



# Ransomware and Cyber Threat Insights

A GRIT® Report

Q2 2025  
April-June 2025

# Contents



Methodology



Quarterly Ransomware Summary



Threat Actor Trends



Threat Actor Spotlight – DragonForce



Industry Spotlight – Manufacturing



Other Reporting and Events



Quarterly Wrap Up





# 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 are 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 the 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", compromised data brokers and markets, or non-financially motivated data thieves and leakers. While these actors and venues no doubt have impact, 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 second quarter of 2025 granted a slight reprieve from ransomware victim volumes that had increased seemingly nonstop over the past year. GRIT observed a 22.9% decrease in observed victims claimed via ransomware data leak sites and blogs, reflecting the largest reduction in attacks quarter-over-quarter (QoQ) since GRIT began tracking ransomware operations. We generally see the start of a "summer slump" or stagnation of claimed victims during the second quarter, but the dramatic decrease in victims that we observed this year notably exceeds baseline by 10-15%. Despite the relief, we still observed 43.3% increase in publicly claimed victims year-over-year (YoY), which coincides with a 44.9% increase in active threat groups from that same timeframe. Although many of these active threat groups are newer, Emerging and Developing groups are not performing at the level of prolific, Established groups. The sheer number of active groups remains a primary driver of victim volume over time. We'll explore their impact on the ransomware "market" further in this report.

The ransomware ecosystem continues to normalize despite the departures of old and new "leaders," including LockBit and AlphV in 2024 and, more recently, RansomHub in 2025. In their stead, longstanding but previously "second tier" RaaS groups, including Qilin, Akira, and Play, have become the most benefitting from the absorption of experienced displaced affiliates. This growth has not been without growing pains; however, although these groups have claimed victims on par with former leaders in the space, Qilin and Akira have encountered repeated issues with hosting the associated high volume of victim data on their data leak sites.

International law enforcement continued to build upon their successes from preceding quarters, with several darknet marketplaces facing their demise, and the arrests of prominent operators of the infamous BreachForums. Law Enforcement's increasingly visible efforts to indict and arrest the operators behind illicit operations remains a rare "stick" available to counter the narrative of cybercrime as a low-risk, high-reward endeavor.

In sum, Q2 of 2025 shows several positive indications of improvement or progress in the fight against ransomware and cybercrime more broadly – we love to see it. Whether these improvements persist over the long term, or whether Q3 will represent a return to baseline, remains to be seen. In this quarter's report, we'll review some of the key events and drivers behind the changes we're seeing – and whether we assess them to be outliers or representative of long-term shifts.

