GUIDEPOINT® SECURITY

GRIT®

2025 Q1 Ransomware & Cyber Threat Report

Contents

Methodology

Data collected for this report was obtained from publicly available resources, including threat groups themselves, and has not been validated by alleged victims. Collected data is reviewed for potential duplications or inaccuracies, and adjusted accordingly. Thus, the number of publicly observed attacks and the actual number of attacks conducted may not be equal. Some groups do not publicize all of their victims and almost all groups offer an option to withhold announcement if the victim pays a ransom within a specified timeframe and/or remove the victims once a ransom has been paid. Additionally, some groups include incomplete information about their victim or claim an attack despite successfully attacking only a small subset of their target. For these reasons, the data in this report is useful in aggregate, but should be evaluated as a report consisting of data sources that have variability. Despite that variability, this report is still an accurate representation of the total ransomware threat landscape.

We note that this report includes data and analysis of several groups that may be better described as "extortion" groups rather than "ransomware" groups. These groups may eschew encryption and instead focus only on data exfiltration and extortion, or may not perform intrusion operations of any kind, instead extorting or re-extorting organizations based on historically compromised data. While these groups do not deploy ransomware, we are including them in our reporting due to their relationships with other ransomware groups and their impact on the extortion-based cybercrime environment.

Finally, we make efforts to exclude from our data those groups which self-identify as “hacktivists”, groups we assess with high confidence to be serial fabricators, or non-financially motivated data thieves and leakers. While these actors and venues doubtlessly have impacts, we distinguish them from financially-motivated cybercrime and data extortion which is the primary focus of this report. For this reason, our data may periodically reflect lower total numbers of incidents than other, similar public reports.

Quarterly Ransomware Summary

The ransomware ecosystem is off to a hot start in Q1 2025, with a greater number of victims posted to data leak sites than any other quarter in history. The year-over-year and quarter-over-quarter increases we observed are shocking at face value, but a deeper dive reveals that several things had to come together to reach these new heights.

The Intermittent data extortion group Clop (also stylized as Cl0p) served as the primary driver of this increase, claiming 348 of the 2,063 total victims we observed in Q1 – around 17%. Deploying tactics that have become the group's *Modus Operandi*, Clop extorted a vulnerability in a managed file transfer application at scale, resulting in widespread data theft within impacted environments across many organizations in one fell swoop. Even though this attack occurred towards the end of 2024, the threat group continued actively posting victims through Q1, following failed negotiations with said victims and other logistical work.

Separately, RansomHub continued to operate at a high operational tempo. The most prolific ransomware as a service (RaaS) group posted 236 victims throughout the quarter, or 11.4% of all observed victims. Akira also contributed substantially to the quarter's high victim count, relying heavily on compromise of VPN and edge devices to claim 213 victims.

In previous iterations of this report, we have discussed the growing "middle class" of ransomware actors, which conduct continuous operations at a more moderate tempo across a greater number of groups. Q1 continued this trend, with a new quarterly record high of 70 named ransomware or data extortion groups observed claiming victims. This "middle class," which includes Play, Lynx, Fog, and others, contribute to a less centralized victim count compared to past years – in which prolific groups such as LockBit and Alphv each accounted for the lion's share of observed victims.

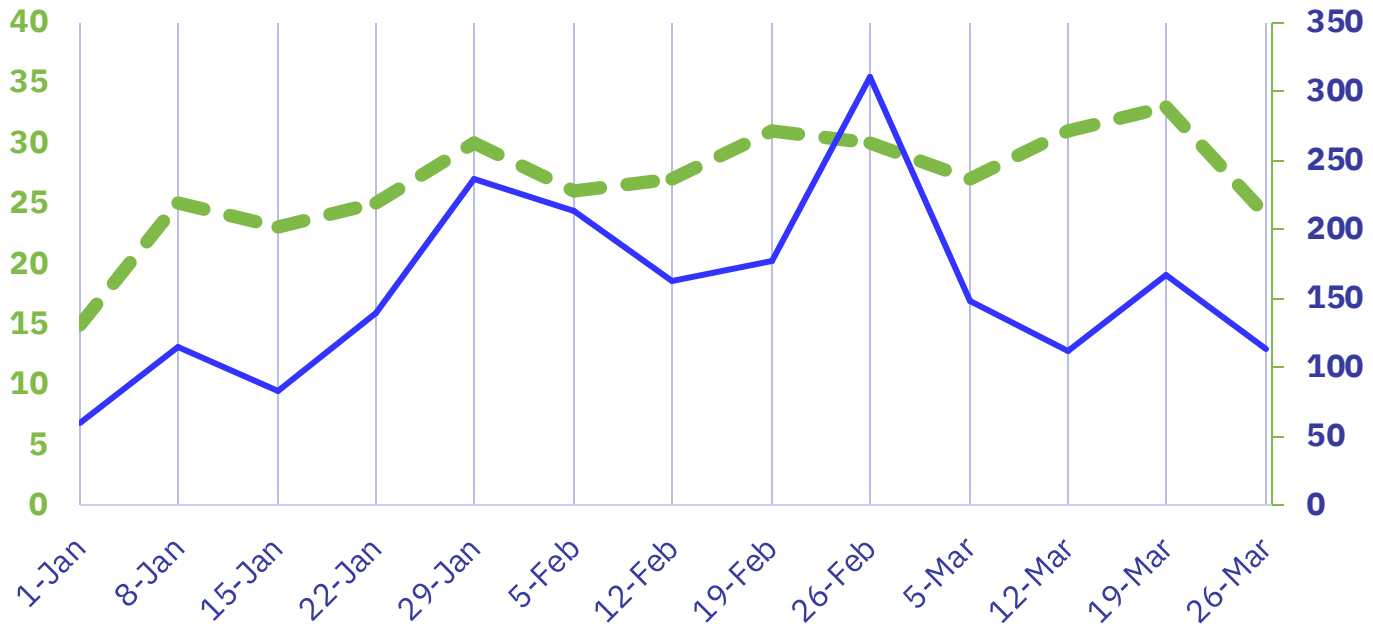
The secret behind this record-breaking quarter is clear: we have observed a rise in ransomware and data extortion groups, with more of them operating continuously. Additionally, high-volume groups, emerging from the collapse of previously disrupted entities LockBit and Alphv, continue to operate with notable efficacy. It remains to be seen whether this quarter will represent a temporary increase or the beginning of a dark year for ransomware victims.

