IT ISAC

CELEBRATING 25 YEARS OF THREAT INTELLIGENCE SHARING

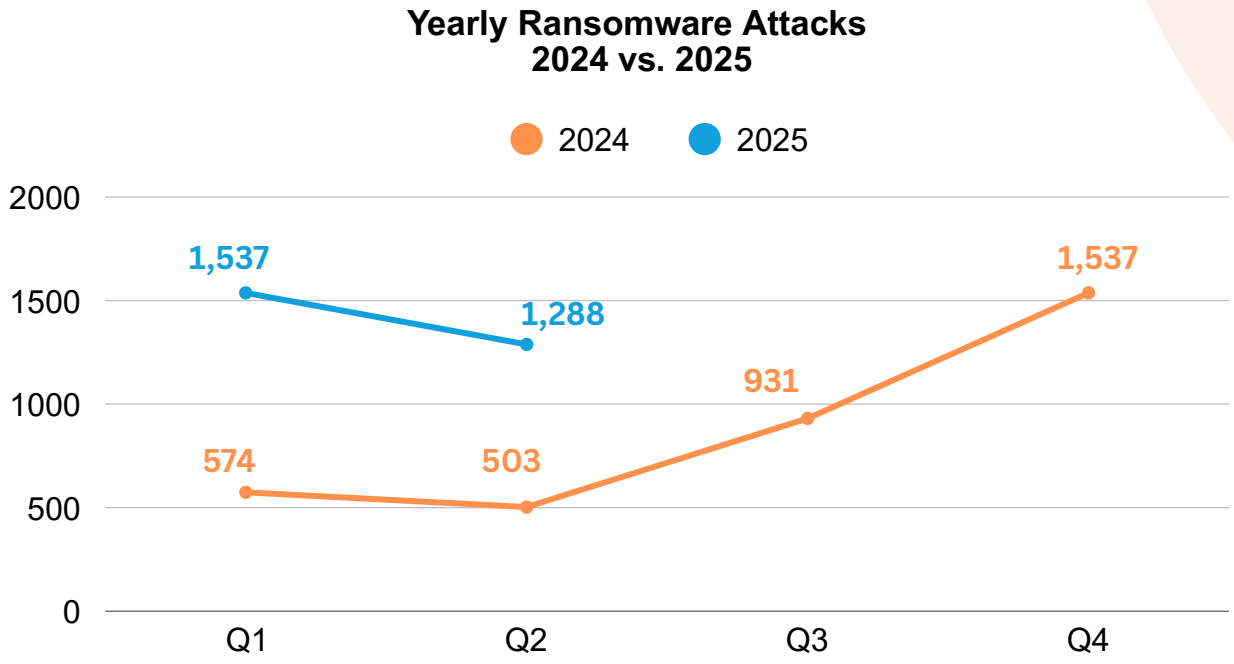
NEW

Quarterly IT Sector Ransomware Analysis

Q2 2025, April - June

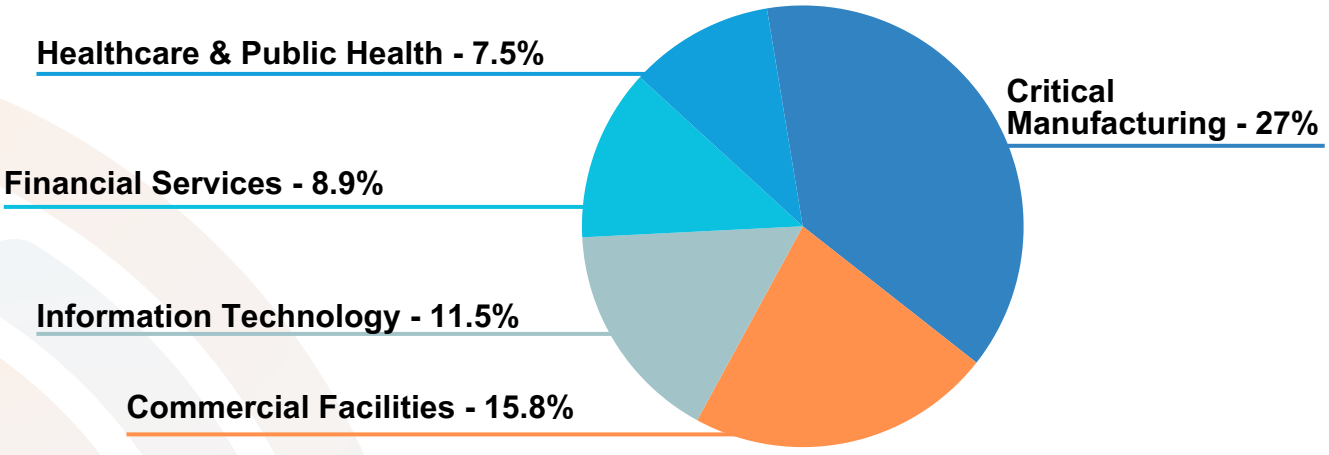
Q2 2025 Analysis
April - June

In the second quarter of 2025, the Information Technology - Information Sharing and Analysis Center (IT-ISAC) recorded a total of 1,288 ransomware attacks. Although this figure represents a decline compared to the 1,537 incidents reported in Q1 2025, it is more than twice the amount observed during the same period last year, when only 503 attacks were observed.



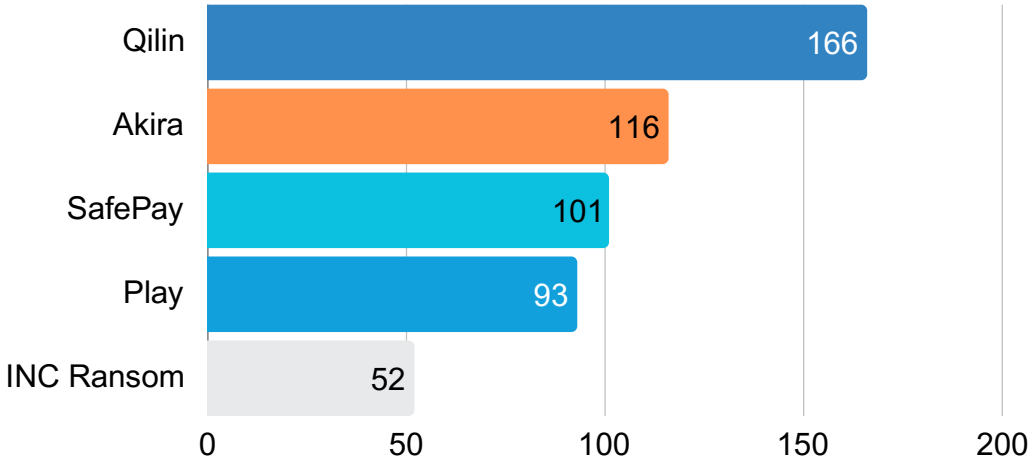
Highest-Targeted Industries Remain Consistent from Last Quarter

Consistent with trends observed in the first quarter of 2025, ransomware actors continued to focus their efforts on a specific set of industries in Q2 2025. The five most frequently targeted sectors were Critical Manufacturing, Commercial Facilities, Information Technology, Financial Services, and Healthcare and Public Health. These sectors remain particularly attractive to threat actors due to their operational importance, high-value data, and often time-sensitive services, which increase the likelihood of ransom payments being made. The continued targeting of these industries underscores the need for enhanced cybersecurity resilience and awareness.



Top Ransomware Actors in Q2 2025

Although the number of ransomware groups continues to grow steadily, five stood out in particular during the second quarter of 2025: Qilin, Akira, SafePay, Play, and INC Ransomware. These groups were especially active and played a prominent role in shaping the ransomware threat landscape during this period.



Qilin

Qilin ransomware, originally known as Agenda, has been active since October 2022 and has rapidly evolved into one of the most dominant ransomware groups of 2025. Operating as a Ransomware-as-a-Service (RaaS), Qilin has targeted over 310 organizations across more than 25 countries, with victims spanning finance, healthcare, manufacturing, law, and telecom sectors. The group's activity surged following the sudden shutdown of RansomHub in April 2025, likely due to an influx of former affiliates. In June alone, Qilin claimed 86 victims, far outpacing its rivals, and demonstrated a diversified targeting strategy, including high-value sectors and a notable increase in financial sector attacks. Qilin has also adopted advanced intrusion techniques, including exploiting critical Fortinet vulnerabilities (CVE-2024-21762 and CVE-2024-55591) to gain initial access via edge devices. With over $50 million extorted in 2024 and continued momentum into 2025, Qilin has firmly established itself as a leading ransomware threat.

