IT ISAC

FOUNDED 2000

Exploring the Depths:

An Analysis of the 2023 Ransomware Landscape and Insights for 2024

Includes Q2 2024 Analysis!

UPDATED JULY 2024

The Information Technology – Information Sharing and Analysis Center (IT-ISAC) has been closely watching ransomware incidents and trends, and has maintained a Ransomware Tracker since 2021. Our information is gathered via open-source sites, the dark web, member input, and information shared between National Council of ISAC members. In 2023, the IT-ISAC recorded a total of 2,905 ransomware attacks globally, with ransomware groups like LockBit, ALPHV/BlackCat, and CL0P taking the lead in terms of the number of victims compromised.

Despite government and law enforcement efforts to take down malicious infrastructure, new ransomware strains continue to emerge. The IT-ISAC tracked 18 new ransomware groups in 2023, reflecting that financial gain continues to be one of the top motivating factors behind cyberattacks. As long as the chances of making money is high and the risk of getting caught is low, ransomware will continue.

Here are some of the key trends and takeaways for 2023 that the IT-ISAC observed:

- Ransomware-as-a-Service (RaaS) operations have significantly reduced the barriers to entry for individuals or groups looking to carry out ransomware attacks. By accessing the dark web, attackers can easily obtain ransomware software packages. Once they gain initial access to a victim's network, they can deploy this software to encrypt files and demand ransom payments.
- Downloading ransomware packages has indeed become relatively straightforward for anyone interested in launching such attacks. However, the methods used by threat actors to gain initial access for deploying ransomware have become more sophisticated. They are increasingly leveraging zero-day vulnerabilities and employing custom tooling, making it challenging for organizations to defend against attacks using readily made ransomware packages.
- There is an increase in data extortion schemes with ransomware groups skipping the encryption process altogether.
- Actors are switching to programming languages like Rust to develop their encryptors, increasing the scope for potential victims beyond Windows users.
- Ransomware actors continue to target third-party vendors to gain access to mission-critical systems and data.
- There is a notable trend in Ransomware actors abusing remote management tools and legitimate software to gain initial access and evade detection.

RaaS Operations:

An Upward Trend in 2023 and Anticipated Growth into 2024

Ransomware-as-a-Service (RaaS) is a cybercriminal business model where threat actors rent or purchase ransomware software and services from developers, allowing them to carry out attacks without the need for having sophisticated technical skills of their own. In 2023, Trend Micro research revealed a notable uptick in RaaS activity. The newfound accessibility to cybercrime has led to an 11.3% increase in the number of RaaS and RaaS-related groups. Furthermore, Trend Micro's findings indicate a significant surge in victim organizations during the first half of 2023, reaching a total of 2,001—a staggering 45.3% increase compared to the latter half of 2022.

This model has significantly contributed to the proliferation of ransomware attacks in recent years. RaaS operations lower the entry barrier for individuals or groups seeking to engage in cyber ransomware attacks. With the availability of RaaS, developers rent the ransomware code and infrastructure, and sometimes even provide support. Operators, often referred to as affiliates, then execute the attacks. Throughout 2023, there has been a significant increase in ransomware attacks facilitated by the acquisition of malicious software using this model. The surge in attacks can be attributed to several factors, including:

- **Accessibility:** Increased accessibility makes it easier for a wider range of cybercriminals, including those with limited technical expertise, to participate in ransomware activities.
- **Flexibility and Scalability:** These services empower malicious actors to tailor their attacks to specific targets and industries.
- **Collaboration:** The collaborative nature of RaaS operations, where developers provide the tools and affiliates execute the attacks, has led to a variety of tactics and targets.
- **Effectiveness:** RaaS is highly effective—it works, and it works very, very well. Operators and cybercriminal groups are discovering the value of saving time and effort by avoiding the need for code development, opting instead to utilize pre-made encryption software like LockBit.

The underground economy supporting these types of malicious services will continue to thrive and likely grow in 2024. The anonymity associated with the darknet environment will persist in contributing to the resilience of this cybercriminal ecosystem, making it challenging for law enforcement and cybersecurity professionals to effectively take down ransomware operations and their operators.