Read on for GRIT's analysis of this quarter, and our thoughts on what is yet to come.

	Q1 2025	Q4 2024	Q1 2024
Total Publicly Posted Ransomware Victims	2,063	1,577	1,023
Active Ransomware Groups	70	60	45
Average Daily Victims	22.9	17.1	11.2

Threat Actor Trends

Rate of Publicly Posted Ransomware Victims, Q1 2025



Total Posts	Total Groups	Average Posts per Week	Average Groups Posting per Week
2,063	70	156	26

Throughout the first calendar quarter of 2025, we observed an increase in attacks on a weekly basis relative to preceding quarters. Though we note that recurring batch posts of victims from Clop – including one of 188 victims on a single day in late February – created spikes across the month. In spite of this, even if we were to remove Clop's 348 victims from consideration in the Quarter's totals, we still would have observed 1,715 victims, an 8.75% quarter-over-quarter and 67.64% year-over-year increase.

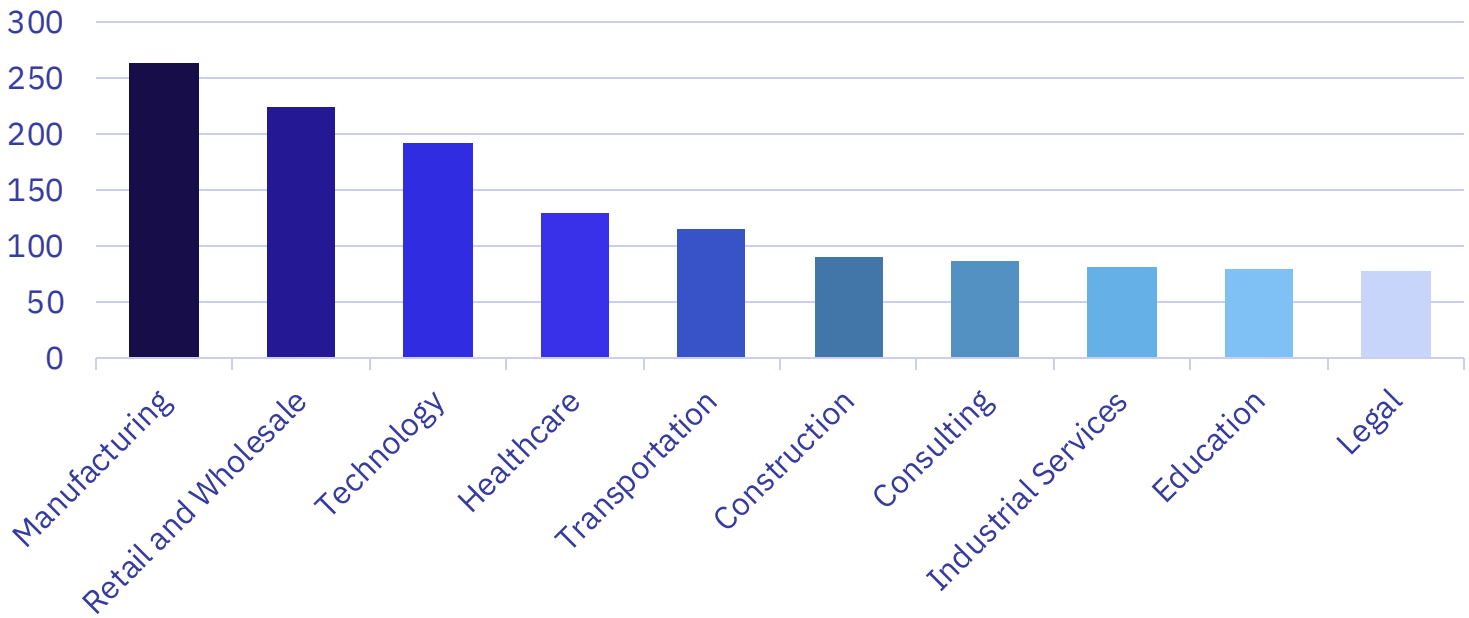
The quarter's overall high victim volume can be attributed, at least in part, to an abnormally high number of uniquely named ransomware and data extortion groups operating throughout the quarter, setting a new quarterly record of 70 active groups. For comparison, we observed 60 active groups in Q4 2024, and only 45 active groups in Q1 of 2024, marking a 16.6% and 55.5% increase, respectively. This suggests that the number of distinctly named ransomware and data extortion groups has not yet "peaked," as the diversity of active groups continues to increase.

Most Impacted Industries, Q1 2025

The industries most impacted by ransomware in Q1 remained largely consistent quarter-over-quarter and year-over-year, with victims from the Manufacturing, Technology, and Healthcare industries remaining among the most frequently observed. The automotive industry saw a moderate 12.2% rise in incidents (from 41 in Q4 2024 to 46 in Q1 2025), signaling continued impacts against an industry that heavily relies on uninterrupted supply chains and continuous operations.

The education industry experienced an uptick in Q1 compared to Q4 last year, with incidents jumping from 68 to 79 (+16.18%). Many schools and universities with dated infrastructure and valuable student data continue to represent an attractive target to both emerging groups and more established threat actors.

Unfortunately, we also observed a staggering doubling of ransomware attacks on non-profits, jumping from 16 to 33 incidents from the previous quarter. These organizations often operate with very limited cybersecurity resources and lack the necessary funds to support modern cyber defenses. Non-profit organizations, including churches, mental health centers, rehab centers, and more, present an easy opportunity for ransomware groups to impact less-well-resourced organizations. Some of the more prominent ransomware groups such as Inc Ransom and RansomHub have each taken part in the total impacts to the non-profit space this quarter.



