknown senders.

Q3 2025 Top 5 Ransomware Groups



RANSOMWARE TREND HIGHLIGHTS

Employment of Living-Off-The-Land (LOTL) Attacks to Evade Defenses:

These attacks involve exploiting legitimate system tools already present in the victim's environment, making detection difficult. Red Canary and Zscaler researchers have observed multiple campaigns abusing legitimate Remote Monitoring and Management (RMM) tools for covert remote access. These tools, normally used by IT admins, are being exploited by actors to blend into normal operations and deploy infostealers and potentially ransomware. In some cases, actors have been observed deploying two RMM tools in rapid succession for redundancy. If one RMM agent is removed, the second one remains as a silent, backup communication channel, enabling the actor to retain control over the compromised system.

Given that RMM software provides high-privileged access to an organization's entire network, it is crucial to conduct a thorough risk analysis before its deployment. If RMM is required, organizations should proactively engage with third-party vendors to understand and document the specific security controls they have implemented to protect the software.

Q3 2025 Analysis
July - September

Vulnerability Exploitation:

In Q3 2025, ransomware actors began exploiting vulnerabilities, including zero-days, in public-facing enterprise infrastructure and network edge appliances to gain initial access and facilitate data theft and extortion. During this period, Arctic Wolf Labs observed a surge in Akira ransomware activity, where the actors targeted SonicWall VPNs and firewalls, obtaining initial access through malicious SSL VPN logins. SonicWall linked these malicious logins to CVE-2024-40766, an improper access control flaw from a year ago. This suggests that the actors likely acquired credentials from unpatched systems, which were then used to authenticate against SSL VPN accounts.

In another campaign observed by Microsoft, a cybercriminal group, dubbed Storm 1175, exploited a critical deserialization zero-day flaw (CVE-2025-10035) in the GoAnywhere Managed File Transfer system. Storm 1175 targeted internet-exposed GoAnywhere instances vulnerable to CVE-2025-10035 for initial access. This was followed by the deployment of tools like RClone for data exfiltration, and ultimately Medusa ransomware to encrypt system files.

Google Threat Intelligence Group (GTIG) and Mandiant also uncovered a large-scale extortion campaign, allegedly linked to the CL0P ransomware group. This campaign entailed sending a high volume of emails to executives at numerous organizations, claiming the theft of sensitive data from the victims' Oracle E-Business Suite environments. Oracle acknowledged the campaign, reporting on October 2, 2025, that actors may have exploited vulnerabilities patched in July 2025. The company later directed customers on October 4 to apply emergency patches for CVE-2025-61882. Analysis by GTIG and Mandiant indicates that the CL0P extortion campaign followed months of intrusion activity. The actor used an exploit chain, possibly related to CVE-2025-61882, to target EBS customer environments as early as August 9, 2025, weeks before a patch was available.

Threat Actors Join Forces:

Ransomware operations are fundamentally changing, with threat actors moving past single-group attacks to form strategic, high-impact alliances. This shift aims to centralize expertise and resources, increasing the scale and success of cyber extortion campaigns. An example of this new, shared operational model is the "Trinity of Chaos," a collaboration between LAPSUS$, ShinyHunters, and Scattered Spider, three of the most notorious English-speaking cybercrime groups operating today. All three groups are known for their advanced social engineering capabilities, employing tactics like vishing, credential theft, and impersonating IT staff to manipulate employees into granting initial network access. While LAPSUS$ and Scattered Spider have long specialized in help-desk impersonation, ShinyHunters recently adopted these vishing techniques, most notably during the campaign against Salesforce environments.

With all three groups now collaborating, their combined operational capabilities have significantly expanded. Interestingly, Trinity of Chaos has shifted to a traditional ransomware operandi, with the announcement of a new ransomware-as-a-service (RaaS), dubbed "shinysp1d3r." Believed to be the first major RaaS offering from English-speaking cybercriminals, shinysp1d3r is under active development and is designed to encrypt VMware ESXi environments. Once operational, this service will likely attract affiliates, expanding Trinity of Chaos' reach and extortion potential.

In addition to shinysp1d3r, a new data leak site on the TOR network has been set up by Trinity of Chaos. The site already lists 39 companies impacted by cyberattacks, including the campaign targeting Salesforce instances. Although no new breaches have been disclosed yet, the creation of a new data leak site in coordination with the announcement of shinysp1d3r, indicates a potential for a new wave of attacks in the near future.

Growing Adoption of Artificial Intelligence (AI):

AI is reshaping the ransomware landscape, enabling actors to launch successful attacks. Notably, AI chatbots like ChatGPT and Gemini have been increasingly abused to generate tailored phishing emails, which are not prone to grammatical errors – a red flag that has historically been used to identify phishing and spam attempts. This, in turn, has made it easier for actors to gain initial access, tricking unsuspecting users into clicking on malicious links or attachments and leading to the deployment of ransomware.