Ransomware Gangs Become More Sophisticated

While ransomware gangs commonly leverage known vulnerabilities to gain initial access to victim environments and tools like Cobalt Strike for post-exploitation activities, 2023 saw a trend in the exploitation of zero-day vulnerabilities (MOVEit, GoAnywhere, Citrix devices, PaperCut, etc.) and deployment of custom tooling by ransomware actors. Most notably, actors like the Play ransomware group are developing custom info-stealers including 'Grixba' and 'Costura' that enable the swift enumeration and exfiltration of files on targeted systems.

In general, Ransomware actors are becoming better at identifying and leveraging zero-day flaws to compromise victim organizations. For instance, in 2023, CL0P ransomware actors uncovered a SQL injection bug (CVE-2023-34362) in the MOVEit file transfer application and were able to exploit the zero-day flaw to compromise and steal data from over 1,000 organizations and 60M+ individuals. It is estimated that CL0P could earn close to $100 million from their MOVEit mass-hacking campaign.

During the same year, this same group of actors also exploited another zero-day in the Fortra GoAnywhere secure file-sharing solution to breach over 130 organizations and impact over 1.17 million individuals.

Despite efforts made by organizations to apply patches promptly, with groups like CL0P abusing zero-day vulnerabilities before patches become available, it's a challenge to deter potential attacks.

Data Extortion Becomes More Common

Ransomware actors are starting to find success in attacks without resorting to deploying a ransomware payload. While the notion of deploying an encryptor and holding files for ransom has traditionally been lucrative for these threat actors, companies and security professionals have become more efficient in decrypting files and finding bugs in encryptors, rendering such attacks less effective.

Consequently, threat actors are increasingly resorting to alternative tactics, such as the extortion of sensitive data, to generate revenue. In such instances, attackers will steal and threaten to disclose the data online unless a ransom is paid. Given that such data may contain a treasure trove of valuable company secrets, it is also not uncommon for other cybercriminals and even business competitors to be willing to pay excessive amounts of money to acquire the data.

New Ransomware Variants Enable Wider Targeting

Programming languages like Rust have become a popular choice among ransomware groups including BlackCat, Hive, Luna, RansomExx, and many more, all of which have released Rust-based encryptors. In particular, Rust is a cross-platform language, enabling actors to target a wider range of victims beyond those running Windows systems. More so, Rust is more difficult to analyze and has a lower detection rate by antivirus engines, making it a suitable language to use when developing malicious payloads.

Go programming language also seems to be popular among ransomware actors. LockBit in particular is starting to test macOS encryptors. Among the latest developments is 'Turtle,' a LockBit variant written in Go that is designed to target macOS systems. Although newer ransomware variants like Turtle may not initially pose a significant threat as they are still under development, the increase in variants and switch to languages like Rust and Go indicate an effort made by ransomware actors to compromise more victims and target operating systems outside of Windows.

Third-Party Vendor Risk

As businesses increasingly rely on external partners for critical services, such as payment processing and cloud infrastructure, these vendors become attractive targets due to their access to sensitive customer data. For instance, late last year, a retailer was breached after threat actors targeted one of its service providers, leading to the exposure of personal information affecting 1,977,486 people. Additionally, the same year, the CL0P ransomware gang showcased heightened sophistication evident in the MOVEit vulnerability exploit, impacting over 2,000 organizations.

Therefore, effective third-party risk management will be an important security priority for many organizations going forward. Regular engagement between companies and their third-party partners meeting with these third-party suppliers can help drive improved security and mitigate potential threats. Third-party suppliers and partners can reduce their susceptibility to these attacks by deploying sound patch management policies and using MFA.

Remote Management Tools and Legitimate Software Leveraged in Ransomware Attacks

There has been a notable trend in the use of legitimate software tools in ransomware attack chains. This includes tools like remote monitoring and management (RMM) software such as AnyDesk and ConnectWise which can be leveraged to bypass administrative requirements and software management control policies as indicated in an advisory published earlier last year by the Cybersecurity and Infrastructure Security Agency (CISA) warning against the malicious use of RMM software. Tools like Rclone, a command-line program to manage files on cloud storage, and AdFind, a command-line query tool used for gathering information from Active Directory, are also being leveraged for nefarious purposes.

