IT ISAC

CELEBRATING 25 YEARS OF THREAT INTELLIGENCE SHARING

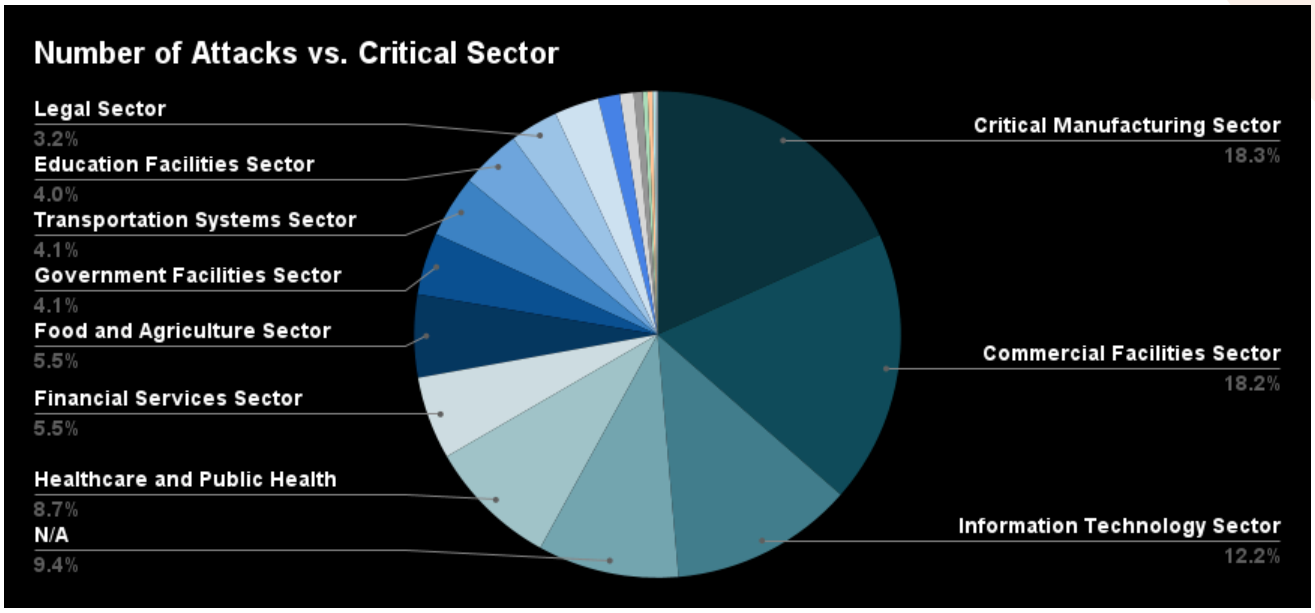
NEW

Quarterly IT Sector Ransomware Analysis

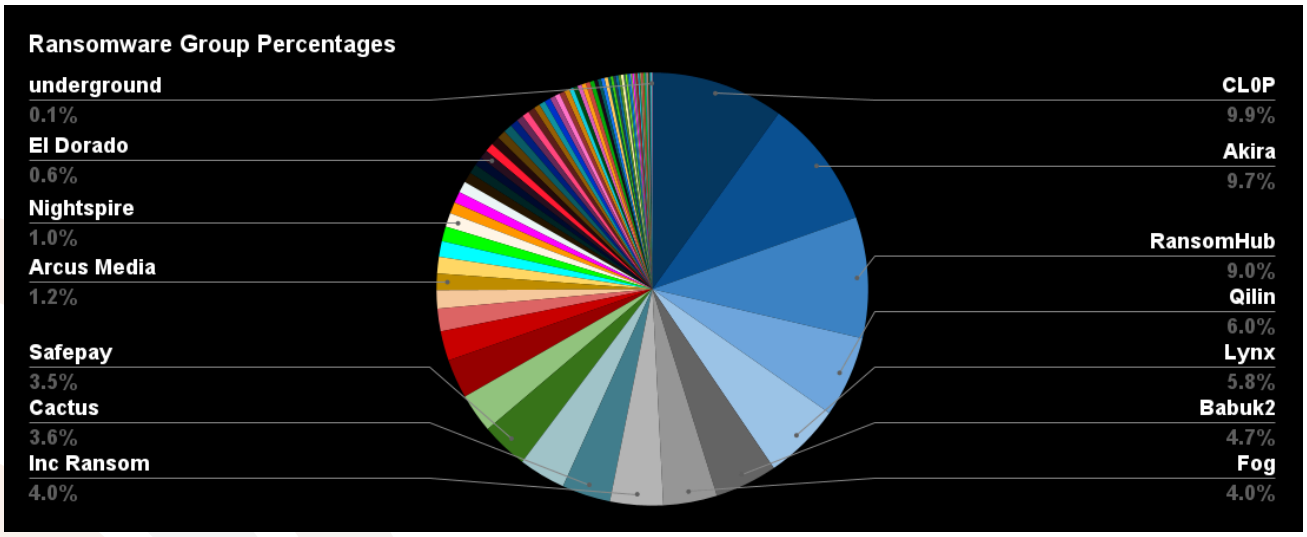
Q1 2025, January - March

Q1 2025 Analysis
January - March

In the first quarter of 2025, the Information Technology - Information Sharing and Analysis Center (IT-ISAC) recorded a total of 1,537 ransomware attacks, highlighting a 1.51% increase over the previous quarter (1,514 attacks observed in Q4 2024). Compared to Q1 2024, where we recorded 572 attacks, ransomware activity has nearly tripled year-over-year. The top three targeted sectors this quarter were critical manufacturing, commercial facilities, and information technology, which together accounted for 28.7% of all ransomware attacks.