Manufacturing
- Clop
- Akira
- RansomHub

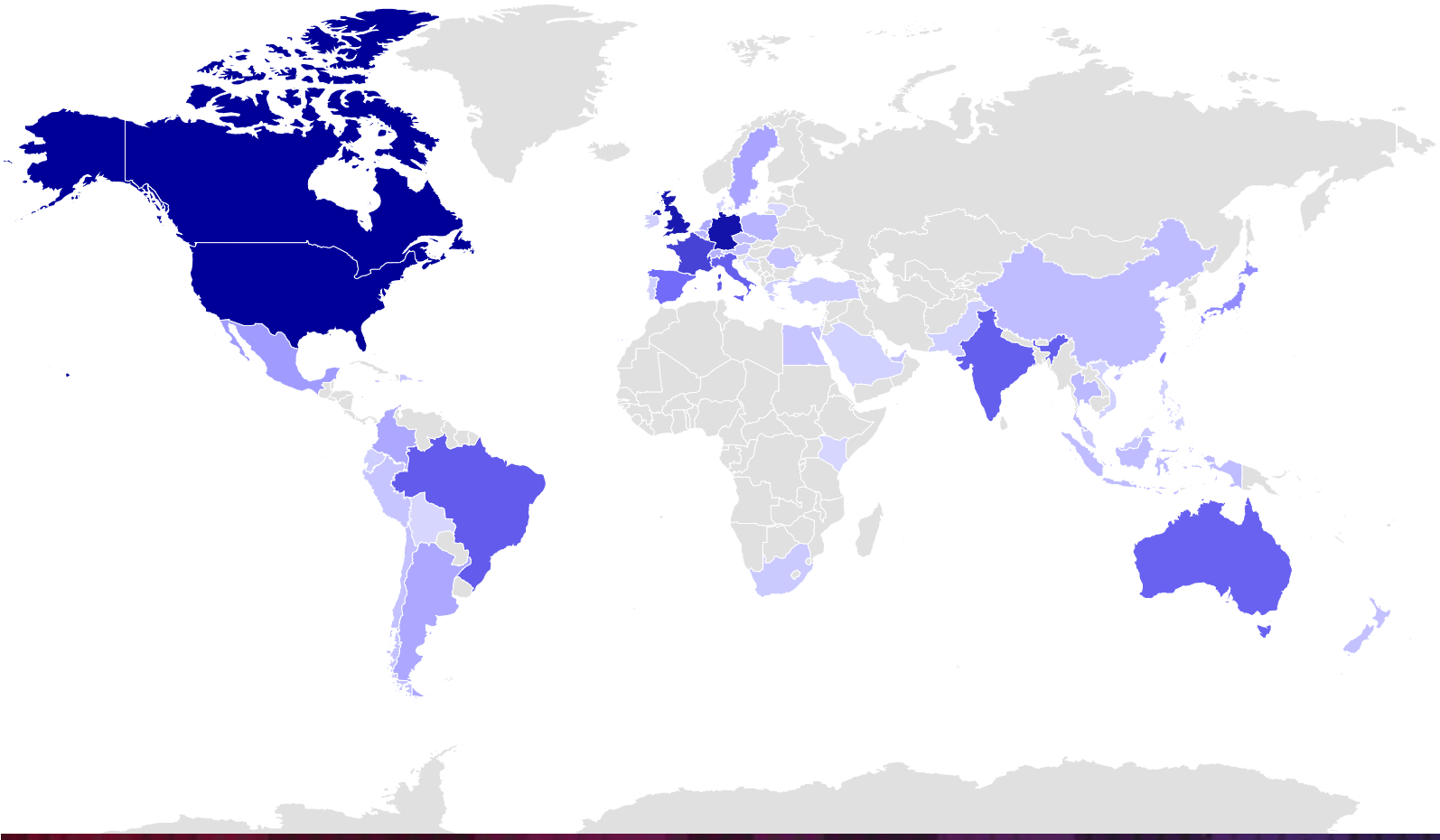
Retail and Wholesale
- Clop
- RansomHub
- Akira

Technology
- Clop
- Fog
- Akira

Healthcare
- Qilin
- IncRansom
- RansomHub

Transportation
- Clop
- RansomHub
- Akira

Geographic Breakdown of Ransomware Victims, Q1 2025



Top 10:

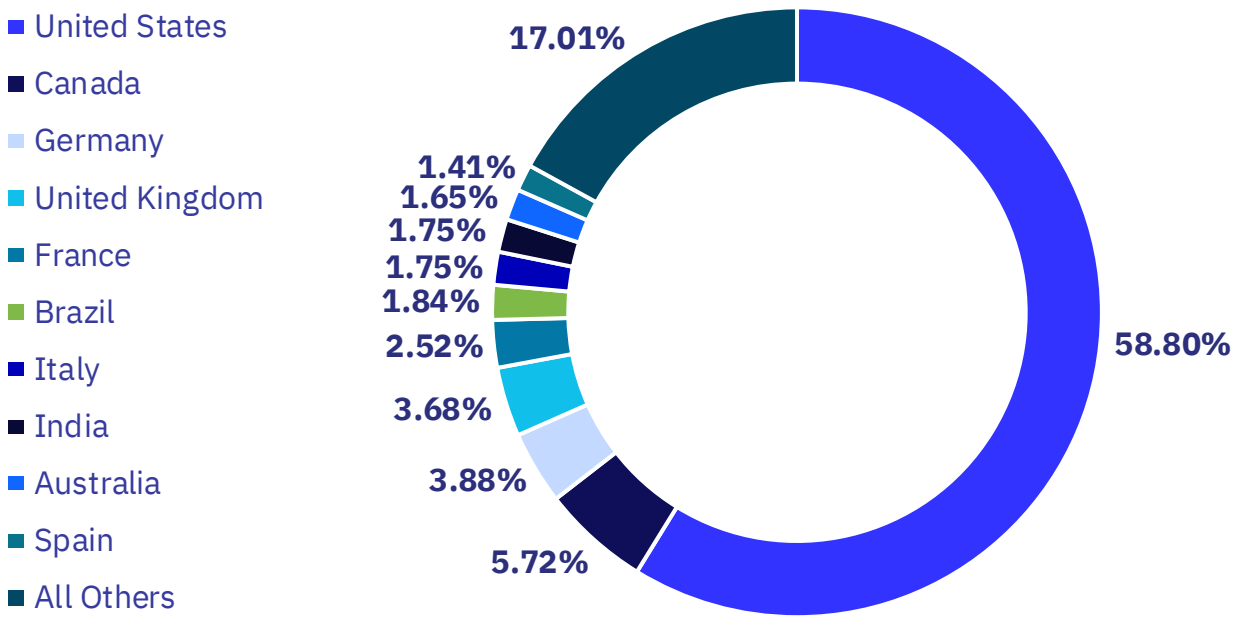
1. United States
2. Canada
3. Germany
4. United Kingdom
5. France
6. Brazil
7. Italy
8. India
9. Australia
10. Spain