Rclone in particular has been deployed by actors like Noberus ransomware to exfiltrate files before encryption. Given that tools like Rclone are legitimate programs, this enables ransomware actors to perform their exfiltration activities without being detected by anti-virus solutions.

What to Expect in 2024

In 2024, the overarching prevalence of ransomware in the cyber threat landscape is anticipated to persist. This enduring trend is underscored by the continual emergence of new ransomware groups, coupled with the adept utilization of tools and services by these threat actors. As long as the likelihood of a payday is high, and the risk of getting caught is low, ransomware will remain a threat.

In particular, Artificial Intelligence (AI) has experienced substantial growth and adoption in the past year. Notably, AI services like ChatGPT have been exploited for purposes such as crafting tailored phishing emails and even generating code to be used in developing malicious payloads. With the help of such services, actors who aren't native to the English tongue can now create phishing messages that are not prone to grammatical errors, making it challenging for end users to detect and defend against such lures.

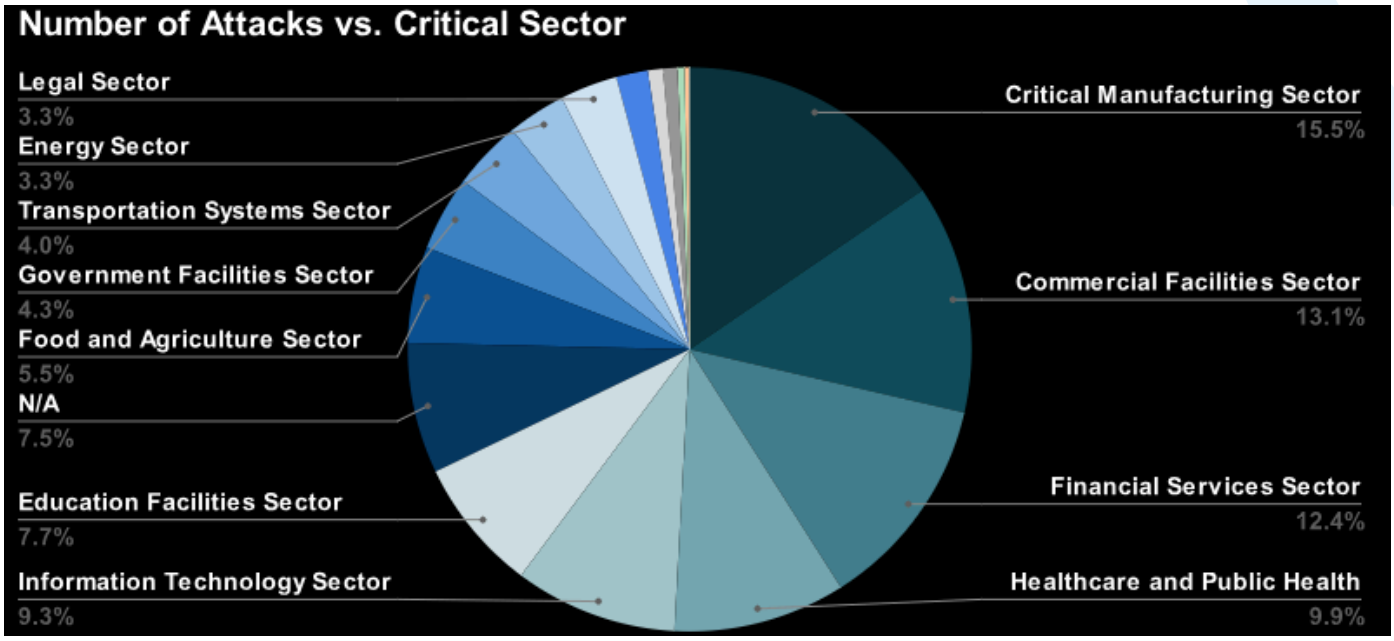
Artificial intelligence is still in the initial phases of development. As the technology improves, we will likely see a continued increase in cybercriminals, including ransomware gangs, exploiting this new tool for malicious purposes.

