IT ISAC

CELEBRATING 25 YEARS OF THREAT INTELLIGENCE SHARING

Exploring the Depths:

Analysis of the 2024 Ransomware Landscape and Insights for 2025

Includes 2024 Quarterly Analyses!

To better understand ransomware attacks and trends, the Information Technology - Information Sharing and Analysis Center (IT-ISAC) started tracking ransomware attacks in 2020. To date, we have tracked over 8,600 ransomware incidents. To monitor and summarize the activity of threat actors, the IT-ISAC team built its own scripts and tools to build lists of ransomware events. By doing this, we have been able to automate information gathering from across public reports, RSS feeds, and internal threat intelligence.

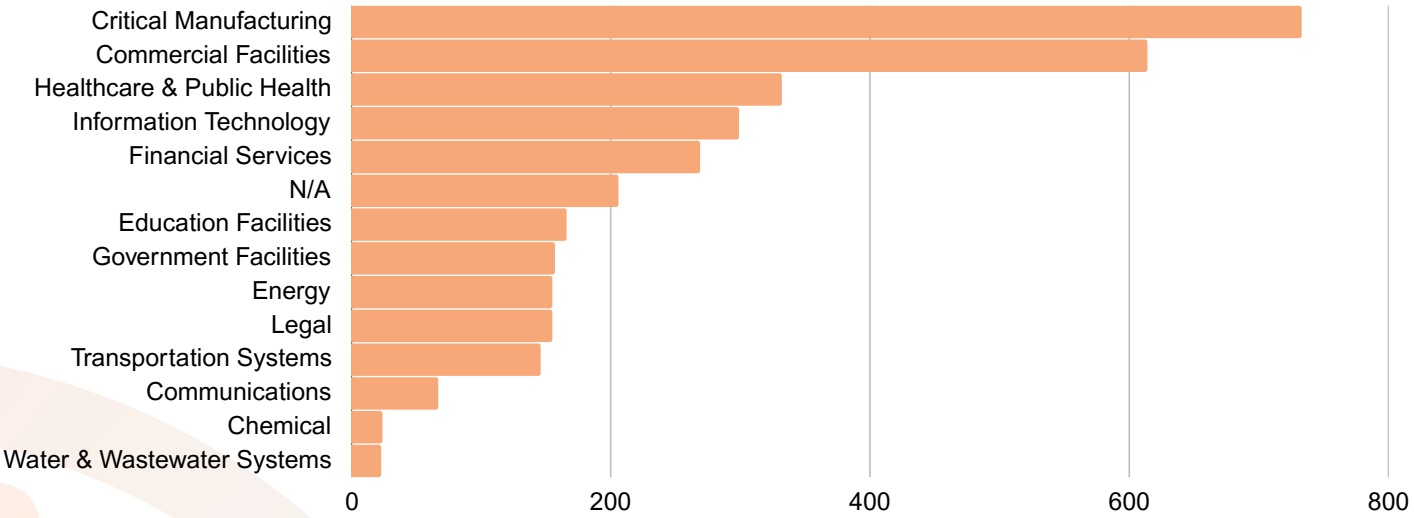
The IT-ISAC team performs detailed analyses by investigating the ransomware groups involved, their operational methods, and the context surrounding each incident. This process includes cross-referencing the data with open-source intelligence (OSINT), industry reports, and internal members' contributions to address gaps such as the affected sector, geographic location, attack timeline, and possible entry points used by the attackers.

The IT-ISAC ransomware tracker database is a collaborative resource accessible to IT-ISAC members and acts as a central hub for monitoring ransomware incidents. By promoting teamwork, the database allows members to analyze trends together. This joint effort improves the capacity of all participants to remain informed and ready, bolstering the overall resilience of the IT-ISAC community against ransomware attacks.

When the IT-ISAC team and its member companies identify new and emerging ransomware groups and incidents, we build comprehensive Adversary Attack Playbooks for them). These playbooks provide in-depth analysis of the groups' tactics, techniques, and procedures (TTPs), equipping members with valuable intelligence to enhance their cybersecurity defenses. The IT-ISAC has developed Adversary Attack Playbooks for approximately 237 threat actors, including detailed intelligence on 86 ransomware operators.

The IT-ISAC tracked approximately 3,500 ransomware incidents in 2024, up from 3,000 in 2023. The steady increase over the years is attributable to an improved ability to track ransomware attacks and an increased level of attacks. We monitored attacks across multiple critical infrastructure sectors.

ATTACKS BY CRITICAL INFRASTRUCTURE SECTOR IN 2024

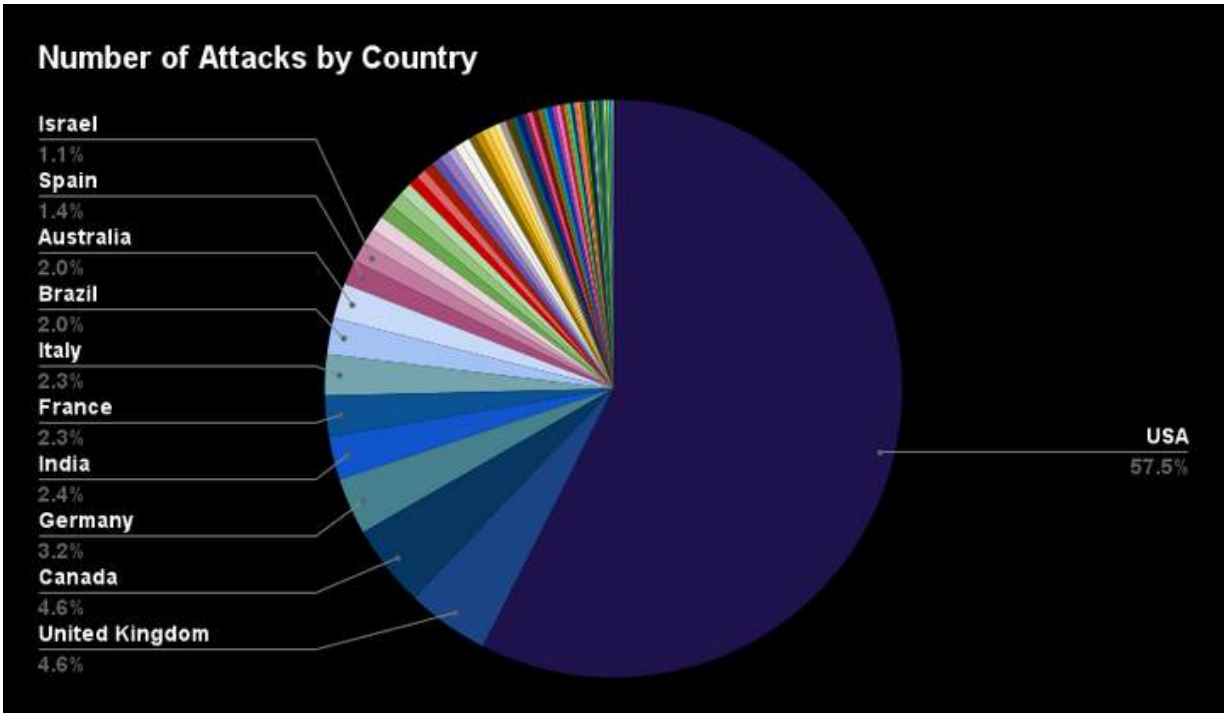


- The **Critical Manufacturing Sector** saw the highest number of attacks we tracked, experiencing 733 attacks (accounting for 20% of all incidents).
- Following closely, the **Commercial Facilities Sector** saw 614 attacks (17%).
- The Healthcare and **Public Health Sector** saw 332 attacks (9%).
- The **Information Technology Sector** was affected by 299 attacks (8%).
- Additionally, the **Financial Services Sector** experienced 269 attacks (7%).
- Finally, the **Food and Agriculture Sector** accounted for 206 attacks (5%).

ATTACKS BY COUNTRY

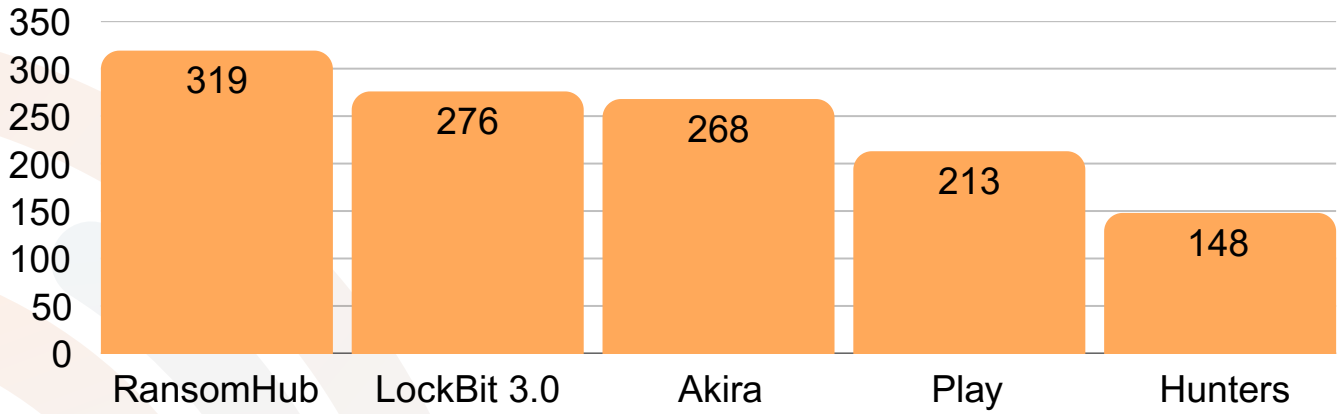
Geographically, our data suggests that ransomware attacks are highly concentrated in the United States. The US accounts for the majority of incidents, with 1,984 attacks (57%), reflecting its position as a significant economic and technological hub. All other countries saw less than 160 attacks (under 5%).

The US is also one of the world's largest economies, housing many high-value corporations and critical infrastructure components. Thus, it is a prime target for ransomware operators who seek to enrich themselves and create chaos.



TOP 5 RANSOMWARE STRAINS

The top five ransomware strains in 2024 were RansomHub, LockBit, Akira, Play, and Hunters International. Together, these five groups accounted for approximately 35% of all ransomware attacks recorded by the IT-ISAC in 2024, highlighting their significant impact on the ransomware landscape.



RansomHub - 315 Attacks

RansomHub initiated operations in February 2024 and has since exfiltrated data from over 300 victims across multiple critical infrastructure sectors, including water and wastewater, information technology, government services, healthcare, emergency services, food and agriculture, financial services, commercial facilities, critical manufacturing, transportation, and communications.