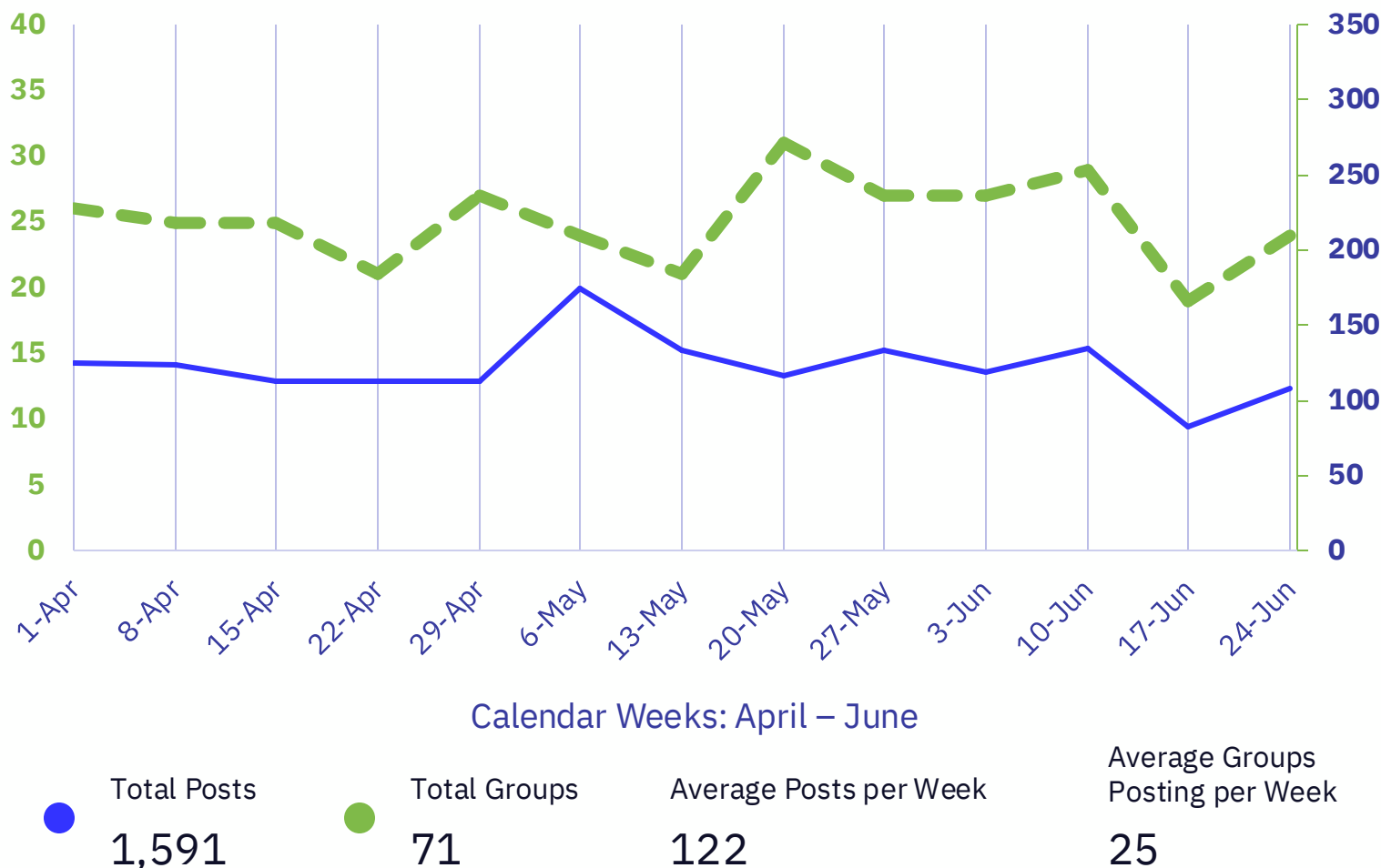
	Q2 2025	Q1 2025	Q2 2024
Total Publicly Posted Ransomware Victims	1,591	2,063	1,110
Active Ransomware Groups	71	69	49
Average Daily Victims	17.5	22.9	12.2