General Ransomware Mitigation

- **Keep your information backed up:** Run backups frequently and store the data from these backups offline in a safe place. Keep them disconnected from the business network; ransomware variants may target backups, deleting or encrypting them if they get access. Regular backups are essential to combating ransomware – if your data becomes encrypted or compromised, then your organization can restore it quickly if an up-to-date backup is on hand.
- **Regularly update and patch systems:** Perform regular maintenance on the security of your systems: specifically operating systems, firmware, and applications. Risk-based assessment can help determine your patch management procedures; we recommend using a centralized patch management system if at all possible.
- **Have an incident response plan ready (and test it):** Not only do you need to have a plan in place for if an incident occurs, but you need to thoroughly test that plan to ensure there are no weak points. A strong incident response plan is one that's been run through a few times to iron out the flaws.
- **Test your security with a third party:** A third party pen tester can find gaps in your security that you may not have otherwise known about or noticed. Ransomware criminals may go to sophisticated lengths to enter any unlocked doors in your network; get assistance to ensure everything is sealed tight.
- **Segment networks for safety:** More and more ransomware attacks don't just focus on capturing data, but aim to throw a wrench in organizations' operations. This makes network segmentation especially important.
- **Thoroughly train your staff:** No matter how sophisticated ransomware attacks become, email continues to be the easiest and most effective pathway in for attackers. Keep employees informed about potential phishing scams and how to avoid them through regular training.
- **Use multi-factor authentication:** Additional failsafes like multi-factor authentication can also provide a layer of protection, requiring more identification from bad actors attempting to compromise an account.
- **Drive improved security of third-party partners:** While organizations should strive to reinforce their own defenses, 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. Less mature members of your organization's supply chain may not have dedicated staff or resources to implement security best practices. Network segmentation should be leveraged, and identity and access management controls should be in place to prevent third-party provisioned accounts from allowing a threat actor into your environment. The Food and Agriculture-ISAC has prepared a Cybersecurity Best Practice Guide for Small and Medium Sized Businesses. This guide offers several low-cost, and easy-to-implement security tips to help secure your less mature supply chain partners.