Operating under a ransomware-as-a-service (RaaS) model, RansomHub recruits affiliates to gain initial access to victim environments and deploy the ransomware on its behalf. In return, affiliates receive a substantial portion of the ransom payments, with RansomHub offering 90% of the total ransom to its affiliates, keeping only 10% for itself. This high payout structure has attracted numerous affiliates, allowing the group to rapidly expand its operations and even surpass LockBit as one of the most active ransomware groups in 2024. A prominent affiliate of RansomHub is Scattered Spider, a cybercrime group known for its sophisticated social engineering tactics. Scattered Spider has been active since 2022 and formerly an affiliate of BlackCat, this group excels in using English-language social engineering to target victims in Western regions. The group is also notorious for its use of SIM swapping and MFA fatigue attacks to bypass multi-factor authentication and compromise user accounts.

LockBit - 276 Attacks

LockBit, initially known as 'ABCD' ransomware, emerged in late 2019 and quickly became the most widely deployed ransomware variant by 2022, targeting both large and small organizations across the world. LockBit operates as a RaaS model, with a core team developing the malware and maintaining the website while affiliates conduct attacks using the tools and infrastructure.

Affiliates of LockBit gain initial access to victim environments through various methods, including the exploitation of remote desktop protocol (RDP), drive-by compromise attacks, phishing campaigns, abuse of valid accounts, and vulnerabilities in public-facing applications. Once access is established, affiliates deploy the LockBit ransomware strain, which is capable of enumerating system information, terminating processes and services, and deleting log files and shadow copies, thereby complicating recovery efforts. In line with many modern ransomware groups, LockBit employs double extortion tactics, encrypting victim files while also exfiltrating sensitive data and threatening to release the files on its public leak site if the ransom is not paid. To facilitate data exfiltration, affiliates utilize Stealbit, a custom tool developed by LockBit, along with open-source tools like RClone, a cloud storage manager, and file-sharing services such as MEGA. LockBit ransom demands typically range from several hundred thousand dollars to millions of dollars, depending on the size of the victim organization and the perceived value of the stolen data.

Akira - 268 Attacks

Since its inception in early 2023, Akira ransomware has compromised hundreds of victims globally, with a particular impact on large enterprises across sectors such as healthcare, finance, and manufacturing. The group typically gains initial access through phishing campaigns or by exploiting vulnerabilities, especially in Cisco and SonicWall firewall and VPN appliances. Once inside the network, the attackers establish persistence by creating new domain accounts and further use tools like Mimikatz and LaZagne to extract credentials, enabling privilege escalation and lateral movement. Akira deploys specialized ransomware variants for different system architectures, including the Windows-specific "Megazord" and "Akira_V2," which target ESXi servers.

In addition to encryption, Akira employs double extortion tactics, exfiltrating sensitive data via tools like FileZilla, RClone, and WinSCP to pressure victims into paying ransom demands. These demands typically range from several hundred thousand to millions of dollars, depending on the scale and profile of the targeted organization.

Play Ransomware - 213 Attacks

Play ransomware, first identified in mid-2022, is a sophisticated strain that impacts organizations across various sectors. It employs a double extortion tactic, encrypting victim data while exfiltrating sensitive information to pressure victims with the threat of public exposure. Notably, Play uses a custom encryption mechanism marked by the string "PLAY" at the beginning of encrypted files and incorporates intermittent encryption to increase speed and evade detection. The ransomware has been seen in a range of critical infrastructure companies, government agencies, and large enterprises.

Attackers leverage vulnerabilities in publicly accessible systems such as VPNs and RDP servers and frequently use phishing emails for initial access. Tools like Cobalt Strike and Metasploit are deployed for post-exploitation activities, with additional credential-stealing techniques like Mimikatz aiding lateral movement and security evasion. Unlike many ransomware groups, Play does not leave a traditional ransom note but instead uses a minimalistic file titled "README.txt" containing instructions for negotiations.

Play ransomware has been linked to significant attacks, including those exploiting vulnerabilities in Microsoft Exchange servers (e.g., ProxyNotShell). In recent developments, the Play ransomware group has expanded its operations by deploying a new Linux variant that specifically targets VMware ESXi environments. This shift indicates an adaptation to compromise virtualized infrastructures, which are commonly used in enterprise settings. Additionally, there have been reports of collaboration between North Korean threat actors and the Play ransomware group, signaling a possible shift in tactics and alliances within the cybercriminal landscape.

Hunters International - 148 Attacks

Hunters International is a RaaS operation that has claimed over 200 victims since its inception in October 2023. The ransomware, written in Rust, is designed to evade detection, accelerate encryption, and ensure compatibility across multiple platforms. It shares code similarities with Hive ransomware but improves on its predecessor by streamlining command-line options and optimizing key management. The actors behind Hunters International typically gain initial access by exploiting vulnerabilities in public-facing applications. Once inside, they use tools such as Plink, Impacket, AnyDesk, and TeamViewer for lateral movement. Hunters International is primarily focused on stealing data rather than merely encrypting it, using file-sharing solutions such as MEGA to facilitate exfiltration.

The group adopts an indiscriminate, opportunistic approach when targeting victims, seeking to maximize ransom payouts by exploiting a wide range of organizations, both small and large, from different industries and sectors. Ransom demands from Hunters International have reportedly reached over $10 million, varying depending on the victim's size and profile.

NOTABLE ATTACKS

Some of the most high-profile attacks do not always come from the most active actors, for example, BlackCat is not among the list of most frequent actors but they were responsible for possibly the most impactful incident to the healthcare sector in 2024. Other notable ransomware incidents reported throughout the year include a major healthcare provider's data being encrypted, local governments facing disruptions due to encrypted public services databases, and a supply chain attack impacting a software company's customers. These events highlight the importance of both implementing robust cybersecurity controls as well as maintaining continuity of operations.

Below are a few major ransomware-related incidents from 2024. These incidents demonstrate the diverse tactics employed by cybercriminals and emphasize the need for strong cybersecurity measures to prevent such attacks.

Change Healthcare

One of the year's most significant attacks occurred against UnitedHealth Group's Change Healthcare on February 21. The healthcare technology company, which provides payment and reimbursement services, suffered a massive data breach, prolonged disruptions, and substantial recovery costs.

In May, UnitedHealth Group CEO Andrew Witty testified during a House Energy and Commerce Subcommittee on Oversight and Investigations hearing. Witty revealed that Change Healthcare was breached through a Citrix portal that did not have MFA enabled.

The attack was carried out by Alphv/BlackCat, a notorious ransomware gang that has targeted several other healthcare organizations in the past. Witty confirmed that Change Healthcare paid the Alphv/BlackCat ransomware group a $22 million ransom to restore operations.

The attack's aftermath continued for months, affecting patient care, insurance submissions, and billing processes. As of January 2025, it was disclosed that the data breach affected 190 million individuals, making it one of the largest U.S. data breaches.

Port of Seattle

On August 24, the Port of Seattle in the State of Washington began experiencing outages related to a ransomware attack. The Port of Seattle is a public agency that also oversees the Seattle-Tacoma International Airport.

While the port's website was down, the airport suffered the brunt of disruptions as bag checking, check-in services, flight information displays, and phone systems went down due to the attack. Some services remained down for two weeks after ransomware encrypted the agency's systems.

In a September 2024 update, the agency said it refused to pay the ransom and, as a result, the threat actors might post stolen data on a public leak site. In an update, the Port of Seattle attributed the attack to the Rhysida ransomware gang, underscoring the severe operational disruptions caused by the incident.

Blue Yonder

On November 22, Arizona-based Blue Yonder, a supply chain management company, disclosed that it had suffered a ransomware attack. The attack disrupted its managed services-hosted environment and caused massive damage to downstream customers, including Starbucks, Sainsbury's, and Morrisons Supermarkets.

Morrisons were forced to rebuild a new warehouse management system for fresh foods and produce, while Sainsbury's suffered service disruptions. The group behind the attack was not identified, but a financially motivated criminal gang is suspected of targeting Blue Yonder's systems for ransom.

Snowflake

Details on the June 2024 attack on Snowflake customers are still under investigation, but reports indicate data theft for extortion. This is consistent with the recent trend of ransomware operators shifting away from encrypting systems and focusing on stealing sensitive data to extort victims. They often threaten to leak the stolen data on the dark web if ransom demands are not met, amplifying the pressure on organizations to comply.

The cloud storage provider was leveraged in cyberattacks that aimed to access customer accounts using stolen login credentials. Among the high-profile clients affected were Ticketmaster and Santander, where attackers gained access to sensitive data and demanded a substantial ransom in exchange, further emphasizing the growing threat posed by third-party security vulnerabilities.

It is important to note that the breach did not involve any direct compromise of Snowflake's infrastructure. Instead, customer credentials were obtained through information-stealing malware. This allowed the attackers to bypass security measures such as multi-factor authentication

VULNERABILITIES AND TECHNIQUES

Overall, attacks observed in 2024 leveraged a wide range of initial access methods, including exploiting system and software vulnerabilities, employing social engineering tactics to deceive individuals into granting unauthorized access, and deploying malware to infiltrate and compromise victim networks. Below, we highlight some of the more significant vulnerabilities being exploited and common techniques used by ransomware attackers.

CVE-2024-40766 - SonicWall

In 2024, the Akira ransomware group executed a significant attack by exploiting a critical vulnerability in SonicWall devices. This vulnerability allowed attackers to gain unauthorized access to the target organization's network. Once inside, they deployed the Akira ransomware, leading to the encryption of critical data and causing substantial operational disruptions.

Organizations can implement several key strategies to prevent such attacks. First, they should consider robust patch management, promptly applying security patches for known vulnerabilities, including CVE-2024-40766. Additionally, maintaining strong network defenses is crucial to detect and block any suspicious activity. Regular security audits are essential for identifying and addressing weaknesses in the organization's cybersecurity posture.

CVE-2024-55956 - Cleo File Transfer Software

We saw file transfer software exploited by the CL0P ransomware gang in attacks. The vulnerability allows threat actors to upload malicious Java files that can execute arbitrary code on affected systems. This follows another Cleo vulnerability (CVE-2024-50623) which was exploited in ransomware attacks earlier in the year. The U.S. State Department is offering a $10 million bounty for information linking the CL0P ransomware gang to any foreign government.

Organizations should adopt a multi-layered cybersecurity approach to mitigate these vulnerabilities. Regularly updating and patching systems is crucial to addressing known vulnerabilities. Educating employees about cybersecurity best practices, including the risks of downloading files from untrusted sources, can help prevent accidental infections. Implementing strong authentication measures, such as multi-factor authentication (MFA), limits unauthorized access to sensitive systems and data. Network segmentation can further enhance security by isolating critical systems and reducing the spread of malware in the event of an attack.

Compromised RDP Credentials

One significant LockBit ransomware attack leveraged compromised RDP credentials to gain initial access to a target organization’s network. In this instance, the attackers exploited weak password practices and used brute force attacks to obtain access to the exposed RDP port. Once inside, they moved laterally through the network, escalating privileges and deploying the ransomware payload. This attack highlights the critical importance of securing RDP access with strong, unique passwords, MFA, and limiting remote access to trusted IP addresses.