In addition to helping attackers with their grammar, AI can help ransomware actors in other ways. Researchers at ESET recently uncovered what is believed to be the first known AI-powered ransomware, PromptLock. The malware is written in the Go Programming language. It uses the gpt-oss-20b model from OpenAI locally via the Ollama API to dynamically generate malicious Lua scripts on demand, which it then executes. These scripts are generated from hardcoded prompts and can enable actors to enumerate the local filesystem, inspect target files, exfiltrate selected data, and perform encryption. Although PromptLock has yet to be employed in attacks in the wild, and is believed to be a proof-of-concept or work in progress, its discovery points to how AI tools can be used to automate various stages of ransomware attacks.

Ransomware Brand Mimicry For Psychological Impact:

Q3 2025 saw a continued trend in actors impersonating well-known ransomware groups to extort funds from victims. At the beginning of the year, we observed actors sending ransom notes via email and physical letters, claiming to be from well-known groups like CL0P and BianLian. These notes informed victims of breaches and threatened to leak stolen data online if the victim refused to comply with the ransom demands. Similar activity has been recently spotted, with groups like Kawa4096 intentionally mimicking the branding and operational styles of more-established ransomware groups such as Akira and Qilin.

Q3 2025 Analysis
July - September

Akira and Qilin are dominant players within the ransomware landscape, accounting for a significant percentage of the total ransomware attacks observed by the IT-ISAC since the beginning of this year. Given the reputation of these groups, actors like Kawa4096 are seeking to use their notoriety to instill a sense of fear and credibility, enhancing the effectiveness of extortion. According to the AhnLab Security Intelligence Center, Kawa4096's ransom note shows notable similarities to that of the Qilin ransomware.

The content and format of the ransom note used by Kawa4096 are highly similar and almost identical to those deployed by the Qilin ransomware group. This note follows the typical double-extortion template, informing victims of the attack, detailing the theft of sensitive data, threatening public exposure, and providing instructions for negotiation and decryption. Using a note nearly identical to Qilin's Kawa4096 effectively amplifies the psychological pressure on victims to pay the ransom quickly. Additionally, Kawa4096's data leak site on the Tor network displays a visual similarity to that of the Akira ransomware group. Akira is known for using a distinctive retro-style Tor site, reminiscent of an 1980s green-screen console or command-line interface. By adopting a similar design, Kawa4096 attempts to instill the same level of fear and perceived credibility that the Akira ransomware group has garnered since its debut.

WHAT TO EXPECT THROUGH THE REST OF 2025

1 Zero-Day and N-Day Exploitation Against Internet-Facing Infrastructure:

Building on the momentum from Q3, ransomware operators are expected to continue leveraging vulnerabilities in public-facing enterprise infrastructure, particularly VPNs, file transfer systems, and business applications. The exploitation of older, unpatched flaws such as CVE-2024-40766, alongside recent zero-days like CVE-2025-10035 and CVE-2025-61882, highlights a persistent gap in timely patch management. As a result, Q4 will likely see continued or even increased exploitation of both known and unknown vulnerabilities, particularly those affecting widely deployed solutions with inadequate exposure management.

2 Coordinated, Multi-Group Campaigns

With the formalized alliance between LAPSUS$, Scattered Spider, and ShinyHunters under the "Trinity of Chaos" banner, Q4 will likely bring a new wave of joint campaigns that blur the lines between data theft, extortion, and ransomware deployment. These actors' combined expertise in social engineering and credential-based access makes them uniquely positioned to bypass traditional perimeter defenses. The launch of their TOR-based leak site suggests preparations for publishing new victim data, signaling that fresh, large-scale attacks are imminent.

3 Ransomware Targeting Cloud and Virtualized Environments

Looking ahead to Q4, ransomware operators are expected to increasingly pivot toward targeting cloud-based and virtualized infrastructure, as enterprises continue migrating critical workloads and data to hybrid and cloud-native environments. This is evidenced by the recent announcement of shinysp1d3r, which is currently under development by Trinity of Chaos. Designed to target VMware ESXi environments, shinysp1d3r highlights a strategic move by adversaries to tailor ransomware for the underlying infrastructure of many cloud deployments. While not yet operational, the emergence of shinysp1d3r indicates that threat actors are actively preparing to exploit the growing reliance on virtual machines and cloud platforms.

How We Collect Our Data

Note that metrics were obtained via open-source sites, the dark web, member input, and information shared between National Council of ISAC members. Due to outside assistance in monitoring ransomware attacks from partners and third parties, our metrics are likely biased towards the information technology and food and agriculture sectors.

ABOUT THE IT-ISAC

Operating for over 25 years, the IT-ISAC has served as the leading private-sector hub for threat intelligence sharing within the information technology sector. Founded in 2000, we are a nonprofit, member-funded, and member-driven organization dedicated to helping IT companies - and those that rely on IT for critical business operations - collaborate, manage cyber risks, and respond effectively to threats.

We provide a trusted, vendor-neutral forum where members can exchange actionable cyber threat intelligence, share best practices, and strengthen collective defense strategies. Our mission is to build a diverse community of organizations committed to cybersecurity, acting as a force multiplier to enable meaningful collaboration and enhance the security posture of all involved.

Learn more about the IT-ISAC by visiting it-isac.org or emailing us at membership@it-isac.org.