By the Numbers

Ransomware Attacks Against Critical Infrastructure Globally 2023

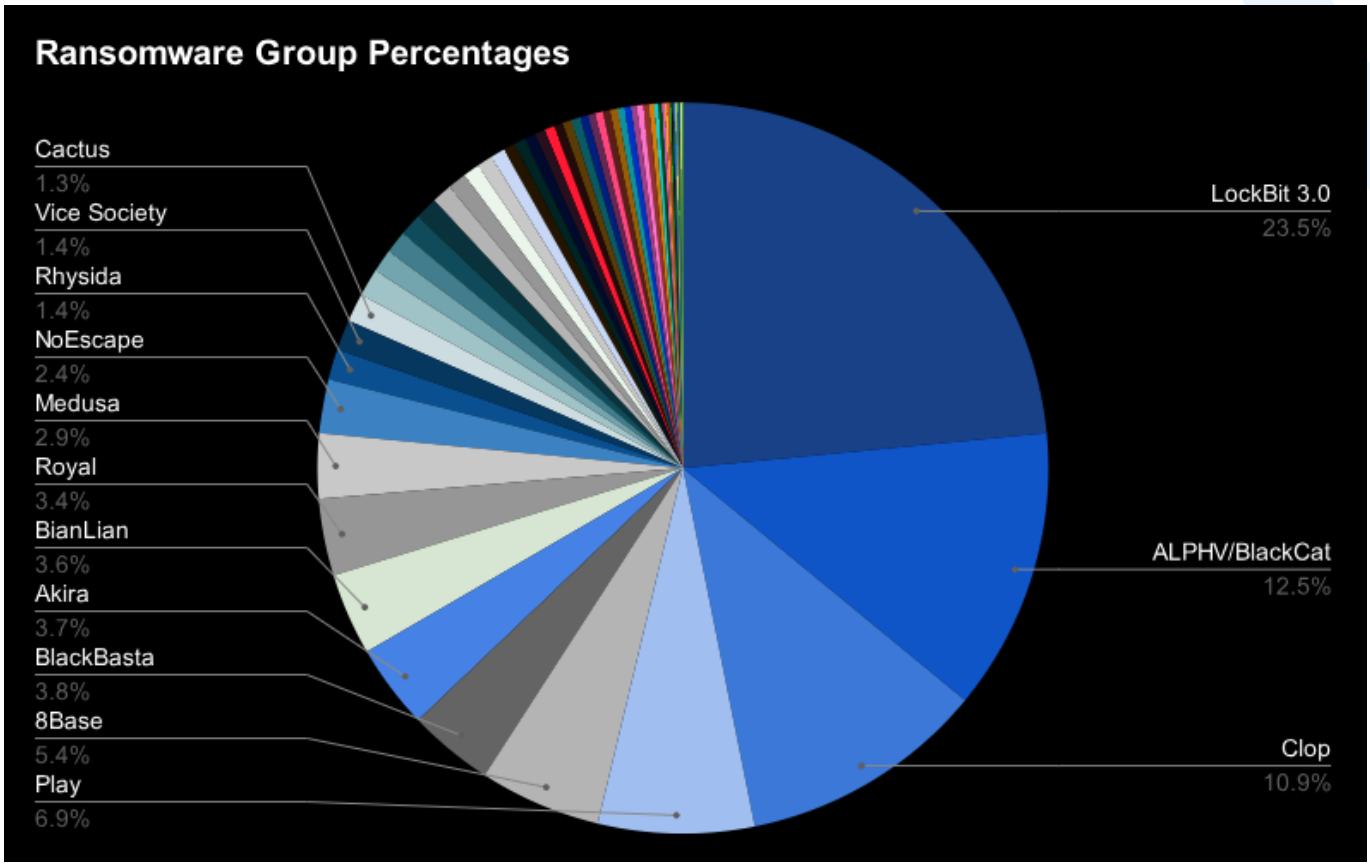


TOP 5 | Ransomware Attacks Against Critical Infrastructure

- Critical Manufacturing Sector - [468 Attacks] - [15.5%]
- Commercial Facilities Sector - [398 Attacks] - [13.1%]
- Financial Services Sector - [375 Attacks] - [12.4%]
- Healthcare and Public Health Sector - [299 Attacks] - [9.9%]
- Information Technology Sector- [283 Attacks] - [9.3%]