Social Engineering

A RansomHub affiliate, known as Scattered Spider, carried out a significant cyberattack by leveraging social engineering techniques to gain initial access. The attackers used Google Voice to impersonate a C-suite executive and contacted the organization's IT help desk, convincing them to reset the executive's password. This manipulation granted the attackers unauthorized access to the network, which they subsequently leveraged to deploy the RansomHub ransomware encryptor.

Organizations can conduct regular training sessions on social engineering and phishing awareness to mitigate attacks like these to educate employees about recognizing and responding to suspicious communications. Companies should also consider implementing strict access controls and ensure that only authorized personnel have administrative privileges. Additionally, IT administrators may want to require MFA for all critical accounts, including those used by IT help desks, to prevent unauthorized password resets. Network segmentation can assist in isolating sensitive systems within the network to limit the spread of malware in case of an attack. Conducting regular security audits and monitoring access logs can help detect any unusual activity and strengthen an organization’s cybersecurity posture.

Remote Access Trojans

Hunters International has utilized tools such as SharpRhino, a sophisticated C# remote access trojan (RAT) designed to penetrate corporate networks by targeting IT professionals. This malicious software is disseminated as a digitally signed installer, which make alterations to the Windows registry to ensure persistence and execute PowerShell commands to deploy ransomware on affected systems, causing significant financial losses and operational disruptions for the targeted organizations.

Organizations can implement a multi-layered cybersecurity strategy to mitigate the risks posed by tools like SharpRhino. Strong network segmentation can limit lateral movement and contain potential breaches within isolated segments. Regularly updating and patching software and operating systems helps fix known vulnerabilities and reduce attack surfaces. Enforcing strong authentication practices, such as using unique passwords and enabling multi-factor authentication (MFA), prevents unauthorized access. Employee security awareness training is crucial in helping staff recognize and report phishing attempts or suspicious emails containing malware. Deploying reputable antivirus and anti-malware solutions configured to update signatures and scan files upon execution automatically adds another layer of defense. Implementing network monitoring tools allows organizations to detect anomalous traffic or indicators of compromise (IoCs) associated with known malware families like SharpRhino.

Additionally, application whitelisting ensures that only approved software can run on endpoints, blocking the execution of unknown or malicious programs. Finally, having a robust incident response plan in place, including clear steps for stakeholder communication, containment measures, and post-incident analysis, strengthens an organization’s ability to respond effectively to a breach. By adopting these measures, organizations can significantly reduce the risk of attacks by leveraging tools like SharpRhino and enhance their overall cybersecurity resilience.

AI–RELATED RANSOMWARE ATTACKS

The integration of AI in the development of ransomware presents a new level of evolution in cyber threats. Attackers are currently using AI to streamline their operations – they are using AI to perform tasks that free up humans to perform other activities – and to create more sophisticated attacks. With AI, ransomware will be able to adapt in real time and be far more effective than it is currently.

One example is an attack from FunkSec, a new ransomware group, seen in December 2024. This group has built its malware on artificial intelligence (AI), using it to avoid detection while launching attacks unprecedented in sophistication in the ransomware landscape. The AI-driven ransomware of FunkSec self-modifies its behavioral patterns and changes its tactics in real-time by analyzing the target's security posture, successfully bypassing all forms of conventional gatekeeping – including antivirus software and firewalls. Many traditional security measures are incapable of detecting and mitigating such attacks. Our tracking shows that FunkSec victimized 54 companies. As AI evolves, ransomware attackers can employ its capabilities to unleash further advanced and targeted attacks that could lead to an increased number of victims and the severity and impact of such attacks as we move on into 2025.

The FunkSec attacks highlight an increasing trend toward utilizing AI by cybercriminals to upgrade the sophistication and impact of ransomware campaigns. Strong cybersecurity practices are needed to defend against AI-powered threats. These include implementing rigorous security controls and ensuring you have access to timely and relevant threat intelligence. Active participation in sector-specific ISACs help companies remain at the cutting edge of emerging threats.

IMPACT ANALYSIS

The consequences of a ransomware attack can be dire, impacting not only an organization's operational capabilities but also its ability to recover from financial losses and reputational damage. Financially, the immediate costs can be overwhelming. We've gathered some great metrics this year, but it can be difficult to identify how many companies pay a ransom, and for how much. Some organizations resolve to make their ransom payments discreetly to preserve their reputations and avoid appearing as easy prey for a follow-up attack. The ransom demand can vary a lot according to a range of conditions, from the size of the firm to the kind of data compromised, right down to the severity of the attack. Ransom payments are usually paid in cryptocurrencies, which can be difficult to trace. Another thing to consider is that not every company agrees to pay the ransom. Sometimes companies are even able to restore data from backups or external recovery options. Because of this, we monitor the frequency of attacks and the initial ransom demand, but it may be difficult to determine the actual financial damage accurately.

According to Verizon's 2024 Data Breach Investigations Report, the median amount of the initial ransom demand represented 1% of the victim organization's total revenue, with 50% of demands falling between 0.13% and 8%. Furthermore, the median adjusted financial loss for those who paid the ransom in 2024—after law enforcement efforts to recover funds—was approximately $46,000, marking a substantial increase from 2023's median of $26,000. In short, depending on the size of the organization, millions of dollars in ransom may be demanded to regain access to encrypted data.

However, even if these demands are met, there is no assurance that the encrypted data will be restored, nor is there any guarantee that attackers won't return for additional payments in the future. Recovery expenses can also mount quickly, as organizations must invest in forensic investigations, system restoration, and efforts to enhance cybersecurity measures to prevent future attacks. Legal fees and regulatory fines may also apply, particularly if sensitive customer data is compromised, triggering compliance breaches with data protection laws such as GDPR or HIPAA.

IMPACT ANALYSIS CONT'D

In the event of a ransomware attack, an organization's operational capabilities can be significantly hindered. With actors locking systems and encrypting data, this can prevent employees from accessing critical resources, halting day-to-day operations and leading to significant productivity losses. Depending on the scale of the attack, essential services may be delayed or stopped entirely, resulting in service interruptions that can affect customers and partners. Recovery efforts can take weeks or even months, during which time the business may struggle to operate at full capacity, leading to long-term operational setbacks and economic losses.

Another burden that organizations may face due to a ransomware attack is reputational damage. As these attacks often expose vulnerabilities in an organization's cybersecurity measures, customers, partners, and stakeholders may lose trust in the organization's ability to protect sensitive information. This can lead to a loss of business and damage to brand reputation. In some cases, the negative media coverage surrounding an attack can have a lasting impact on the organization's public image, making it difficult to regain support from consumers, stakeholders, and partners.

Additionally, ransomware attacks can extend beyond a single organization to disrupt the wider supply chain, shining a light on the interconnectedness of our critical infrastructures. Attackers often target weaknesses and vulnerabilities in third-party vendors or partners, creating a domino effect of breaches. A compromised supplier or business partner can inadvertently infect an organization with ransomware, causing further operational disruptions and financial losses. If you recall back in 2021, the VSA software used by Kaseya was attacked by the REvil ransomware group, which exploited a vulnerability to deploy ransomware on systems managed by MSPs. The vulnerability was leveraged by the attackers to deploy ransomware not only on the systems of Kaseya but also on the systems of its clients, thereby hitting more than 1,500 companies worldwide. The result showed how fast an attack on a single supplier can cascade through an interconnected network of organizations, resulting in significant operational disruption and financial losses. In industries that rely heavily on interdependent supply chains, such as manufacturing or healthcare, the cascading effects of these attacks can be particularly devastating, impacting multiple entities simultaneously and further complicating recovery efforts.

Overall, ransomware attacks' financial, operational, reputational, and supply chain impacts can severely hinder an organization's ability to recover and thrive in the long term. These attacks can leave lasting scars, requiring substantial investments of time and resources to restore both business operations and public trust.

DEFENSE & MITIGATION INSIGHTS

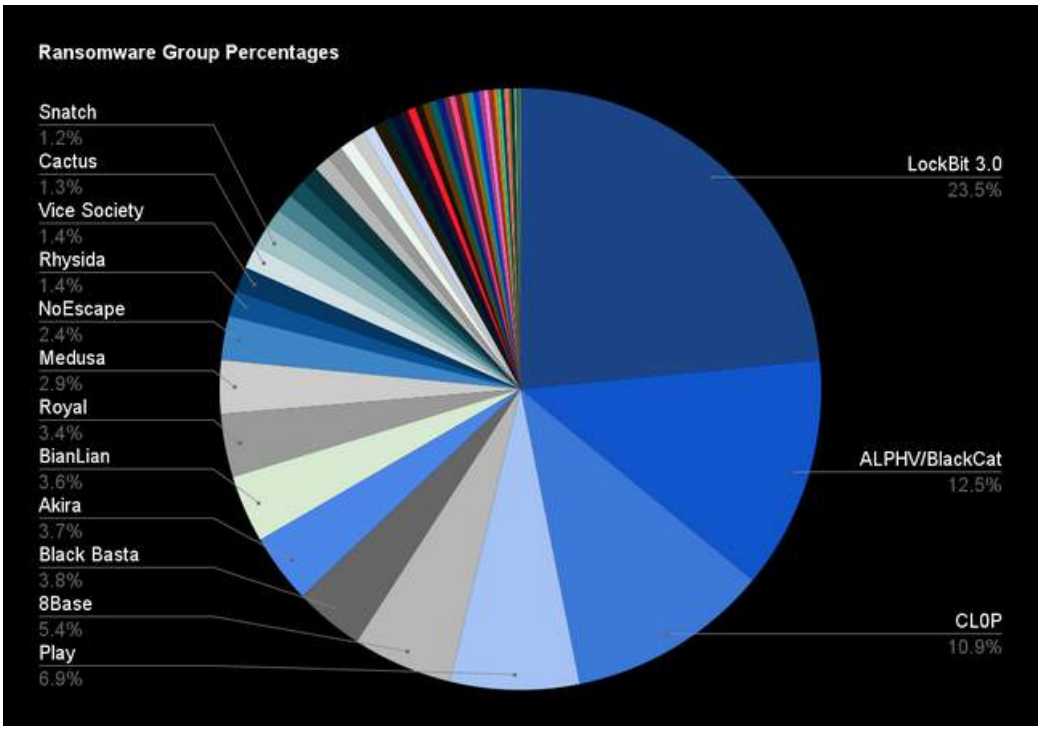
While no single or combination of actions can guarantee that your company will not become a victim of ransomware, based on our research, there are steps companies can take to reduce their risk and to improve their ability to recover should they become a victim.