# Threat Actor Trends

# Rate of Publicly Posted Ransomware Victims, Q2 2025



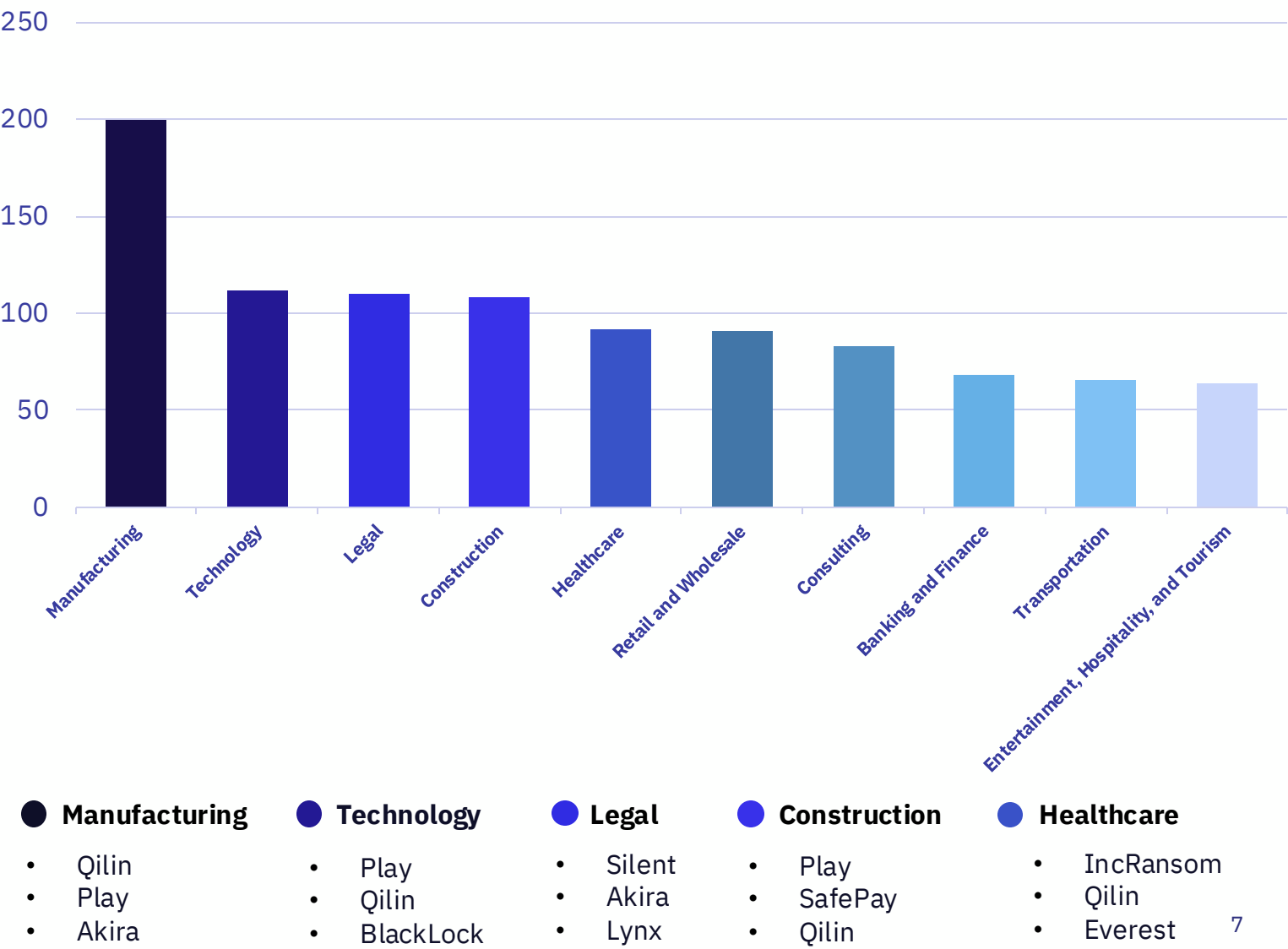
Q2 2025 saw a mostly consistent rate of victim posts throughout the quarter, with a slight decline in ransomware activity towards the end of June. This deflation seems to have been caused in part by both Akira and Play decreasing their activity during this window, claiming only one and five victims during the week of June 17th, respectively. This observation reflects the extent to which the most prolific ransomware groups continue to drive the bulk of observed ransomware victims.

Even though Q2 contained one more unique threat group than Q1, in which we observed 70 active groups, posting rates appeared to have declined overall throughout this quarter, with 122 posts per week compared to the 156 average posts per week in the previous quarter. This is likely impacted by the Q1 posts of Clop – known for their mass exploitation of vulnerabilities and data extortion – which accounted for 348 victims, or 27 posts per week in Q1. When adjusted for these victims, the difference in weekly volume – 122 in Q2 vs. 129 in Q1 – is much less stark.