Ransomware Impacts by Country, Q1 2025

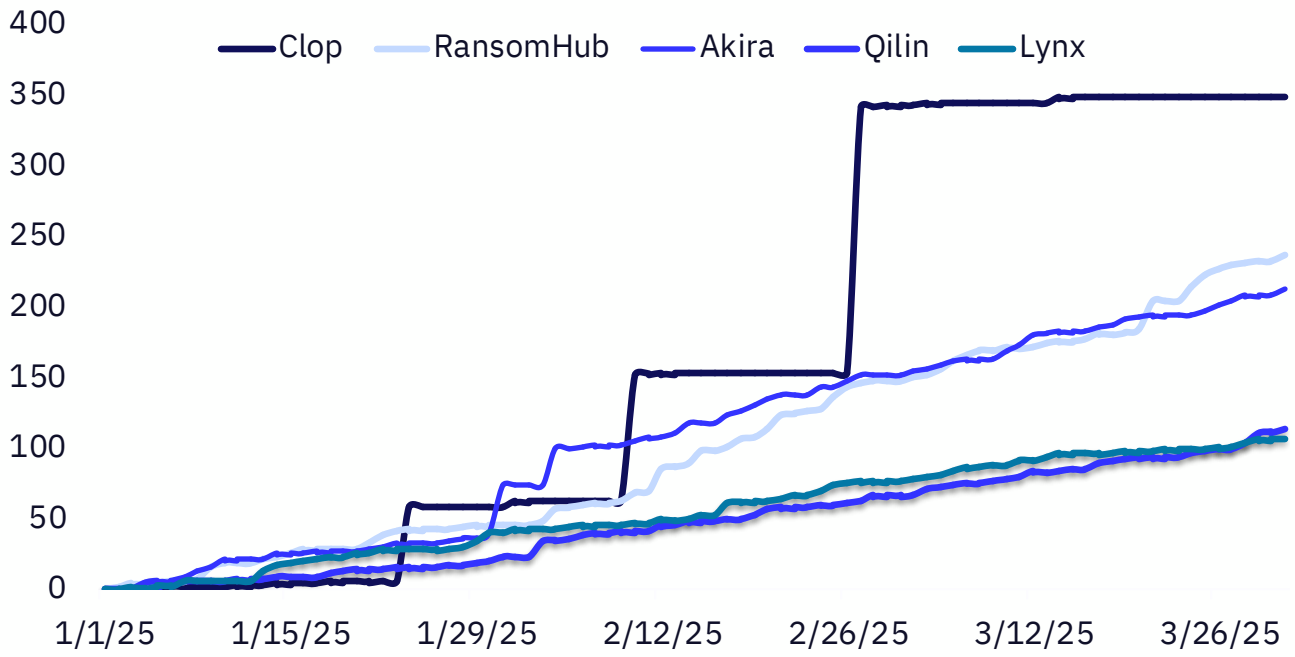
While the United States remains, the country most impacted by ransomware, the Q1 presented an increased percentage of US-based victims at 58.8% – the highest we've observed since we began tracking ransomware statistics in 2022. Other western nations – Canada, Germany, the United Kingdom, and France – remain among the most impacted, and the developing economies of Brazil and India continue to receive numbers of victims. The presence of Italy among the most impacted countries is historically anomalous.

As ransomware continues to plague organizations and nations worldwide, one country remains a notable outlier: China. Over the past two years, out of 11,538 recorded ransomware victims, only 56 were reportedly located in China. Given the country's massive economy, the relative lack of ransomware incidents is in stark contrast compared to other modern economies. While it's tempting to assume that Chinese organizations are simply better defended, the reality is likely more complex. Factors such as government control, cultural tendencies, and cybersecurity policies all likely play a role in shaping this anomaly.

However, recent developments indicate that China might not be entirely off-limits for the current crop of ransomware operators. Threat groups including RansomHouse, DarkVault, CrazyHunter, DragonForce, Hellcat, and Play have all posted alleged victims headquartered in China in Q1 2025. Whether this marks the beginning of a larger trend or remains an exception will depend on how effectively these groups can navigate the barriers that have historically deterred ransomware activity in China.



Cumulative Victims by Threat Group



Clop

Clop's resurgent mass exploitation tactics resulted in its clear placement among the most impactful ransomware and data extortion groups in Q1. Clop's use of tranches to post groups of victims spread over time can be observed in the above chart, reflected in periodic spikes followed by 1-2 weeks without activity. We assess that once Clop's posting of victims from recent campaigns is complete, they will return to a period of dormancy until such time as they uncover and weaponize a similar vulnerability for future mass exploitation.