- **Backup your data, system images, and configurations, regularly test them, and keep the backups offline:** Ensure that backups are regularly tested and that they are not connected to the business network, as many ransomware variants seek to find and encrypt or delete accessible backups. Maintaining current backups offline is critical because if your network data is encrypted with ransomware, your organization can restore systems.
- **Update and patch systems promptly:** Perform regular maintenance on the security of your systems, including timely maintenance of operating systems, applications, and firmware. Consider using a centralized patch management system and a risk-based assessment strategy to drive your patch management program.
- **Test your incident response plan:** Nothing shows gaps in plans more than testing them. Encourage teams to review some core questions and use those to build an incident response plan. Examples of core questions include: Are you able to sustain business operations without access to certain systems? If so, for how long? Would you turn off your manufacturing operations if business systems such as billing were offline?
- **Check your security team's work:** Use a third-party pen tester to test the security of your systems and your ability to defend against a sophisticated attack. Many ransomware criminals are aggressive and sophisticated and will work tirelessly to find "unlocked doors".
- **Segment your networks:** Ransomware attacks have recently shifted from stealing data to disrupting operations. It's imperative that your corporate business functions and manufacturing/production operations are separated. You should also carefully filter and limit internet access to operational networks, identify links between these networks, and develop workarounds or manual controls to ensure that ICS networks can be isolated and continue operating if your corporate network is compromised. We recommend regularly testing contingency plans, such as manual controls, to maintain safety-critical functions during a cyber incident.
- **Train employees:** Email remains the most vulnerable attack vector for organizations. Train users how to avoid and spot phishing emails. Implementing MFA can also help prevent malicious access to sensitive services.
- **Drive improved security of third-party partners:** Suppliers, partners, and other supply chain entities who are impacted by ransomware can impact critical services and disrupt production. In some cases, ransomware actors may even target an organization's less mature supply chain partners to exploit the larger entity. Members of your organization's supply chain may not have dedicated staff or resources to implement security best practices. Put identity and access management in place and leverage network segmentation to prevent third-party provisioned accounts from allowing a threat actor into your environment. The Food and Ag-ISAC has prepared a Cybersecurity Best Practice Guide for Small and Medium Sized Businesses. This guide offers several low-cost, easy-to-implement security tips to help secure your less mature supply chain partners.
- **Implement multi-factor authentication:** External-facing assets that leverage single-factor authentication (SFA) are highly susceptible to brute-forcing attacks, password spraying, or unauthorized remote access using valid (stolen) credentials. Therefore, external-facing applications and services that currently allow SFA should be configured to support multi-factor authentication (MFA).

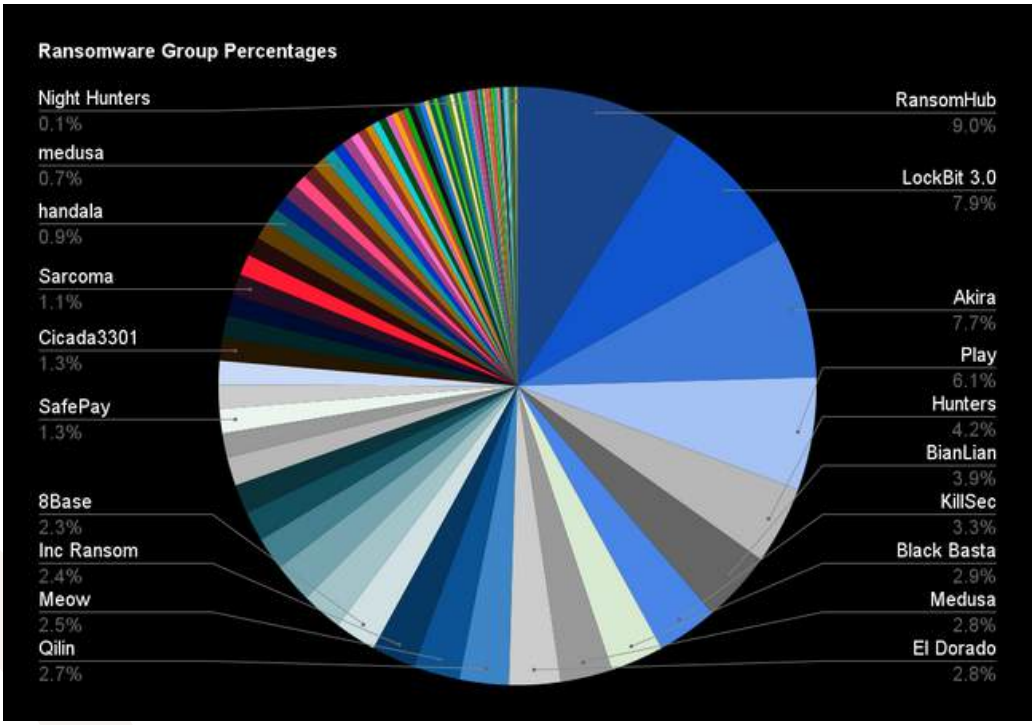
2023 vs. 2024 Ransomware Group Percentages

The variation in ransomware groups' percentages between 2023 and 2024 testifies to progress in cybersecurity, law enforcement efforts, and enhanced organizational defenses. Disruptions to major groups, along with stronger security measures and global cooperation, have reduced some threats while enhancing resilience. As awareness and innovation grow, so does the security of the digital landscape.

2023



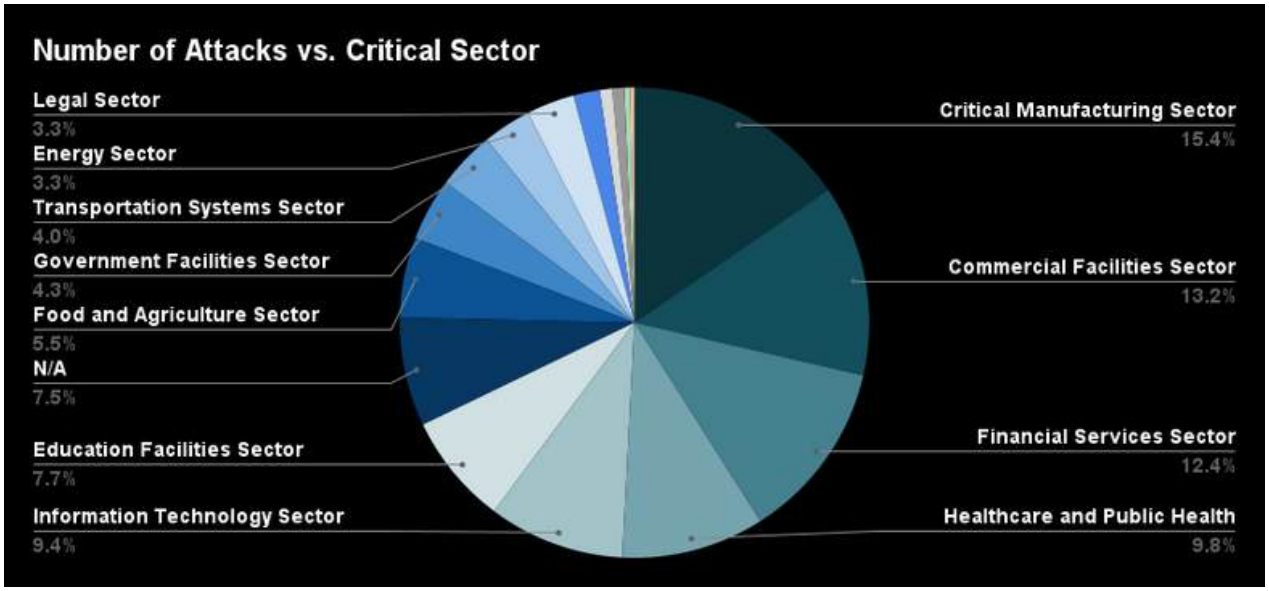
2024



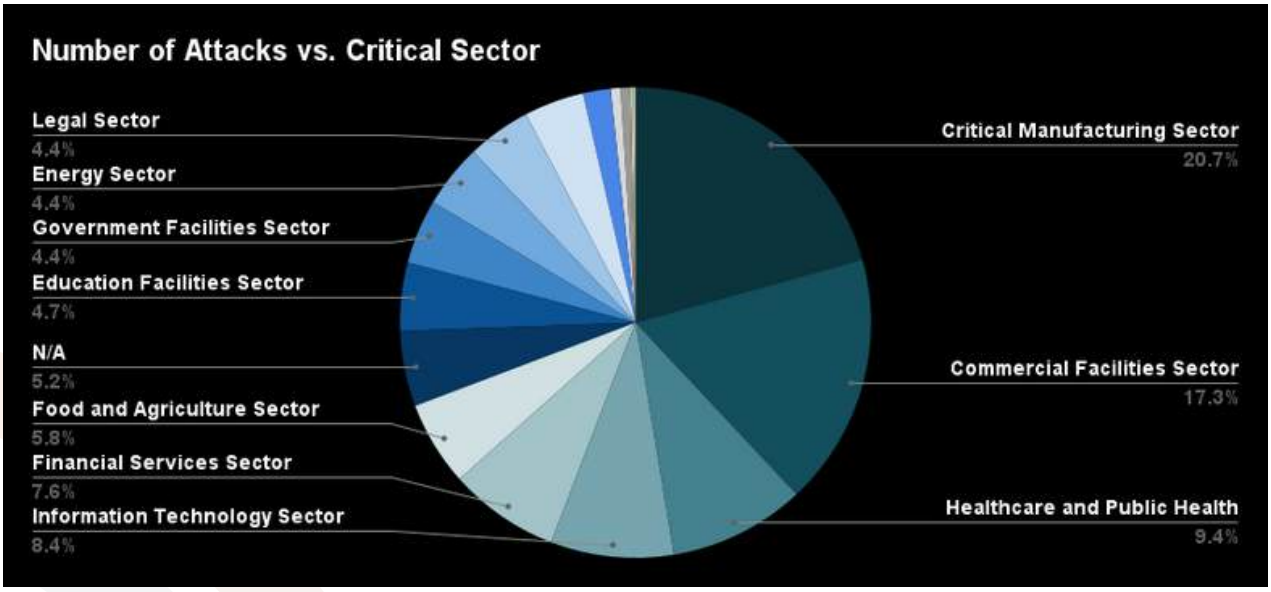
2023 vs. 2024 Ransomware Attacks Per Critical Sector

Ransomware attack comparisons across critical sectors in 2023 and 2024 show some changes. Critical Manufacturing and Commercial Facilities have grown from 15.4% to 20.7% and from 13.2% to 17.3%, respectively.