By the Numbers

Ransomware Attacks by Group Globally 2023

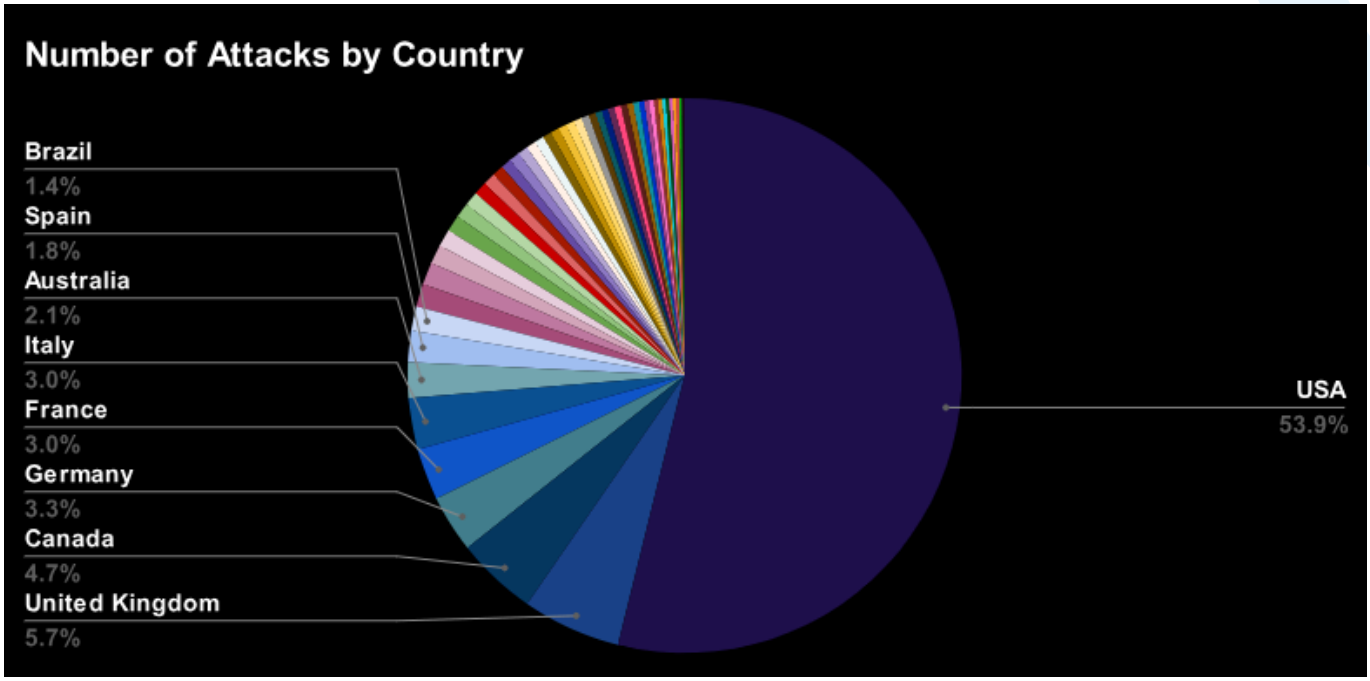


TOP 5 | Ransomware Attacks by Group

- LockBit 3.0 - [711 Attacks] - [23.5%]
- ALPHV/BlackCat - [378 Attacks] - [12.5%]
- Cl0p - [330 Attacks] - [10.9%]
- Play - [209 Attacks] - [6.9%]
- 8Base - [163 Attacks] - [5.4%]

By the Numbers

Ransomware Attacks by Country Globally 2023



TOP 5 | Ransomware Attacks by Country

- United States of America - [1565 Attacks] - [53.9%]
- United Kingdom - [167 Attacks] - [5.7%]
- Canada - [137 Attacks] - [4.7%]
- Germany - [97 Attacks] - [3.3%]
- France - [88 Attacks] - [3.0%]

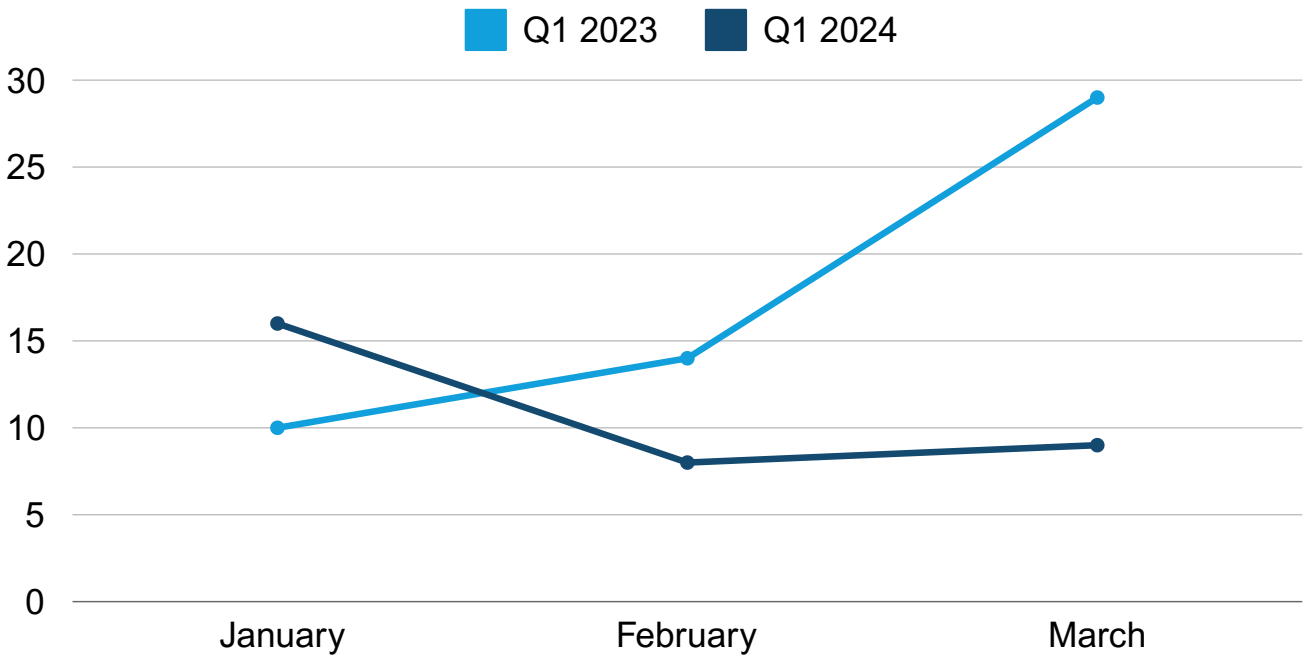
Q1 2024 Analysis
January - March

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.