RansomHub

RansomHub remains the most prolific RaaS group by victim volume, consistently holding the position it seized quickly in late 2024. The group's victim posts remain voluminous but steady, with the group falling short of Q4s observed victim count by only four posts. Unlike Clop, RansomHub shows one of the more consistent posting schedules and threatens data publication at their own discretion, usually immediately following a failed or ignored negotiation.

Akira

Although we observed numerous "technical difficulties" impacting Akira's infrastructure over the course of the quarter, the group remains one of the most prolific RaaS groups by victim volume, exhibiting a staggering 110% increase in observed victims from Q4 2024 to Q1 2025 with 213 observed victims. The group's increased activity can be more clearly observed year-over-year, in which Akira's activity has jumped 261%. This increase could reflect continued operational success in attacking VPN and perimeter devices, as well as the absorption of experienced affiliates from other ransomware groups.

Threat Actor Spotlight: Hellcat

Threat Actor Spotlight: Hellcat

Hellcat, a Developing ransomware operation, first began claiming victims in October 2024, but it has quickly sought public attention across multiple outlets through outlandish demands and multiple interviews. For example, in an early and well publicized attack against a French energy company, Hellcat demanded a ransom of $125,000 “in baguettes.”

While “marketing” efforts for most ransomware operations typically take place on deep and dark web forums, members of Hellcat have opted to instead take a more public approach. Hellcat’s operators have participated in multiple interviews, granting a greater degree of visibility into the inner workings of that group relative to their contemporaries. This is abnormal behavior for threat actors who are generally concerned with their Operational Security (OPSEC), but due to either naivety or an overinflated sense of confidence, Hellcat’s members have repeatedly, and perhaps inadvertently, disclosed details regarding the group’s operations, allowing researchers to partially identify several members. Many of the individuals within Hellcat publicize their actions on the social media site X, where they regularly share updates on their cybercrimes. We’ve noted a few of the group’s more public members to take a closer look.

Threat Actor Spotlight: Hellcat (Continued)

Hellcat Operator: Pryx
Other Aliases: holypryx, sp1d3r

Pryx is a cybercriminal who has been active since at least June of 2024, according to the activity from the user's profile on the dark web forum XSS. Pryx appears to be an administrator of the group based on an interview conducted by Osint10x. The interview also yielded some key information on Pryx, such as the claim that they are only 17 years old, and their reliance on phishing for initial access into victim networks. The actor also displays immature attitudes throughout their online presence, including openly racist and antisemitic views.

Reviewing Pryx's activity on the dark web forum XSS also helps identify some other potential OPSEC missteps. Pryx posted in June 2024 that they were able to breach a community college in New Jersey, United States, and were offering to sell data from the incident. One user, `coolman1`, questioned Pryx as to why they selected the community college for their attack, to which Pryx responded "I wanted to study there, I visited the site and boom there is an idor [insecure direct object reference] lol." Pryx's claim of being 17 years old aligns with a normal age that someone could reasonably be for seeking out secondary education. It would be unusual for someone outside the United States to travel to the country to enroll in a community college, although we cannot entirely rule out this possibility.

Pryx has also uploaded and shared YouTube videos in certain XSS threads. One such video, titled *xss.is competition pryx*, displays Pryx sharing their screen while showcasing their submission for a competition held on XSS. The screenshare shows Pryx's date and time of recording, which are in the standard Year/Month/Date format commonly used in the United States.

These two data points, coupled with the actor's exclusive use of language by an evident native English speaker leads GRIT to assess with a low degree of confidence that Pryx is located within the United States. If Pryx continues their lackluster attitude towards OPSEC, there is a fair probability of the actor inadvertently disclosing additional information that could lead to their identity.

Pryx's response to a user's question on XXS

Threat Actor Spotlight: Hellcat (Continued)

Hellcat Operator: Miyako
Other Aliases: Miya

Miyako is a self-proclaimed administrator of Hellcat according an interview with the actor held by Osint10x. It is this interview that Miyako discloses some insight on their methodology. Miyako presents themselves as an individual who is methodical in their OPSEC procedures, specifically stating “I route all operations through layers of VPNs and TOR nodes, use burner devices, and maintain strict OPSEC. My code and communication avoid linguistic patterns that could lead to attribution. I also diversify my monetization efforts to avoid creating patterns." They also shed some light on their initial access methods by highlighting spear phishing, in particular, as an effective measure.

Hellcat Operator: Rey
Other Aliases: wristslit, ReyXBF, HikkI-Chan

Rey appears to be an affiliate of Hellcat and not a member in the administrative aspect. Rey has been active on the illicit forum, BreachForums, since at least August of 2024. Similar to Pryx, Rey portrays an immature persona in the forum, consistently using overtly racist and antisemitic language throughout their post history. In addition, Rey’s communications across BreachForums are consistent with those of a native English speaker, suggesting they could reside in an English-speaking country. Of note, on February 28, 2025, Rey shared a supposed dox on themselves, indicating that they were a 27-year-old Irish female. It is less likely that this dox is legitimate, as GRIT was unable to validate any of the information contained in the post. Despite allegedly working as a Hellcat operator, Rey still opts to share some of their ill gained victim data to BreachForums instead of the Hellcat data leak site, which could represent attempts by Rey to maintain their own personal brand independent of Hellcat.