2023



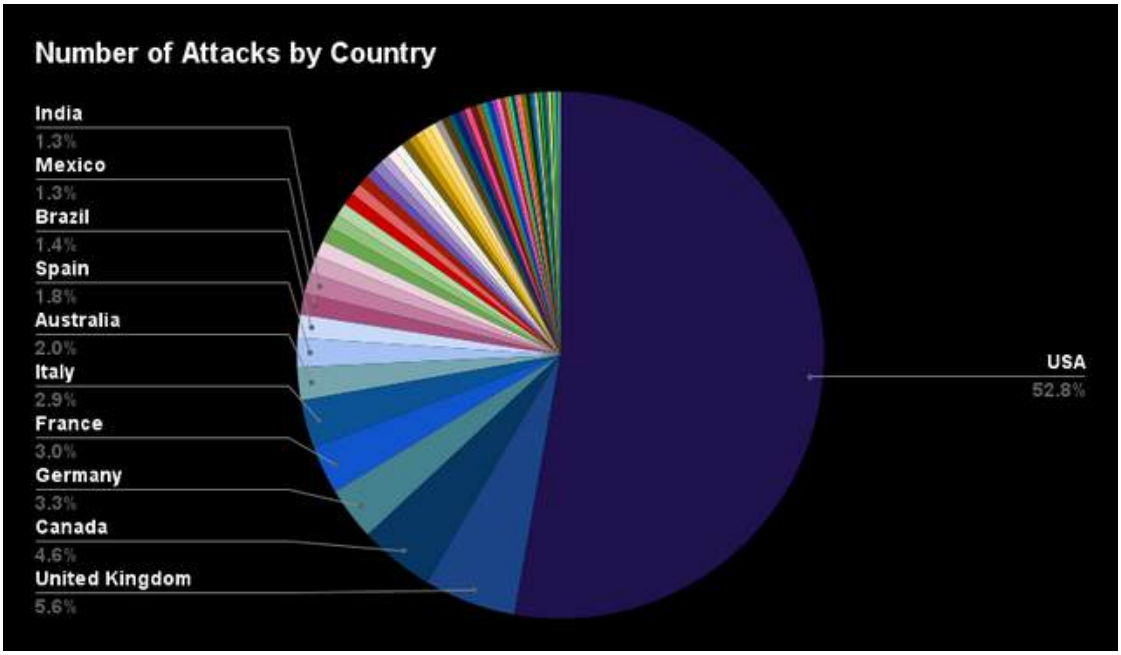
2024



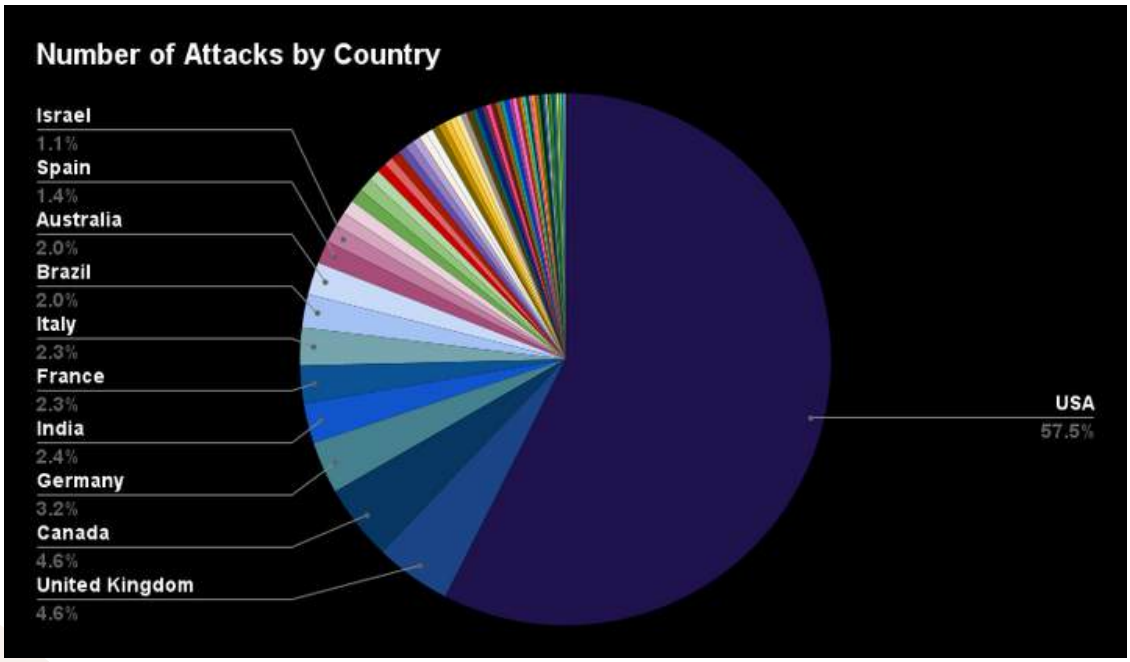
2023 vs. 2024 Ransomware Attacks By Country

The USA remains the most impacted, with the number of attacks increasing from 52.8% in 2023 to 57.5% in 2024. This could be attributed to its advanced economy and critical infrastructure.

2023



2024



2025 Predictions

Ransomware continues to evolve at an alarming rate. Based on current data and the new TTPs initiated by emerging threat actors, the IT-ISAC expects several key developments in the ransomware arena for 2025.

1. **Continued Rise in Critical Sector Targeting**
   The end of 2024 saw a dramatic rise in the number of ransomware attacks. This trend continues into 2025. We expect attacks to increase across critical infrastructure. As long as there is a high likelihood of the bad actors making money and a low likelihood of them getting caught, the attacks will certainly continue.

2. **Increased Use of Zero-Day Exploits**
   Ransomware groups in the limelight such as RansomHub and LockBit are already known to exploit zero-day vulnerabilities. We forecast that throughout 2025, these methods will be adopted more widely by threat actors, with groups that could be sponsored by states, like CL0P, extending their capabilities. Zero-day vulnerabilities, especially in public-facing applications, will be key targets, and organizations should invest in advanced threat detection and patch management systems to defend against such attacks.

3. **Continued Movement to Double Extortion and Data Theft**
   Double extortion involves infecting the target with ransomware, exfiltrating sensitive information, and then threatening to sell the information unless a ransom is paid. This trend is most likely to stick around in 2025.

   Groups like RansomHub and Akira pioneered the technique, which has not only evolved but is expected to continue spreading. Double extortion is particularly effective against industries handling sensitive data, such as Healthcare and Financial Services, where organizations face relentless pressure to maintain confidentiality and comply with HIPAA and GDPR regulations. Attackers exploit this urgency by encrypting data and threatening to leak it publicly, increasing the likelihood that victims will pay the ransom.

4. **AI-Powered Ransomware Evolution**
   A significant trend to watch for in 2025 is the rise of AI-powered ransomware. Start-ups like FunkSec have begun integrating AI into their malware, allowing real-time changes to their operational code to slip through traditional defenses. As a result, the sophistication of ransomware campaigns may improve to the point where traditional security measures may not be enough. In this shift, we expect the security industry to likewise adapt by incorporating AI into its defensive products.

5. **Increasing Geographic Spread**
   We anticipate that the geographic distribution of ransomware attacks will expand in 2025 as cybercriminal groups diversify their operations. Countries with expanding digital infrastructures could face an increase in threats as they adopt new technologies. Moreover, emerging markets with rapidly growing internet access and digital services could become new hotspots for ransomware actors in the coming year.

6. **Continued Ransomware-as-a-Service (RaaS) Model Growth**
   We expect that In 2025, the RaaS model will grow and become more active. Groups like LockBit and RansomHub have successfully utilized this business model, allowing affiliates to conduct attacks while providing them with infrastructure and tools. As more affiliates join these networks, we expect an increase in the volume of attacks, particularly targeting organizations with less robust security measures, such as small and medium-sized businesses (SMBs).

2025 Predictions Cont'd

7 **Enhanced Data Exfiltration Techniques**
We expect cybercriminal groups to refine their data exfiltration tactics during 2025. Groups like Akira and Hunters International have already begun using advanced methods for stealing sensitive information, utilizing tools such as RClone and FileZilla to encrypt and exfiltrate data. As the process of exfiltrating data becomes a key component of ransomware attacks, organizations must prioritize implementing robust data protection measures, including encryption-at-rest and in-transit, along with heightened monitoring to detect any unusual file transfers.

8 **Supply Chain Attacks Become More Common**
We foresee a rise in supply chain attacks following the discovery of vulnerabilities in critical sectors such as technology, healthcare, and manufacturing. As a result, we are likely to see these vulnerabilities exploited in supply chain attacks in 2025. We expect attackers to impact suppliers and service providers to try to gain entry into larger organizations. This may cause businesses to scale up third-party risk management processes and apply zero-trust models to ensure that their supply chain partners remain steadfast in their cybersecurity discipline.

Founded in 2000, the Information Technology - Information Sharing and Analysis Center (IT-ISAC) is a non-profit organization that augments member companies' internal capabilities by providing them access to curated cyber threat analysis, an intelligence management platform, and a trusted forum to engage with senior analysts from peer companies.

We serve as a force-multiplier that enables collaboration and sharing of relevant, actionable cyber threat information, effective security policies, and practices for the benefit of all.

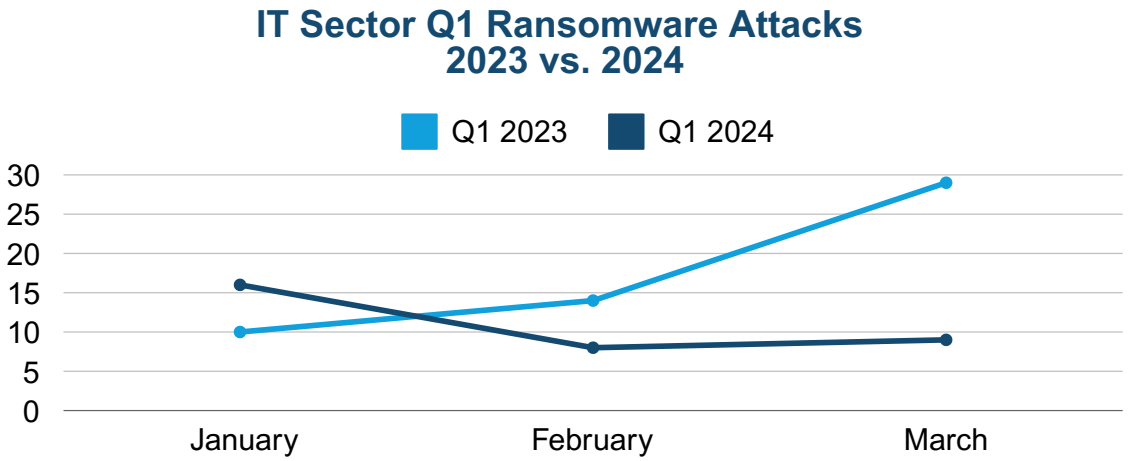
2024 Quarterly Analysis

Q1 2024 Analysis
January - March

The first quarter of 2024 has shown some changes in the ransomware landscape. Ransomware attacks started strong in January (up 54% from January 2023). However, this increase was short-lived, with attacks decreasing by 42% in February 2024 compared with February 2023, and decreased 55% in March 2024 compared with March 2023. This decrease is likely due to law enforcement efforts to take down ransomware infrastructure.