IT Sector Q1 Ransomware Attacks
2023 vs. 2024



Q1 2024 Analysis Continued

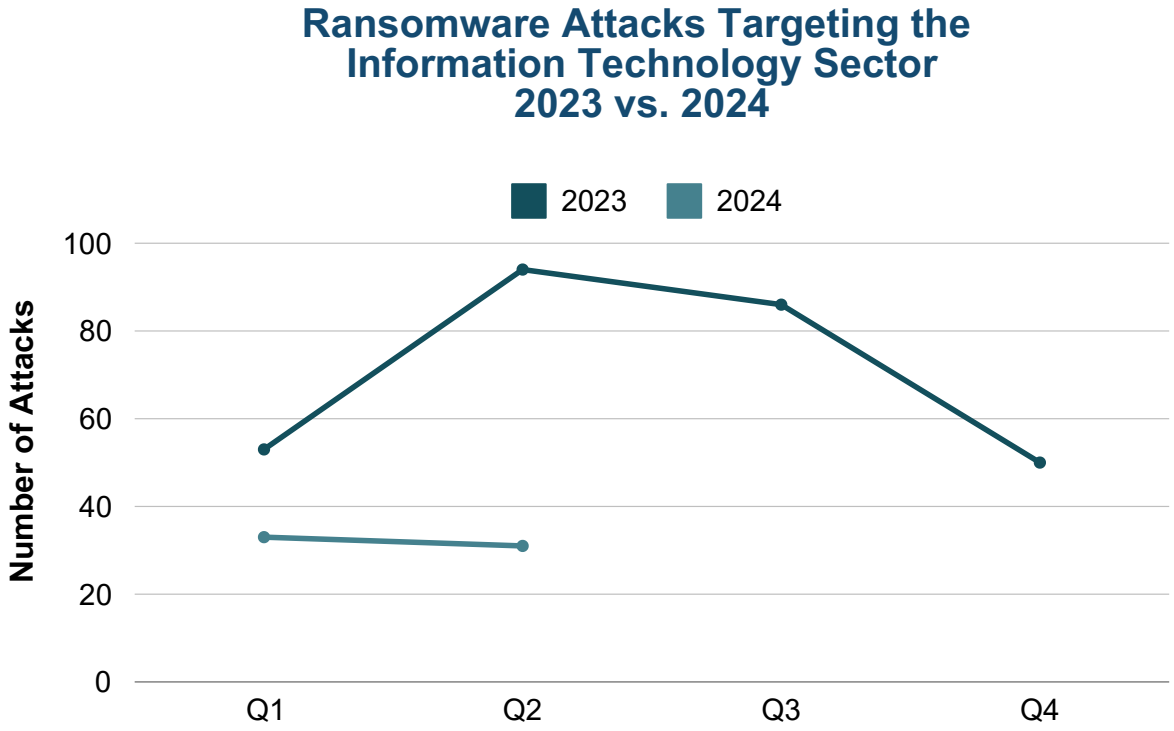
Another noteworthy event was law enforcement's takedown of BlackCat's infrastructure in December 2023, and LockBit's in February 2024. These groups typically occupied the top positions in monthly ransomware attack rankings. However, since the takedowns, operational functionality has declined for both 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 BlackBasta, 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.