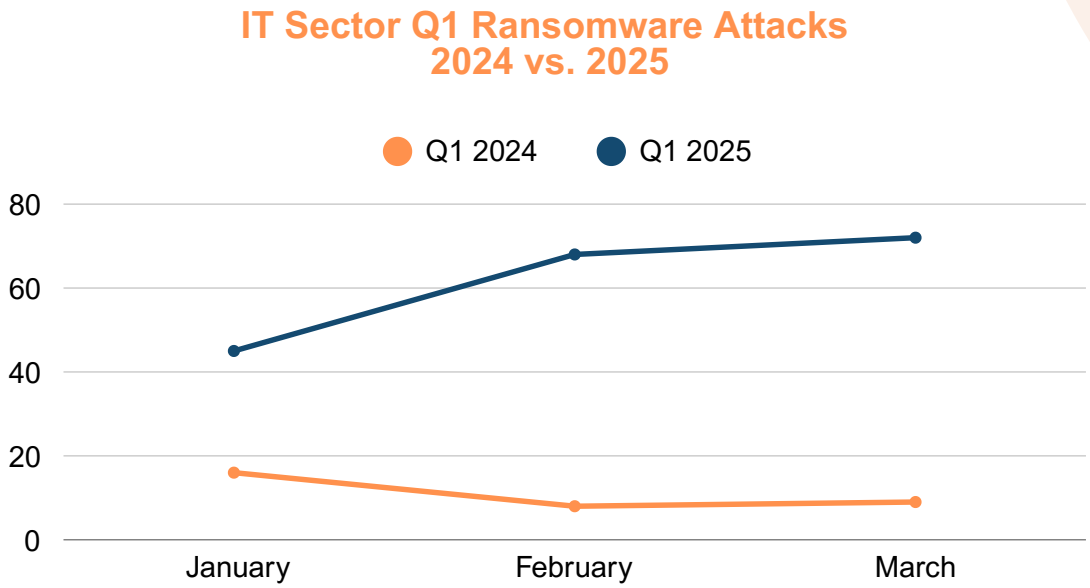


Leading the forefront were the ransomware groups CL0P, Akira, RansomHub, Qilin, and Lynx, which together were responsible for 40% of all attacks observed in Q1 2025.



Q1 2025 Analysis Cont'd

The IT sector experienced a surge in ransomware attacks during Q1 2025 compared to the same period in 2024. This increase can be attributed to several key factors, including the exploitation of newly disclosed vulnerabilities, the growing accessibility of Ransomware-as-a-Service (RaaS) platforms, and perhaps most notably law enforcement disruptions targeting major ransomware groups, such as the takedown of BlackCat in late 2023 and LockBit's infrastructure in February 2024.