In the first quarter of 2024, the top three ransomware groups that targeted the Information Technology (IT) sector were LockBit (33%), Akira (28.6%), and BlackCat (19%). This lineup is very similar to 2023, with the only minor difference of Akira replacing CL0P for second place.

One notable trend in 2024 is a decrease in activity from CL0P. This group had major success last year after identifying a zero-day vulnerability in the MOVEit file transfer software. With hundreds of organizations across the globe relying on the software, the ransomware gang was able to swiftly compromise dozens of vulnerable appliances and net millions of dollars in ransom. As organizations started to secure their appliances, the number of successful compromises decreased over time. What was believed to be a successful run eventually came to an end, with CL0P activity significantly decreasing since then. In Q1 of 2024, only 6 CL0P attacks have been observed compared to the 53 in 2023.

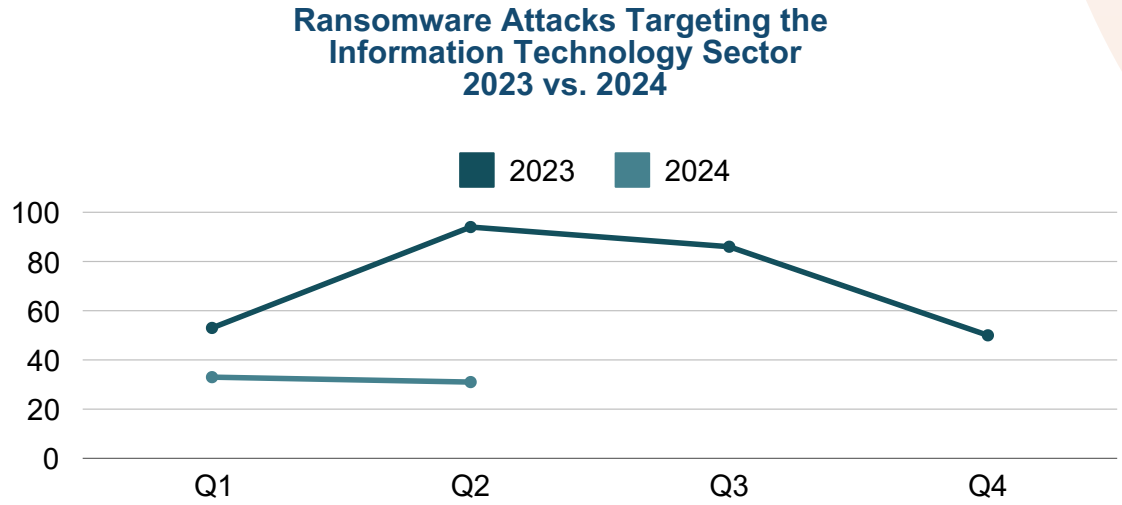


Another noteworthy event was law enforcement's takedown of BlackCat's infrastructure in December 2023, and LockBit's in February 2024. These groups typically occupied the top positions in monthly ransomware attack rankings. However, since the takedowns, operational functionality has declined for both groups, with Play ransomware now replacing LockBit as the most active ransomware group and BlackCat operations completely ceasing in March 2024. It remains to be seen whether BlackCat will resume operations, nonetheless, this at least temporary hiatus in activity puts the spotlight on the emergence of other ransomware entities that have been steadily gaining traction. Noteworthy among these groups are Play, Akira, 8Base, and Black Basta, whose activities are increasingly garnering attention within the ransomware landscape.

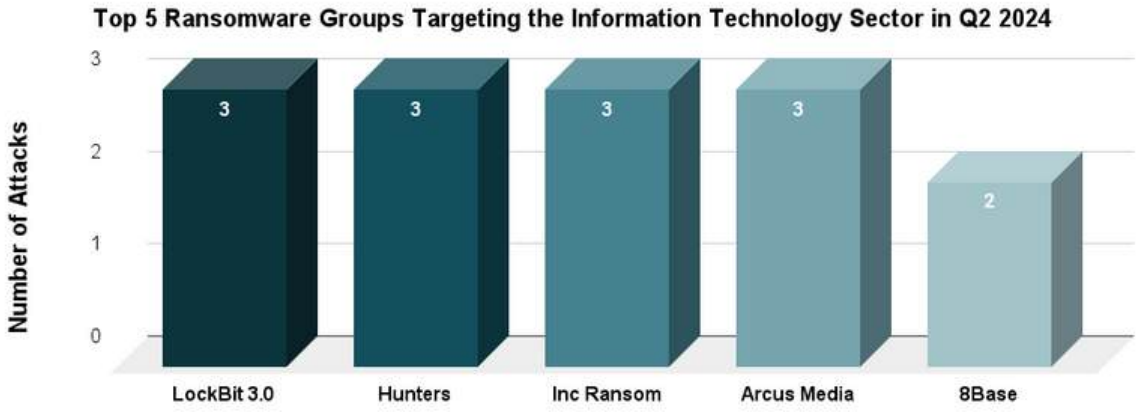
While the IT sector continues to be a prime target of ransomware attacks, the Healthcare and Public Health sector saw a 36% increase in ransomware attacks in Q1 of 2024 compared to the previous year. This trend aligns closely with an announcement made by a BlackCat administrator in December 2023, wherein affiliates were encouraged to direct their efforts toward targeting hospitals. Although the precise motivations behind the administrator's direction remain unclear, this underscores a concerning reality that healthcare providers have become increasingly attractive targets for cybercriminals.

Q2 2024 Analysis
April - June

In the second quarter of 2024, the Information Technology - Information Sharing and Analysis Center (IT-ISAC) observed a 21% decrease in ransomware attacks compared to the first quarter. The top three targeted sectors throughout this year's Q2 were critical manufacturing, commercial facilities, and healthcare, which together accounted for 47.6% of all attacks.



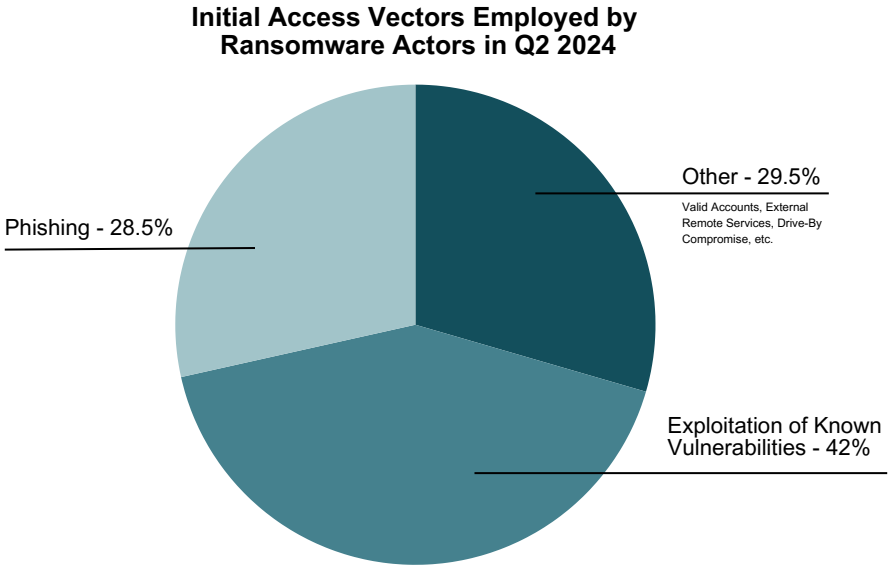
While the information technology sector was targeted less frequently, it still accounted for 6.9% of all attacks – with groups like LockBit, Hunters, Inc Ransom, and Arcus Media being the top 5 most active ransomware groups in this sector.



Law enforcement initiatives to take down infrastructure belonging to BlackCat/ALPHV in December 2023 and to LockBit in February 2024 have taken a toll on the ransomware landscape. BlackCat/ALPHV, which previously ranked high in monthly ransomware attack rankings, is no longer operational – contributing to the overall decline in ransomware attacks. Although LockBit remains active, it is no longer as prolific as it once was. Following the takedown of LockBit's infrastructure earlier this year, researchers at Trend Micro observed that LockBit had been relisting old victims on its data leak site and populating the site with fake victim data to maintain an appearance of normalcy and suggesting total operational capacity. Recent listings on LockBit's data leak site indicate that the group still employs this tactic.

Q2 2024 Analysis Cont'd

Ransomware actors continue to exploit existing vulnerabilities, highlighting the importance of timely patching and vulnerability management. Based on ransomware attacks reported by the IT-ISAC in Q2 of 2024, the exploitation of known vulnerabilities accounted as an initial access vector for 42% of all incidents, followed by phishing at 28.5%.



Below is a list of some of the vulnerabilities exploited by ransomware actors in Q2:

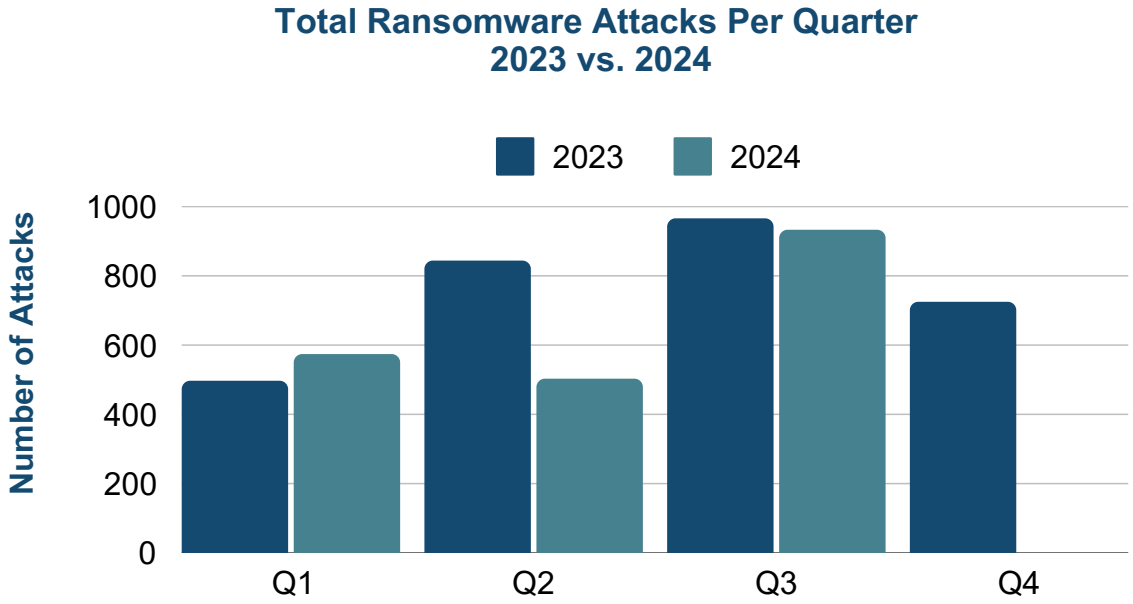
- **CVE-2020-1472: Netlogon Elevation of Privilege Vulnerability**
  - Successful exploitation of this flaw can allow an attacker to gain domain administrator privileges and take control of the entire domain. With control over the domain, an actor can create, delete, or modify accounts, access sensitive data, and even install malware, disrupting operations. Symantec observed CVE-2020-1472 being exploited by RansomHub for initial access.
- **CVE-2023-22518: Improper Authorization Vulnerability In Confluence Data Center and Server**
  - Successful exploitation allows an unauthenticated attacker to reset the Confluence application and create a new Confluence administrator account. Cado Security Labs investigated several reports of Cerber ransomware being deployed onto servers running the Confluence application via the CVE-2023-22518 exploit.
- **CVE-2024-26169: Windows Error Reporting Service Elevation of Privilege Vulnerability**
  - Successful exploitation lets local attackers gain SYSTEM permissions. Symantec investigated an attack in which an exploit tool for CVE-2024-26169 was deployed. While the actors were not successful in deploying the ransomware payload, researchers attributed the attack to the Black Basta ransomware gang based on the TTPs employed (use of batch scripts masquerading as software updates).
- **CVE-2024-4577: Remote Code Execution (RCE) Flaw in PHP's CGI Mode**
  - An attacker can exploit this flaw by sending a specially-crafted request to a vulnerable PHP application, allowing them to execute arbitrary code with the same privileges as the web server. Imperva Threat Research reported on attacker activity leveraging this PHP vulnerability to deliver TellYouThePass ransomware.