Threat Actor Spotlight: Hellcat (Continued)

Hellcat Operator: grep

Although originally mentioned as an administrator by Miyako and Pryx, grep has since attempted to distance themselves from the group. On March 21, 2025, grep published a post on X claiming that they no longer are participating in cybercrime, including ransomware activities.

grep announcing their withdrawal from "cybercriminal activity"

We cannot assess the validity of grep's withdrawal from criminal activities, but just days later, on April 1, grep shared another X post which could indicate they are still actively stealing data from an "IT company." grep also regularly interacts with X posts created by both Rey and Pryx, further indicating the user still has some association with the Hellcat group.

grep disclosing an alleged "campaign" against an IT company

Industry Spotlight: Non-profits

Industry Spotlight: Non-profits

One of the more unfortunate findings this quarter was the doubling of ransomware attacks against non-profit organizations, jumping from 16 to 33 reported incidents in the previous quarter. These organizations often operate with minimal cybersecurity resources and lack the necessary funds to support modern cyber defenses. As the cost of cybersecurity tools, personnel, and services continue to rise, smaller organizations may be unable to afford adequate defenses to keep up with prolific ransomware threats. On a related note, many non-profits maintain a financial focus on their mission rather than the improvement of internal processes, in general, such as properly configured backups and incident response plans. Non-profits often rely on shared platforms or other third-party vendors, which elevate the risk of infection. Not to mention, many of these organizations entirely outsource their IT to a third-party that may not prioritize security.

Depending on the type of non-profit organization, the classification of internal or hosted data may vary widely as some may not house any important or sensitive data. In contrast, rehab or mental health organizations may have troves of sensitive information on individuals. Conversely, some churches or other religious organizations may have more important corporate data than personal data. Another factor that comes into play is the lack of critical applications used by most non-profits. In a ransomware incident, it would be fairly uncommon for a non-profit's operations to be fully stalled due to encryption beyond some minor inconveniences. For example, software used by churches largely control scheduling, events, media, and outreach; however, the downtime experienced may not compel an organization to aim for any settlement with the threat actor to obtain a decryption tool.

Ransomware groups heavily rely on their reputation; one of the ways in which they seek to gain notoriety is to "boost their stats" by claiming more victims than other groups. While attacking non-profit and charitable organizations may not build a very good reputation for a brand based on good morals and values, a high victim count can demonstrate a rather formidable threat to their victims and to the public. In this light, non-profit organizations such as churches, mental health centers, rehab centers, societal organizations, and others, present an easy opportunity for ransomware groups seeking to inflate victim counts. Two of the more prominent ransomware groups - Inc Ransom and RansomHub - are among the more prominent ransomware groups who have taken part in the increased total impacts on the non-profit sector this quarter, which 7 and 6 victims, respectively.

While it has been atypical for ransomware threat actors to disproportionally target non-profit organizations, we do recognize this upward trend, and will continue tracking and analyzing the motive for financially motivated threat actors to employ this particularly amoral practice. GRIT does not assess any sudden change in motivation for ransomware groups to heighten targeting this industry, however, many non-profits remain an easy target for opportunistic threat actors.

Other Reporting and Events

Vulnerability and Exploitation Roundup, Q1 2025

Analysis of Q1 2025 vulnerability data reveals a significant overall increase in volume, from 11,201 added vulnerabilities in Q4 2024, to 12,333 vulnerabilities published in Q1 2025. The prevalence of CWE-79 (Cross-Site Scripting), CWE-89 (SQL Injection), and CWE-352 (Cross-Site Request Forgery) underscores the continued exploitation of web application vulnerabilities.

Weakness	Count
CWE-79 - Cross-site Scripting	2521
CWE-89 - SQL Injection	948
CWE-352 - Cross-Site Request Forgery	699
CWE-862 - Missing Authorization	612
Unknown CWE	471
CWE-74 – Command Injection	367
CWE-94 - Code Injection	358
CWE-787 - Out-of-Bounds Write	302
CWE-416 - Use After Free	302
CWE-284 - Improper Access Control	276

Total weaknesses reported in Q1 of 2025

Severity	Count
Medium	5285
High	3606
Unkown	2101
Critical	835
Low	503
None	3

Vulnerability breakout by severity in Q1 2025

Vulnerability and Exploitation Roundup, Q1 2025 (Continued)

Notably, the Known Exploited Vulnerabilities (KEV) dataset saw a marked increase in additions during Q1 2025 relative to preceding quarters, indicating an increasing diversity of actively exploited flaws. In Q1 2024, 44 additions were made to the KEV, whereas 70 additions were reported in Q1 2025, marking a 75% year-over-year increase. The added vulnerabilities were largely the result of deserialization, command injection, and path traversal weaknesses, among others.

Weakness	Count
CWE-502 - Deserialization of Untrusted Data	6
CWE-78 - OS Command Injection	6
CWE-22 - Path Traversal	5
CWE-36 - Absolute Path Traversal	4
CWE-122 - Heap-based Buffer Overflow	4
CWE-416 - Use After Free	4
CWE-506 - Embedded Malicious Code	2
CWE-288 - Authentication Bypass Using an Alternate Path or Channel	2
CWE-787 Out-of-Bounds Write	2
CWE-125 - Out-of-Bounds Read	2

Top 10 CWEs for the KEV in Q1 2025

Examining the KEV dataset further, the top CWEs added in Q1 2025, such as CWE-502 (Deserialization of Untrusted Data) and CWE-78 (OS Command Injection), differ from those of Q1 2024 (CWE-787 and CWE-94) and Q4 2024 (CWE-78 and CWE-306), illustrating a potentially shifting landscape of actively exploited vulnerabilities. This difference indicates a shift from memory corruption-based vulnerabilities (CWE-787, Out-of-Bounds Write and CWE-94, Code Injection) to web application and potentially API-related vulnerabilities (CWE-502 and CWE-78) between early 2024 and early 2025. This variability in exploited vulnerability types suggests a dynamic threat environment where attackers rapidly adapt their tactics based on the ever-changing vulnerability landscape.

Vulnerability and Exploitation Roundup, Q1 2025 (Continued)

The dominance of Microsoft products, particularly Windows, in the list of vendors and across all quarters (36 Microsoft-based KEV additions in all of 2024) reinforces the importance of robust patch management for widely deployed systems, as Microsoft's Windows is the most widely used operating system around the world. It is also worth noting that as of Q1 2025, the total number of Microsoft vulnerabilities added to the KEV is already approaching 50% of those posted in all of 2024, potentially reflecting a greater volume of Microsoft ecosystem vulnerabilities under exploitation "in the wild." Additionally, the consistent appearance of Ivanti products within the top vendor lists across multiple quarters warrants attention as well, indicating potential recurring or increased targeting of Ivanti products across a wide range of threat actors.