# Most Impacted Industries, Q2 2025

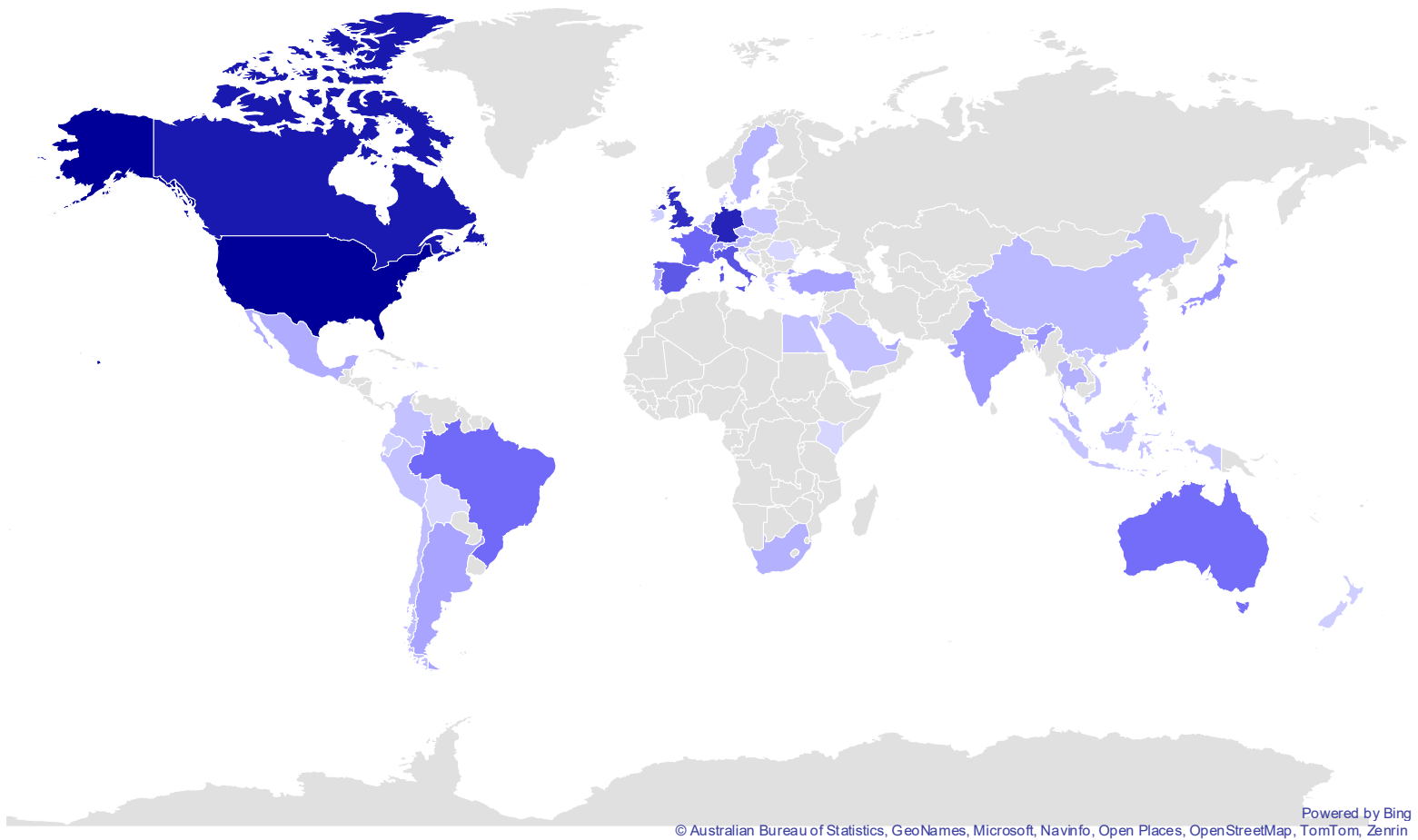
The manufacturing industry remains the most impacted industry among verticals in Q2. We explore this industry and the effect ransomware has had upon it later in this report. The entertainment, hospitality, and tourism sectors saw increased attacks throughout Q2, bringing them into the “top 10” most impacted verticals for the first time since Q3 2023. Q2 brought 27 unique threat groups all attacking at least one victim that was categorized in entertainment, hospitality, and tourism sector, with Play claiming the highest concentration of 10 victims.

Healthcare saw diminished attacks throughout Q2 2025, falling from the “top 5” most impacted industry for the first time since Q2 2022. This may reflect targeting and attack preferences or internal rules of the newly leading threat groups; in particular, affiliates of Akira, the second-most-active group this quarter, have only been observed to have claimed 11 healthcare victims since the group's emergence, out of over 700 total victims.