Exploiting these flaws can allow actors to gain access to sensitive information, execute code remotely, install malicious payloads, and escalate privileges to take complete control over targeted systems. Organizations should prioritize patching these vulnerabilities and implementing robust security measures to mitigate the risks associated with them.

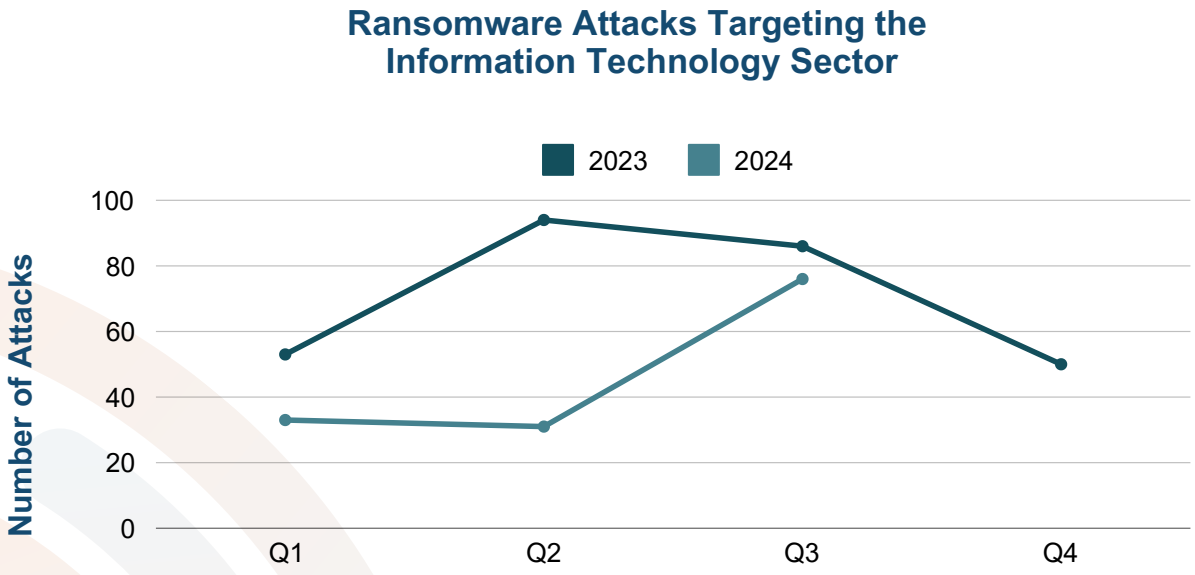
Q3 2024 Analysis

July - September

In the third quarter of 2024, the Information Technology - Information Sharing and Analysis Center (IT-ISAC) recorded a total of 933 ransomware attacks, highlighting an 85% increase over the previous quarter (503 attacks). This significant increase seen between Q2 and Q3 2024 is a result of the IT-ISAC's recently improved methodology in tracking ransomware attacks. Relying on APIs and RSS feeds to automate the collection of cyber incidents attributed to ransomware; these events are vetted for duplicates and manually added to the ransomware tracker and closely align with vendor reports.

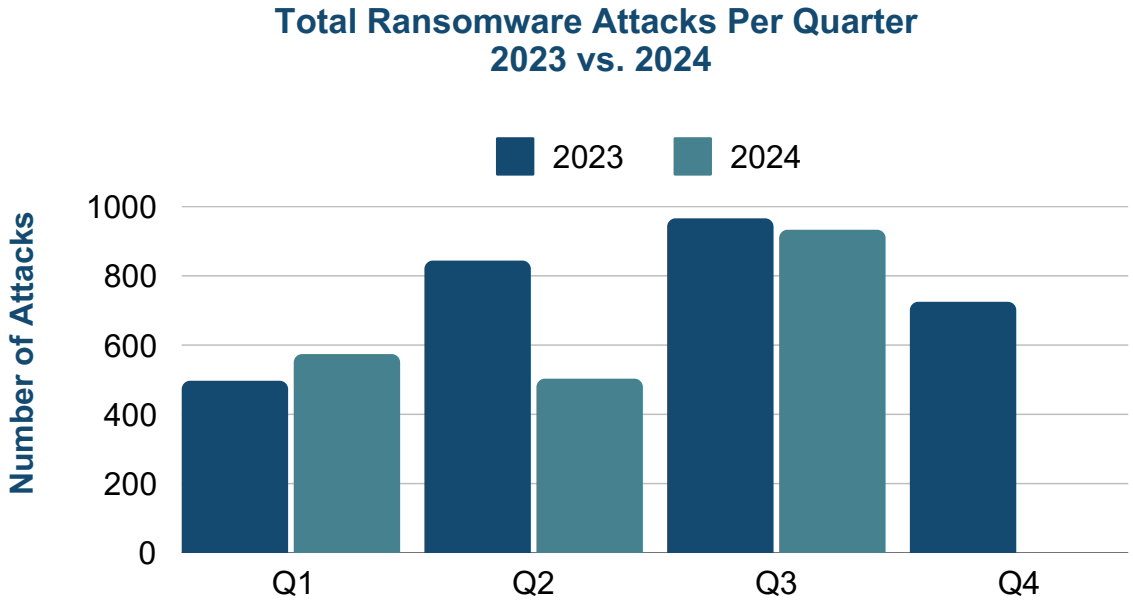


The top three sectors targeted by ransomware (critical manufacturing, commercial facilities, and healthcare) remain unchanged from Q2 2024. However, ransomware attacks aimed at the information technology sector more than doubled in Q3 compared to the previous quarter.

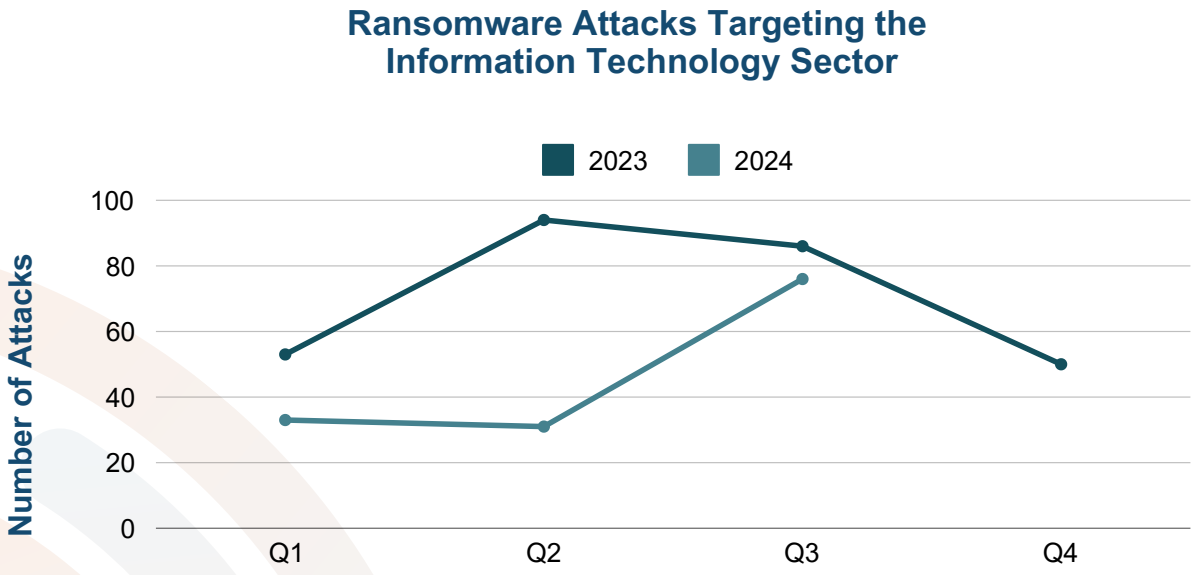


Q3 2024 Analysis
July - September

In the third quarter of 2024, the Information Technology - Information Sharing and Analysis Center (IT-ISAC) recorded a total of 933 ransomware attacks, highlighting an 85% increase over the previous quarter (503 attacks). This significant increase seen between Q2 and Q3 2024 is a result of the IT-ISAC's recently improved methodology in tracking ransomware attacks. Relying on APIs and RSS feeds to automate the collection of cyber incidents attributed to ransomware; these events are vetted for duplicates and manually added to the ransomware tracker and closely align with vendor reports.