Vendors	Count
Microsoft	16
Ivanti	4
Apple	3
VMware	3
Mitel	3
Cisco	2
Sitecore	2
Fortinet	2
Advantive	2
Linux	2

KEV additions by Vendor breakdown in Q1 2025

Law Enforcement Disruption Continues With 8Base Takedown

Since 2024, law enforcement agencies have clearly intensified efforts against ransomware operations, leading to significant disruptions within the world of cybercrime. A notable disruption in Q1 took the form of an international crackdown against the Phobos family of ransomware, including the associated RaaS group, 8Base.

In February 2025, coordinated international operations resulted in the arrest of four Russian nationals suspected of deploying Phobos ransomware under the name 8Base to extort victims across Europe and other regions. These actions also led to the seizure and destruction of 27 servers associated with the ransomware network.

Seizure notice posted on the former site of 8Base

Law Enforcement Disruption Continues With 8Base Takedown (Continued)

8Base, a RaaS group based on the widespread Phobos ransomware family, was responsible for over 1,000 ransomware incidents worldwide, accumulating at least $16 million in ransom payments. Their operations involved double-extortion ransomware, setting ransom demands under the threat of data exposure and public shaming. Based on our observations of former 8Base infrastructure, Q1 takedowns of Phobos and 8Base by law enforcement have, at least temporarily, completely curtailed 8Base operations.

In spite of this short-term success, these disruption operations expose an underlying and unsolved issue of RaaS operations. While the core infrastructure and even leadership of the RaaS group may be effectively disrupted, former affiliates often remain unrestrained and free to realign with newly emerging or existing RaaS groups, continuing their operations and threats to organizations. Following the fall of LockBit and Alphv in 2024, we observed an increase in the operational tempo of several other ransomware groups, reflecting the realignment of these groups' affiliates with other RaaS operations. We are likely to observe a similar realignment of victim volume from 8Base's affiliates in the months ahead.

A logo associated with the former 8Base RaaS Group

Black Basta's Chat Leaks Followed By Operational Cessation

In February 2025, a large cache of internal message logs alleged to be from the Established Black Basta ransomware group were leaked by an individual presumed to be a disgruntled ex-member. These logs contain messages from September 18, 2023, through September 28, 2024, that appear authentic and reflect operational details that the GRIT team has been able to verify from historical incident response cases of the GuidePoint Digital Forensics and Incident Response (DFIR) team, open-source intelligence, and intelligence-sharing partnerships. The leak provided incredible insight into the day-to-day operations of a fairly prolific ransomware operation and likely played a role in its downfall. GRIT has broken down our initial insights provided by these chat logs, in detail, in a standalone blog titled Breaking Basta: Insights from Black Basta's Leaked Ransomware Chats.

This leak was reminiscent of the 2023 Conti ransomware leak in more ways than one. Conti's leak was alleged to be the result of internal disagreements at the onset of the Russia-Ukraine conflict. By comparison, Black Basta is said to have fractured following internal disagreements on the targeting of Russian victims. Given that Black Basta is assessed to have emerged from former Conti team members, it's hard not to view this event as history repeating itself and the group failing to learn from past mistakes.

In January 2025, shortly before the leaks were published, we observed Black Basta's public-facing infrastructure, including their data leak site, unexpectedly going offline. The group has claimed no victims, nor has it shown any signs of activity in the months since. In one of the last messages contained in the leaks, Black Basta members are seen discussing the need to immediately migrate chat platforms.

While the events leading up to, and in the wake of, Black Basta's chat leaks appear to have led to the termination of Black Basta operations in their current form, it is unlikely that the group's members will exit the ransomware ecosystem. We lack sufficient reporting to determine the extent to which the group may have splintered or will attempt to rebrand in the months ahead, though we have high confidence that its component members will continue ransomware operations in some form in 2025. The leadership of Black Basta has shown that they have deep connections to other cybercriminals, including an intimate relationship with the operators of the DarkGate malware as-a-service, and limited reporting indicates that some Black Basta tactics have been observed as associated with a resurgent Cactus RaaS group. Continued increases in the operational tempo of Cactus, as well as further reporting on overlapping tactics, will potentially confirm the realignment of Black Basta affiliates and members in the near term.

Lazarus and the ByBit Hack

On February 21, 2025, hackers with the Lazarus group, allegedly associated with North Korea, executed a massive cryptocurrency heist stealing approximately $1.5 billion in the Ethereum currency (known as ETH). This is not the first crypto heist associated with Lazarus and North Korea, but it is the largest. In this section, we will look at the Lazarus group, how they operate, historic attacks attributed to them, and why North Korea targets cryptocurrency as a major part of its digital operations.

Lazarus History and Operations

Lazarus Group (also known as ZINC, Black Artemis, Labyrinth Chollima, and Diamond Sleet) is an advanced threat actor group with ties to the North Korean regime. The group has been tracked since 2010 and has been responsible for several high-profile attacks, including the recent 2025 ByBit heist, a theft in 2016 of $81 million from Bangladesh's Central Bank, the WannaCry campaign of 2017, and the 2014 Sony Pictures Entertainment attack, among others. Additionally, Lazarus has conducted destructive malware attacks against South Korean targets, including the deployment of wiper malware. Historically, the group has targeted organizations within multiple industries, including defense, healthcare, finance, and entertainment.

Social engineering has traditionally been at the forefront of Lazarus operations with tactics used including spear phishing, drive-by compromises, and other common initial access methods. In the case of the ByBit hack, Lazarus group operators posed as trusted open-source contributors, convincing a SafeWallet developer to install a malicious Docker project. Since Lazarus is considered an advanced threat actor, the reliance on social engineering techniques reinforces the idea that the human element of security is the weakest. Even "advanced" threat actors will use what works because, after all, exploitation of weaknesses is not just for software.