# Geographic Breakdown of Ransomware Victims, Q2 2025



## Top 10:

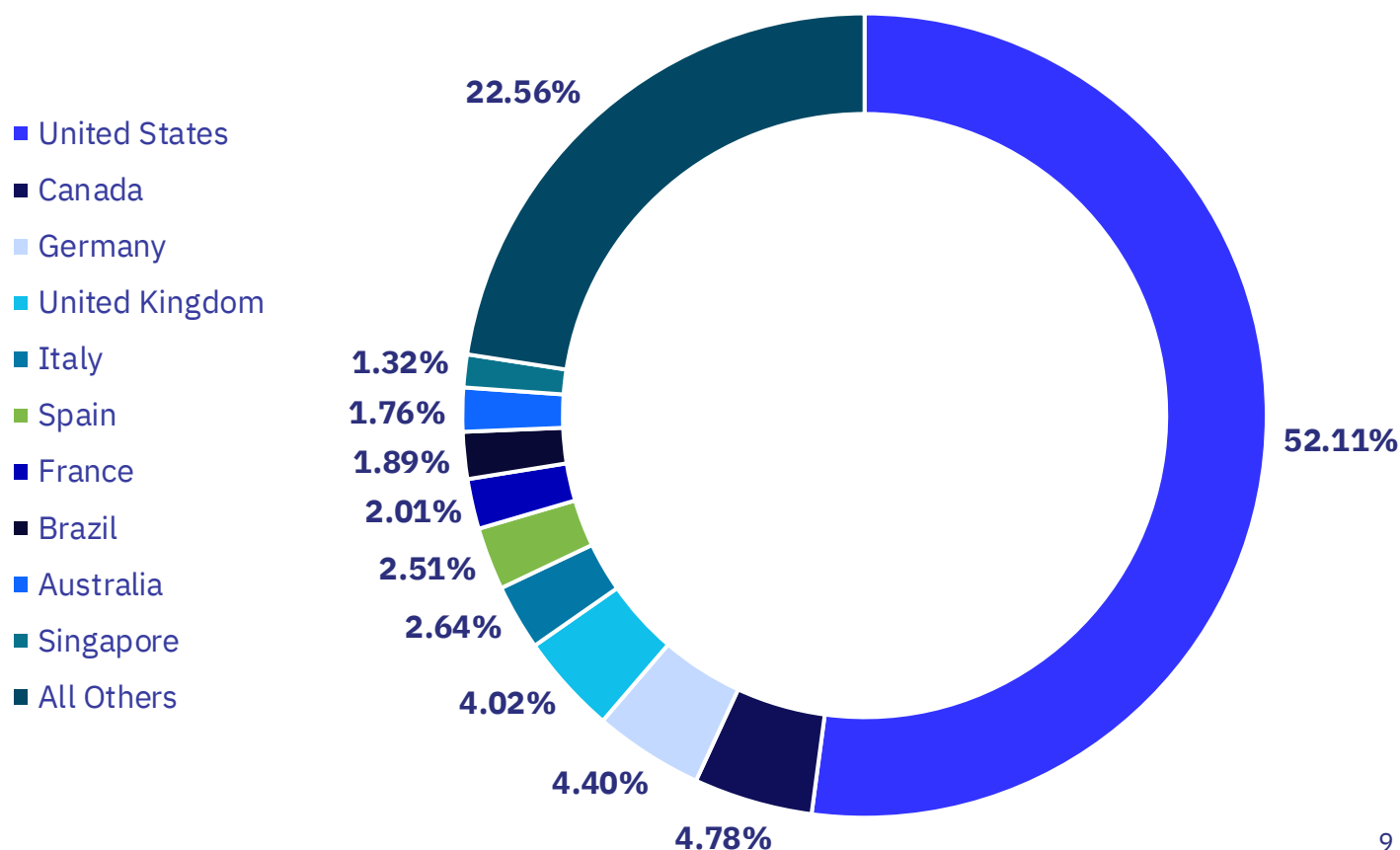
- |                   |               |
|-------------------|---------------|
| 1. United States  | 6. Spain      |
| 2. Canada         | 7. France     |
| 3. Germany        | 8. Brazil     |
| 4. United Kingdom | 9. Australia  |
| 5. Italy          | 10. Singapore |