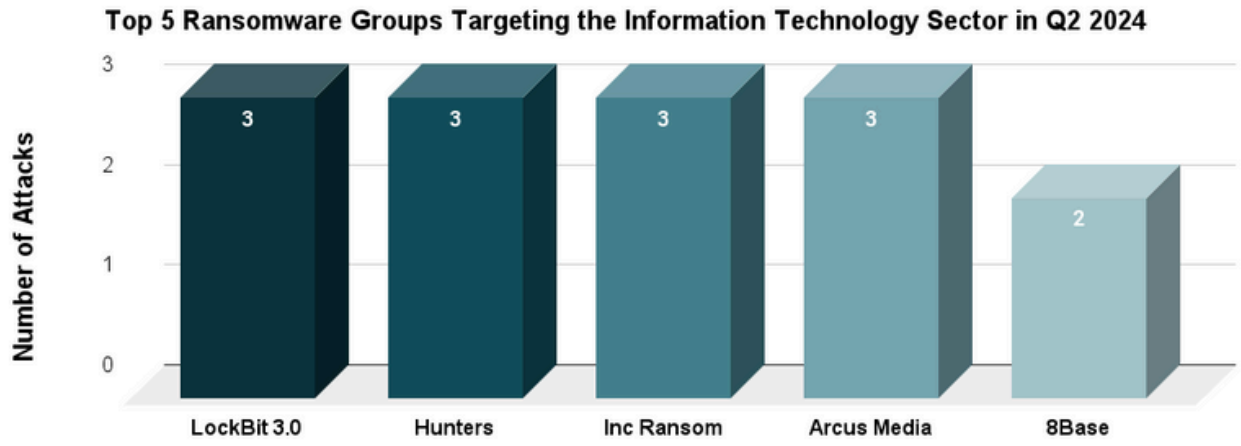
Q2 2024 Analysis

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.

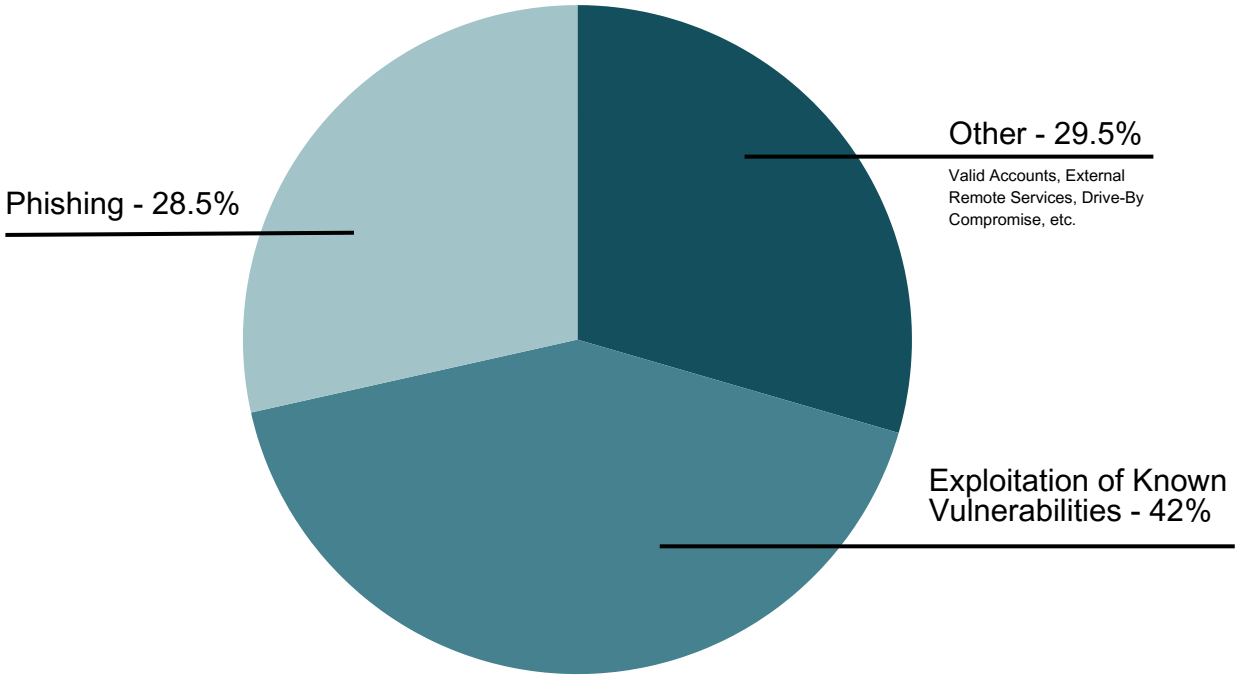


Q2 2024 Analysis Continued

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.

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%.

Initial Access Vectors Employed by Ransomware Actors in Q2 2024



Q2 2024 Analysis Continued

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.

IT ISAC

FOUNDED 2000

How We Collect Our Data

Note that metrics for Q2 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.

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