In addition to social engineering, Lazarus has been known to create custom malware designed for their attacks. Most famously, they allegedly created the malware used in the WannaCry attacks in May 2017. The malware used a leaked NSA backdoor known as EternalBlue, which was an exploit in Microsoft's implementation of the Server Message Block (SMB) protocol. In addition, it also used a previously unidentified backdoor known as DoublePulsar. At the time of its release, many computers worldwide were still vulnerable to this attack, although Microsoft had released a patch approximately one month earlier. Other Lazarus malware creations include the KiloAlfa keylogger, IndiaIndia, and the WhiskeyAlfa, WhiskeyBravo, WhiskeyDelta, and Sharpknot wipers.

The Lazarus group is well-established, prolific, well-funded, and extremely capable, with a history of using custom malware exclusive to their operations. As free and open internet does not exist in North Korea, they are motivated by the same directives and goals as the North Korean government; many of Lazarus' victims include financial targets that ease the funding issues caused by global sanctions on the North Korean regime.

Lazarus and the ByBit Hack (Continued)

Targeting Cryptocurrency

According to a UN Security Council report, between 2017 and 2024, the DPRK conducted 58 suspected cyber-attacks on cryptocurrency-related companies, totaling approximately $3 billion. Targeting cryptocurrency allows North Korea to evade United Nations sanctions and generate revenue. Many of the attacks on cryptocurrency-related organizations follow the same tradecraft as other operations, including the use of phishing lures, social engineering, and third-party compromises.

While cryptocurrency services do make an attempt to combat DPRK funding via stolen funds, the very decentralized nature of the exchanges abused by Lazarus (and their ability to pivot quickly between exchanges) allows for a notable amount of agility in later converting cryptocurrency to usable funds.

Use of Ransomware

Lazarus has demonstrated the use of open-source ransomware tools on multiple occasions, and some reporting indicates potential integration with RaaS groups. Additionally, there have been scenarios where Lazarus group actors have cooperated with South Korean insiders to deploy ransomware, in one case affecting more than 700 victims and $2.6 million in funds. The integration of cryptocurrency and ransomware makes the use of ransomware a natural fit for groups like Lazarus. The widespread availability of open-source ransomware tools provides a perfect mask for hiding activity related to the DPRK.

Crypto Regulation and the State of the Cryptomixer Ecosystem

On March 21, 2025, the United States delisted the Tornado Cash cryptomixer from its list of financial sanctions. The Tornado Cash mixer was used by Lazarus to launder over $455 million in crime-related cryptocurrency since 2019. The relaxing of sanctions on Tornado Cash is, in no doubt, partly due to the favorable stance on cryptocurrency taken by the Administration.

On April 7, 2025, the Administration disbanded the Justice Department's National Cryptocurrency Enforcement Unit, which was responsible for leading investigations into North Korean crypto money laundering. How the long-term effects of easing enforcement will play out is yet to be determined, but it is possible that Lazarus (and similar groups) will take advantage of the situation to continue funding DPRK goals with reduced disruptions.

Quarterly Wrap Up

The first quarter of 2025 represents a high-water mark for the ransomware economy, but it is unclear at this point what this fast start may mean for the rest of the year. After being preceded by another standout quarter in Q4 2024, it appears more likely than not that the upcoming quarter may continue the dramatic upward trend. However, several factors point to a potential cooling in the operational tempo of threat actors as we enter the spring and summer months.

For one, based on several years of data, threat actors typically claim the most victims in Q1 and Q4, with noticeable lows in Q2 and Q3. GRIT has observed readily apparent seasonality in activities from threat actors at every level, and we project that 2025 will be no different. This is by no means a guarantee of market retraction in the ransomware space. If Clop's continued use of mass exploitation attacks is any indication, a single operation of considerable size may be enough to skew the numbers again in any given Quarter. It is entirely possible that other threat actors notice the success of Clop's tactics and attempt to emulate them, although there are some headwinds that present challenges to groups trying to walk in their footsteps. Clop's MFT exploitation events are profitable but require substantial planning, resources, and ultimately, luck. Primarily they require that a threat group develop or purchase a "zero day" vulnerability on a well-established internet-facing application. If the Black Basta leaks are any indication, most threat groups would much rather wait for vulnerabilities to be publicly discovered and weaponized rather than navigate the process and price of obtaining a legitimate zero day.

Other speedbumps may prevent the remainder of 2025 from being as profitable for threat actors as Q1. The pace of disruption to prolific and Established ransomware groups, either by law enforcement or from internal strife, continues to increase. While knowledgeable threat actors can always move and rebrand their operations, they must navigate setbacks and infrastructure replacement, which could introduce substantial friction and costs or force undesirable changes to previously successful TTPs. Perhaps the most dramatic change to the pace of ransomware victims could come in the form of disruption to the biggest player in the RaaS space, RansomHub. GRIT has observed early indications of infighting within the group who, like many before them, may inevitably tear itself apart due to the greed of "rogue" internal actors. As evidenced by the fall of LockBit, any amount of distrust injected into an affiliate program is enough to send actors scattering – with far-ranging and significant impact on the group's continued viability and bottom line.

The biggest question we are asking ourselves is whether or not 2025 will be the biggest year for ransomware to date. While it is possible that we continue to see year-over-year growth in the space, one would hope that the numbers cannot keep going up forever. There are indications from several outlets that, while the pure number of attacks is up, payments to actors have been trending downward. It stands to reason that if this continues, we may see some actors adjust their tactics or even get out of the ransomware game in general if opportunities become outweighed by risks.

Overall, Q1 2025 demonstrated that we have all of the ingredients for another year of record ransomware attacks - but it is up to the defenders to impede these efforts and hopefully reverse the upward trend.