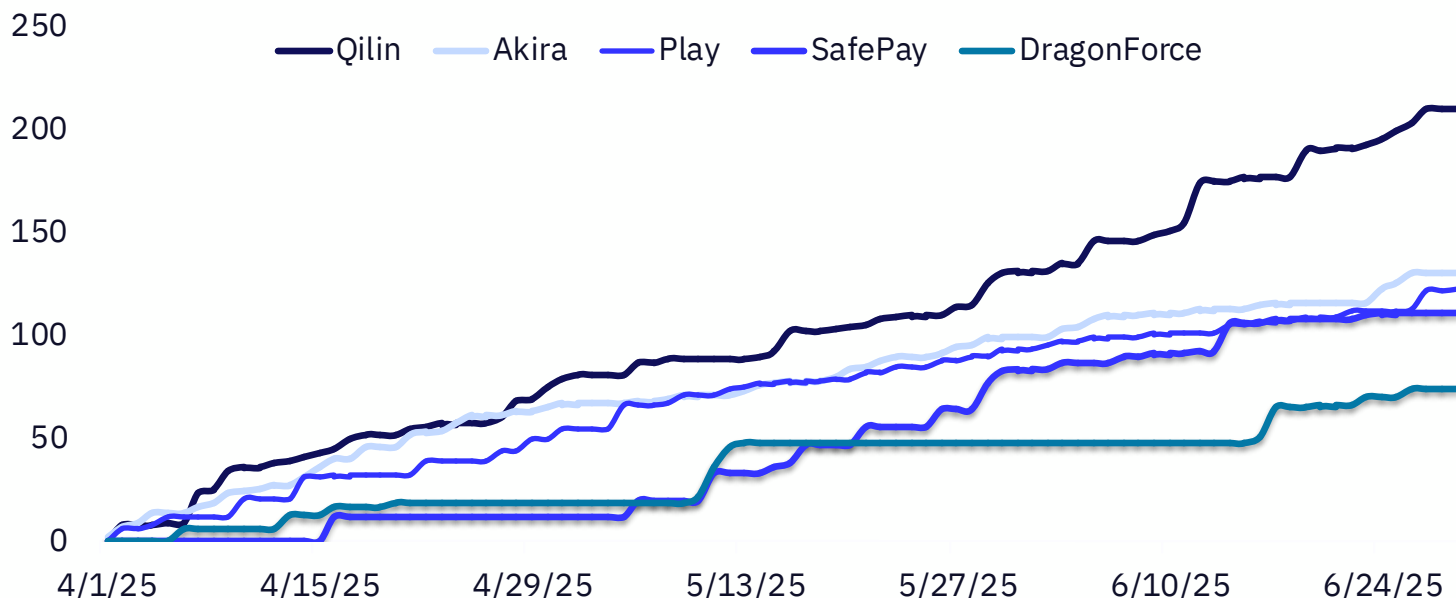
# Ransomware Impacts by Country, Q2 2025

Ransomware's geographic impacts have remained relatively consistent over the last two years. The United States remains by far the most impacted, accounting for ~50% of observed attacks. Canada, Germany, and the United Kingdom remain as secondary targets, frequently shifting positions along with other western European nations among the "top 10." With a high population, diverse economy, and no prohibition on ransom payments, the US almost certainly presents a target-rich environment for opportunistic threat actors. Western European victims likely present as attractive for similar and overlapping reasons.

Notably, we observed more claimed victims in Singapore this quarter than in any preceding quarter since GRIT began tracking ransomware activity, with 21 observed Singaporean victims. This marks two consecutive quarters in which Singaporean organizations experienced a significant uptick in observed attacks, which had previously accounted for only a handful per quarter. This observation is in keeping with our assessments that ransomware groups have increasingly impacted victims in the Indo-Pacific region, including India, Australia, Vietnam, and even China. Qilin accounted for the plurality of observed attacks on Singaporean victims, accounting for 6 of the 21 attacks.



# Cumulative Victims by Threat Group



## Qilin

This quarter, Qilin became the most active threat group by victim volume for the first time since their emergence in 2022. The longstanding outfit drastically increased their operational tempo at the start of 2025 and has continued this same increased pace throughout Q2. It is impressive that the group has been able to maintain operations for almost three years, which is no small feat in the ransomware ecosystem. This established track record could be one reason why it is seeing more activity. The group has built a longstanding "brand," which likely increases trust amidst displaced affiliates of other RaaS operations seeking a second or new home.