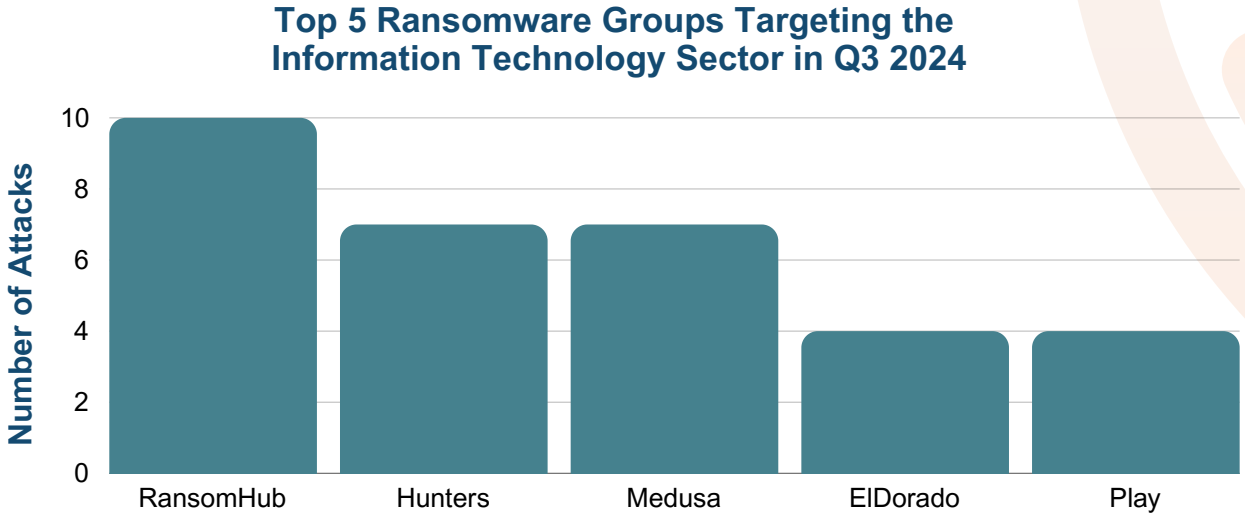


The top three sectors targeted by ransomware (critical manufacturing, commercial facilities, and healthcare) remain unchanged from Q2 2024. However, ransomware attacks aimed at the information technology sector more than doubled in Q3 compared to the previous quarter.



Q3 2024 Analysis Cont'd

The top 3 threat actors that targeted this sector were RansomHub, Hunters, and Medusa ransomware.



RansomHub

A Prominent and Growing Threat Within the Ransomware Landscape

Although RansomHub just initiated operations earlier this year, the group has taken the limelight in recent months, replacing LockBit as the most active ransomware gang. In Q3 2024, the IT-ISAC attributed 110 attacks to RansomHub, accounting for 11.8% of all ransomware attacks recorded, followed by LockBit (8%), Meow (6.6%), and Hunters ransomware (5.4%). A key reason for RansomHub's success can be attributed to affiliates of notorious groups like LockBit and ALPHV/BlackCat joining its rankings.

Following targeted law enforcement operations that disrupted both BlackCat and LockBit's infrastructure within the past year, groups like RansomHub have capitalized on this opportunity to recruit these affiliates into their own ransomware-as-a-service (RaaS) operation. RaaS operations are known for hiring affiliates to gain initial access to victim environments and deploy the encryptor on their behalf. In return, affiliates get a pay cut of the ransom paid by victims. RansomHub, in particular, has incentivized affiliates to join its program by promising to offer affiliates a 90% pay cut of the ransom, a margin that is typically higher than what other RaaS operations provide.

A notable affiliate of RansomHub is Scattered Spider, a notorious cybercrime group known for its advanced social engineering skills. The group has been active since 2022 and was a former affiliate of BlackCat. Members of the Scattered Spider syndicate are proficient in the English language, allowing them to effectively engage with and social engineer victims residing in western regions. Scattered Spider has previously engaged in SIM swapping and MFA fatigue attacks to effectively bypass multi-factor authentication and compromise user accounts. As of recently, the group has focused its efforts on extorting large organizations by partnering with ransomware groups like RansomHub. With the aid of Scattered Spider, RansomHub in turn has managed to quickly scale its operations and compromise dozens of organizations within a very short period of time.

Q3 2024 Analysis Cont'd

Ransomware Tooling

New Ransomware Tool Matrix

A recent report by Symantec highlights the most frequently employed tools in ransomware attacks in 2024. Windows native binaries such as PsExec, Netscan, and PowerShell were the top three tools abused by ransomware adversaries between January and September 2024. PsExec is a tool that can be used to execute a program on another computer and has been typically used by ransomware actors to move laterally across systems. On the other hand, Netscan is used to discover and retrieve information about network devices. In contrast, PowerShell is a scripting tool that is used to run commands, download payloads, and move laterally across systems. Overall, utilities that are native to the Windows environment allow ransomware actors to evade detection since the operating system already trusts these tools. Since many systems come pre-installed with these utilities, actors can exploit them without the need to download and execute additional files.

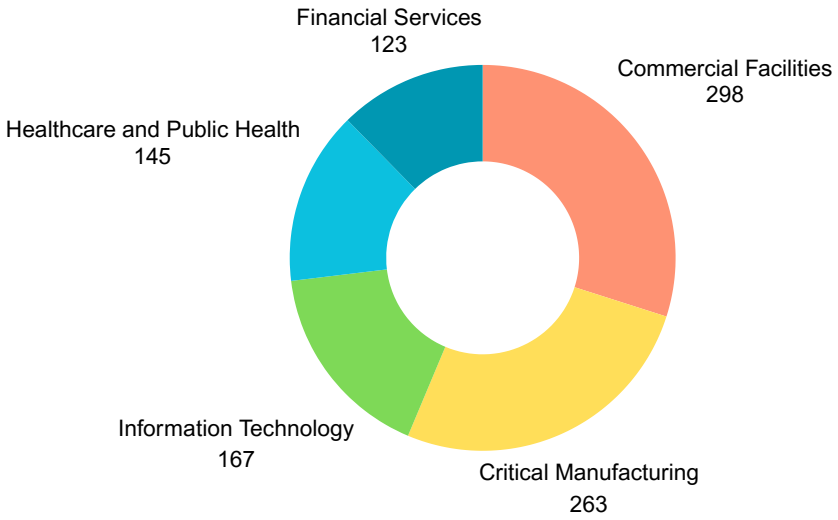
In addition to tools like PsExec, NetScan, and PowerShell, ransomware actors have increasingly exploited remote monitoring and management (RMM) software in their attacks. While these tools are typically employed by IT professionals for remote administration and technical support, ransomware actors have leveraged them to gain unauthorized access to victim environments. Based on a new Ransomware Tool Matrix developed by security researcher Will Thomas (aka BushidoToken), Anydesk, Splashtop, Atera, ScreenConnect, and TeamViewer rank as the top five RMM tools abused by ransomware actors. Given the widespread use and familiarity of these applications within organizations, their exploitation allows ransomware actors to reduce the likelihood of detection significantly.

The new open-source Ransomware Tool Matrix, available on GitHub, provides a comprehensive overview of tools commonly used by ransomware actors at each stage of the cyber kill chain. This matrix is regularly updated and references various advisories from government agencies such as the FBI and CISA, as well as from security vendors, specifically highlighting tools identified as being exploited by these ransomware actors. Organizations seeking to bolster their defenses against potential ransomware attacks can utilize this matrix as a foundational resource. For example, if a particular tool is listed as being exploited by ransomware and is currently present on company systems, it is crucial to monitor the activities associated with that tool continuously. Additionally, if the software is installed but not actively in use, it is recommended that it be uninstalled to reduce potential exploitation and impact.

Q4 2024 Analysis

October - December

Last year concluded with a notable surge in ransomware activity. In Q4 of 2024, the IT-ISAC recorded a total of 1,514 ransomware attacks, making 8,343 total tracked ransomware attacks for the 2024 year. The uptick in Q4 showed a 62% increase compared to Q3, which saw 933 attacks. The top five sectors targeted during this period outlined below.



Leading the forefront were ransomware groups such as RansomHub, Akira, KillSec, CL0P, and Play, which together were responsible for 35% of all attacks observed in Q4.

The increase in attacks during Q4 can be attributed to several factors. With holidays like Christmas and Thanksgiving falling towards the end of the year, many employees request time off. This creates the perfect storm for ransomware actors, who often exploit the reduced presence of IT personnel during the holidays. With fewer IT staff available to detect, mitigate, and respond to incidents, the window of opportunity for attackers to gain access to networks and deploy malicious payloads increases. Furthermore, many organizations, anticipating a slower period or downtime during the holidays, may inadvertently relax their security posture, leaving critical systems vulnerable to exploitation. Ransomware groups are well aware of this shift in the business environment and strategically tailor their attacks to exploit periods of reduced vigilance. They understand that the likelihood of successfully infiltrating an organization increases when defenses are weakened and response times are slower.

Groups like Akira and CL0P ransomware played a pivotal role in Q4, launching widespread attacks and compromising a significant number of victims. A common aspect among these two groups is their ability to identify and exploit critical vulnerabilities in widely used products across organizations globally. In August 2024, SonicWall addressed a critical improper access control flaw (CVE-2024-40766) in its SonicOS management access and SSLVPN, which could allow unauthorized access to resources and, under certain conditions, cause the firewall to crash. Although patches were released, thousands of SonicWall appliances remained unpatched, enabling Akira to exploit this opportunity to gain initial access to victim environments and deploy its encryptor.

Q4 2024 Analysis Cont'd

In December 2024, the CL0P ransomware group exploited a zero-day vulnerability, tagged as CVE-2024-55956, in Cleo's managed file transfer products—Harmony, VLTrader, and LexiCom. This vulnerability allowed unauthenticated attackers to import and execute arbitrary Bash or PowerShell commands on host systems due to the default settings of the Autorun directory, ultimately leading to remote code execution (RCE). CL0P used CVE-2024-55956 to exfiltrate data from numerous organizations. The group has listed 66 victims from this campaign. However, CL0P notes that this list represents only those victims who were contacted but did not respond to the ransom demand, suggesting that the actual number of affected companies could be significantly higher.

In past campaigns, CL0P has had a notable track record of exploiting zero-day vulnerabilities in file management solutions, repeatedly targeting critical systems to gain unauthorized access. Between late 2020 and 2021, the group leveraged multiple zero-day exploits—CVE-2021-27101, CVE-2021-27102, CVE-2021-27103, and CVE-2021-27104—in the Accellion file transfer application, targeting approximately 100 organizations to extort sensitive data. In 2023, CL0P continued its trend of discovering vulnerable systems, executing unauthorized commands, and compromising sensitive data. The group exploited a command injection flaw (CVE-2023-0669) in the GoAnywhere Managed File Transfer platform, which allowed them to compromise around 130 organizations. Also, in 2023, CL0P launched one of its most successful campaigns ever, exploiting a zero-day vulnerability (CVE-2023-34362) impacting the MOVEit File Transfer platform. As a result, CL0P was able to breach and exfiltrate data from over 2,000 organizations. While CL0P may not be as active as other ransomware groups every month, its consistent ability to identify and exploit zero-day vulnerabilities underscores its persistence and its ongoing threat to organizations worldwide.

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.

IT ISAC

CELEBRATING 25 YEARS OF THREAT INTELLIGENCE SHARING

MEMBERSHIP@IT-ISAC.ORG
IT-ISAC.ORG