CL0P's Dominance in Ransomware Attacks

In Q1 2025, CL0P maintained its position as one of the most prominent ransomware groups, responsible for approximately 10% of all observed attacks during the quarter. A key part of CL0P's recent activity has centered on the exploitation of CVE-2024-50623, a zero-day vulnerability in Cleo's managed file transfer platforms —specifically, Harmony, VLTrader, and LexiCom. Organizations commonly use these platforms for secure file exchanges, and the vulnerability allows for unrestricted file uploads and downloads, enabling attackers to infiltrate networks, steal sensitive data, or achieve remote code execution. In mid-December 2024, CL0P exploited CVE-2024-50623 to compromise and exfiltrate data from dozens of victims. The CL0P group listed over 60 organizations on its data leak site as part of the Cleo campaign, but noted these were only entities that had been contacted and failed to respond, indicating the true number of affected organizations was likely higher.

By March 2025, CL0P's data leak site showed another surge in publications, with over 150 organizations listed at the time of writing. These new victims seem to have been added as a result of CL0P's December attack on users of Cleo's file transfer solutions. While it remains uncertain whether this represents the complete list of victims or if CL0P is still exploiting vulnerable Cleo instances, organizations using the file transfer solution should prioritize applying the latest patches immediately to mitigate potential attacks.

Q1 2025 Ransomware Trends Observed

1 Impersonation of Ransomware Groups for Extortion

A growing trend in the cybercrime landscape is that of fraudsters who mimic well-known ransomware groups like CL0P and BianLian to extort money from victims. This tactic is becoming more widespread, with attackers increasingly using the reputations of established ransomware groups to enhance the credibility and urgency of their demands. For instance, impersonators of CL0P are attempting to capitalize on the group's notoriety and the fear of data exposure by sending ransom notes that pressure organizations into paying. In one such case, the attackers posed as CL0P and claimed to have successfully exploited a vulnerability in Cleo's managed file transfer platforms. They asserted that this exploitation granted them unauthorized access to the victim's network, allowing them to steal sensitive data. To add legitimacy to their claims, the attackers included a link to a media blog post reporting that CL0P had stolen data from 66 Cleo customers using this method.

Additionally, the BianLian group has been a target for impersonation as well. The FBI issued a warning that fraudsters have been sending physical letters through the United States Postal Service, claiming to be from the BianLian group. These letters assert that the attackers have compromised corporate networks and stolen sensitive data, threatening to leak it unless the recipient agrees to pay a ransom.

This tactic of impersonating notorious ransomware groups amplifies the threat of extortion, as it preys on the fear of reputational damage or data breaches. It also blurs the lines between different types of cybercrime, making it more difficult for organizations to discern genuine ransomware attacks from simple fraud.

2 Shift Towards Vulnerability Exploitation and Persistent Extortion

Traditional ransomware attacks, which typically involve encrypting a victim's data and demanding payment for decryption keys, are increasingly being replaced by more nuanced and persistent extortion tactics. Today, groups like SecP0 are shifting tactics to focus on discovering critical vulnerabilities in widely used systems and threatening to disclose these flaws to the public unless a ransom is paid.

SecP0 recently claimed to have identified weak encryption practices in Passwordstate's database, which could allow attackers to steal sensitive credentials. Given that many organizations rely on Passwordstate to manage their passwords, this flaw could potentially allow malicious actors to access sensitive credentials, which could then be used to gain unauthorized entry into organizational networks and systems.

Overall, by threatening to publicly expose vulnerabilities, groups like SecP0 can apply prolonged pressure on organizations, forcing them to pay ransoms to avoid reputational damage, legal ramifications, or further system exploitation. This method provides a more sustained form of leverage compared to traditional encryption-based attacks, as the threat remains hanging over the victim for an extended period, making it more difficult for them to recover or secure their systems.

Q1 2025 Analysis Cont'd

Overall, Q1 2025 has witnessed several significant developments in the ransomware landscape. CL0P continued its dominance, particularly by exploiting vulnerabilities in Cleo's file transfer platforms. The quarter also highlighted a disturbing rise in the impersonation of notorious ransomware groups, such as CL0P and BianLian, by fraudsters seeking to extort organizations using fear tactics. Additionally, the trend towards vulnerability exploitation and persistent extortion tactics is gaining traction, with groups like SecP0 shifting focus from traditional encryption-based attacks to threats involving the public disclosure of critical vulnerabilities. These evolving tactics underscore the increasingly complex and pervasive nature of threat actors, making it essential for organizations to remain vigilant and proactive in securing their systems.

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 ag 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.