Q2 2025 Analysis
April - June

Akira

Akira ransomware, first identified in March 2023, is a rapidly evolving RaaS group known for its distinct retro-themed data leak site and aggressive multi-extortion tactics. Victims are typically directed to a TOR-based portal to negotiate, and failure to pay results in the public release of stolen data. Akira targets large enterprises across a broad range of sectors, including education, finance, manufacturing, real estate, and healthcare, demanding ransoms from $200,000 to over $4 million. The group employs a wide array of tactics, techniques, and procedures (TTPs), including phishing, exploitation of public-facing applications, credential dumping (e.g., LSASS memory), and use of legitimate remote access tools like AnyDesk. Akira has recently refined its ransomware payloads, reverting from a Rust-based ESXi encryptor back to C++ variants, and now uses the ChaCha8 cipher for faster encryption. Notably, Akira has also focused on exploiting VPN vulnerabilities and leveraging valid accounts for initial access. While the group briefly experimented with data theft-only extortion in early 2024, it has since returned to its original double-extortion model, encrypting files and threatening data exposure to maximize pressure on victims.

SafePay

The SafePay ransomware group emerged in October 2024 and has quickly gained attention for its aggressive tactics and technical sophistication. Believed to be derived from leaked LockBit source code, SafePay encrypts files with a .safepay extension and drops ransom notes labeled readme_safepay.txt. The group operates a dark web leak site where it lists victims and offers stolen data for download to pressure organizations into paying ransoms, indicating a clear dual-extortion strategy. SafePay embeds most of its configuration directly into the binary, streamlining execution without requiring extensive command-line customization. It also features anti-analysis techniques, such as API hashing and obfuscation, and actively disables endpoint defenses using LOLBins, like PowerShell, to turn off Windows Defender. Data is typically exfiltrated using tools like WinRAR and FileZilla prior to encryption. The ransomware avoids execution on systems with Cyrillic language settings, suggesting an Eastern European origin. While current variants primarily target Windows environments, the group may expand to other platforms as it evolves.

Play

Play ransomware, also known as Playcrypt, began its operations in June 2022 and has since become a significant threat across North America, South America, and Europe, compromising nearly 900 organizations, including critical infrastructure. The group employs a double extortion model, encrypting systems while exfiltrating sensitive data. Play typically gains initial access through valid account abuse and the exploitation of public-facing applications such as FortiOS (CVE-2018-13379, CVE-2020-12812), Microsoft Exchange (ProxyNotShell), and SimpleHelp RMM (CVE-2024-57727). It leverages tools like AdFind for Active Directory reconnaissance, Grixba and GMER to disable antivirus software, and Mimikatz for credential harvesting. Lateral movement and persistence are achieved using Cobalt Strike, PsExec, and Group Policy Objects, while data exfiltration is carried out using WinRAR and WinSCP. Encrypted files receive the “.PLAY” extension, and ransom notes are deposited in public directories. The group has also developed an ESXi variant that targets virtual environments, demonstrating its expanding technical capabilities and aggressive operational scope.

INC Ransomware

INC Ransomware, first detected in July 2023, operates a double extortion scheme, using both private and public leak sites to pressure victims into paying. The private site requires credentials provided by the attackers and serves as a communication portal, while the public site hosts leaked data from non-compliant victims. Initially observed targeting Windows environments, INC Ransomware released a Linux variant in December 2023, followed by an updated Windows version in March 2024. The group gains initial access through spear-phishing and exploitation of known vulnerabilities, including CVE-2023-3519 in Citrix Netscaler ADC and Gateway. Once inside, Inc. Ransomware exfiltrates large volumes of sensitive data, such as employee records and corporate files, and threatens public exposure to coerce ransom payments.

Scattered Spider - Another Key Player in the Ransomware Landscape

During Q2 2025, we observed a surge in activity from Scattered Spider, a notorious cybercriminal syndicate known for its advanced social engineering tactics. While Scattered Spider is not officially branded as a ransomware group, the syndicate has a history of partnering with ransomware gangs such as ALPHV/BlackCat, Play, and more recently DragonForce (Microsoft has observed Scattered Spider deploying DragonForce ransomware, particularly within VMware ESX hypervisor environments) to carry out high-impact extortion campaigns.

A notable aspect about Scattered Spider is the systematic way it selects and targets victims. Scattered Spider has employed a pattern of concentrating on one sector at a time when launching attacks. Initially, in April 2025, the group targeted the retail sector, breaching prominent retailers like Marks & Spencer and Co-op. Since then, Scattered Spider has shifted focus to other sectors, including Insurance and more recently the Transportation and Aviation sectors. The focus on a single industry for weeks or months at a time, seems to be a strategic tactic implemented by Scattered Spider. By concentrating its efforts on one sector at a time, Scattered Spider is able to fine-tune its attacks around common workflows and security gaps specific to that sector, allowing the threat actor to maximize its operational efficiency.

As Scattered Spider continues its wave of attacks across different industries, it becomes imperative that organizations become familiar with the tactics, techniques, and procedures (TTPs) employed by this group and secure defenses accordingly. A new blog by Microsoft highlights updated TTPs and provides insights on defensive recommendations that organizations are advised to review. The blog post can be accessed here.

Q2 2025 Trends
April - June

Ransomware Tactics Are Evolving Beyond Financial Motives

Recent campaigns, such as the deployment of Fog ransomware against a financial institution in Asia, reveal that some actors are increasingly blending traditional ransomware techniques with cyber-espionage. In this case, attackers utilized legitimate employee monitoring software, such as Syteca, which is capable of screen capturing and keylogging, alongside advanced post-exploitation frameworks like GC2 and Adaptix C2. These tools enabled covert communication and long-term persistence within the network, a clear deviation from the typical 'smash-and-grab' model, where attackers encrypt, extort, and exit quickly. Additionally, the attackers implemented a persistence mechanism after encryption, indicating they intended to remain in the victim environment even after executing their payload. This combination of surveillance tooling, sophisticated lateral movement, and strategic footholds suggests a dual-purpose campaign where financial extortion may have been secondary to intelligence collection or broader espionage objectives. It marks a growing trend where ransomware is no longer just a profit-driven attack vector but also a covert access tool for prolonged reconnaissance.

The Ransomware Ecosystem Remains Highly Adaptive

The abrupt disappearance of RansomHub in April 2025 illustrates how the ransomware landscape is driven by rapid shifts in group infrastructure and affiliate loyalties. Within days of RansomHub going offline, Qilin ransomware activity surged, as displaced affiliates were absorbed and its operations expanded. This swift redistribution of resources highlights the resilience of the ransomware-as-a-service model and the agility of threat actors in regrouping under new banners, thereby preserving their operational continuity despite internal collapses or external pressure.

Ransomware Groups Are Shifting Tactics Toward Extortion-Only Models

Hunters International, a well-known RaaS operation, recently announced its official shutdown and stated that it will provide free decryption tools to assist victims in recovering their encrypted data without having to pay ransoms. Hunters International, which has been active since late 2023, was responsible for nearly 300 global ransomware attacks that affected various organizations, including government entities, healthcare networks, and major corporations. In a recent statement posted on its dark web leak site, the group stated that the decision to end operations was not made lightly and acknowledged the impact it had on the affected organizations.

"After careful consideration and in light of recent developments, we have decided to close the Hunters International project. This decision was not made lightly, and we recognize the impact it has on the organizations we have interacted with," the cybercrime gang stated in a message posted to its dark web leak site.

Although the group did not detail the "recent developments" prompting the closure, it follows an announcement from Hunters International in November 2024, citing increased law enforcement scrutiny and diminishing profitability as reasons for winding down. As part of their exit, Hunters International removed all entries from its extortion portal and offered guidance to victims on how to request decryption support.

While the gesture of releasing free decryptors by a ransomware gang may appear altruistic, it's more likely a strategic retreat in response to mounting legal and operational risks. Offering decryptors could be an attempt to reduce legal exposure or soften future prosecution. However, it also undermines the criminal model of ransomware by enabling victims to recover data without payment, which could set a precedent and embolden more resistance against ransomware demands. Furthermore, it may indicate a shift in cybercriminal tactics toward extortion-only models, such as "World Leaks," where data theft without encryption is harder to trace and prosecute, yet equally damaging.

Q2 2025 Takeaways
April - June

In Q2 2025, the ransomware landscape demonstrated heightened sophistication and adaptability, with threat actors blending traditional ransomware tactics with long-term persistence and espionage techniques. The abrupt disappearance of major ransomware players, such as RansomHub, coupled with the rapid expansion of competitors like Qilin, highlights the ecosystem's dynamic and resilient nature. Additionally, the shift by groups like Hunters International toward extortion-only models, marked by the release of free decryptors and a move away from direct encryption, reflects evolving strategies in response to intensified law enforcement scrutiny and changing market pressures. These developments underscore an increasingly complex threat environment, demanding more comprehensive and proactive cybersecurity defenses. To navigate this evolving threat landscape, organizations must prioritize cyber resilience and consistently follow established best practices to mitigate risks. Referencing CISA's StopRansomware Guide, implementing layered defenses, maintaining offline backups, and conducting regular incident response exercises are crucial steps in protecting against potential ransomware attacks.

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.