## Akira

Mirroring Qilin, Akira has also seen increased activity since the start of the year, but Akira failed to keep up their pace from Q1, in which they claimed a staggering 213 victims. At 133 victims in Q2, Akira is still a prolific threat, and current pacing reflects Akira's graduation from a former "middle class" participant in the ransomware ecosystem to one of the most prolific Established groups active today. The group benefits from its targeting of and impacts on ESXi servers, increasing the available attack surface in enterprise environments.

## Play

Play actors similarly appear to be seeing increased operations due to the power vacuum left after RansomHub's apparent departure from the ransomware scene. We note this as an intelligence question that remains partially unanswered, as conflicting reporting exists as to whether Play functions as an insular or RaaS organization. Play observed a 41% QoQ increase in claimed victims to their data leak site from Q1 2025 to Q2.

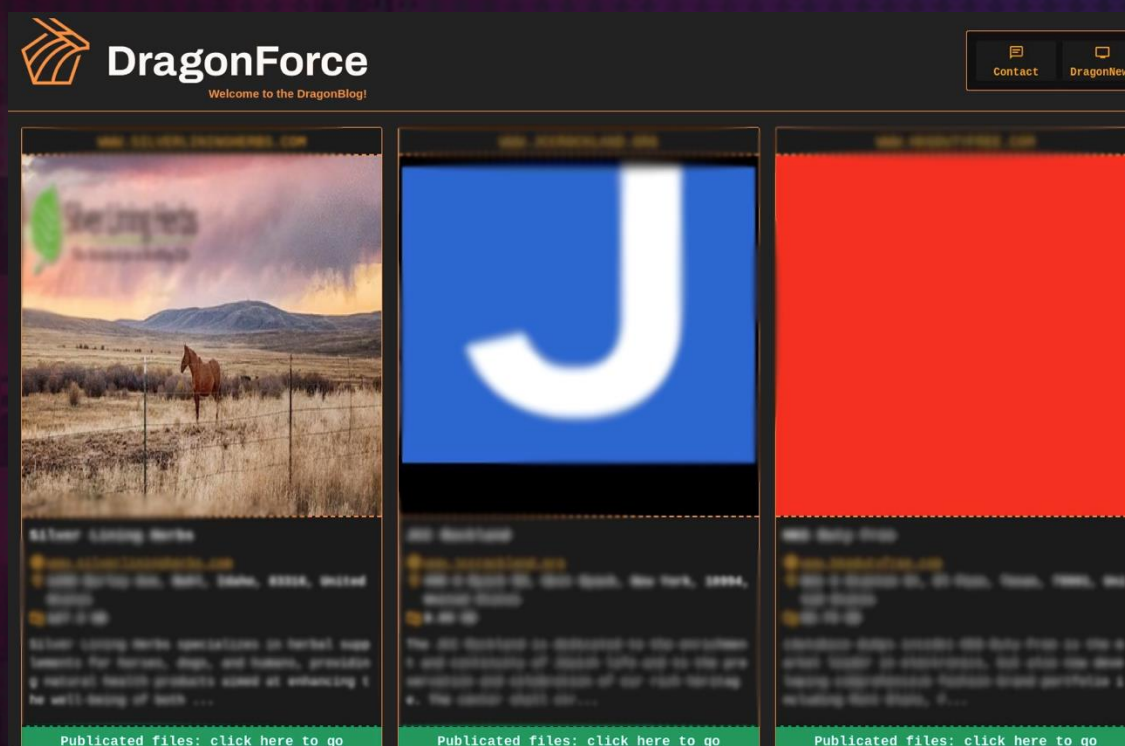




# Threat Actor Spotlight – DragonForce

# Threat Actor Spotlight – DragonForce

DragonForce first gained international attention in late 2023, following an attack on the Ohio Lottery Commission, marking its emergence as a group willing to engage in double extortion. The group's initial payloads bore striking similarities to the LockBit. Ostensibly leveraging this code base, the group's affiliates gained the ability to reach a wide array of enterprise environments.

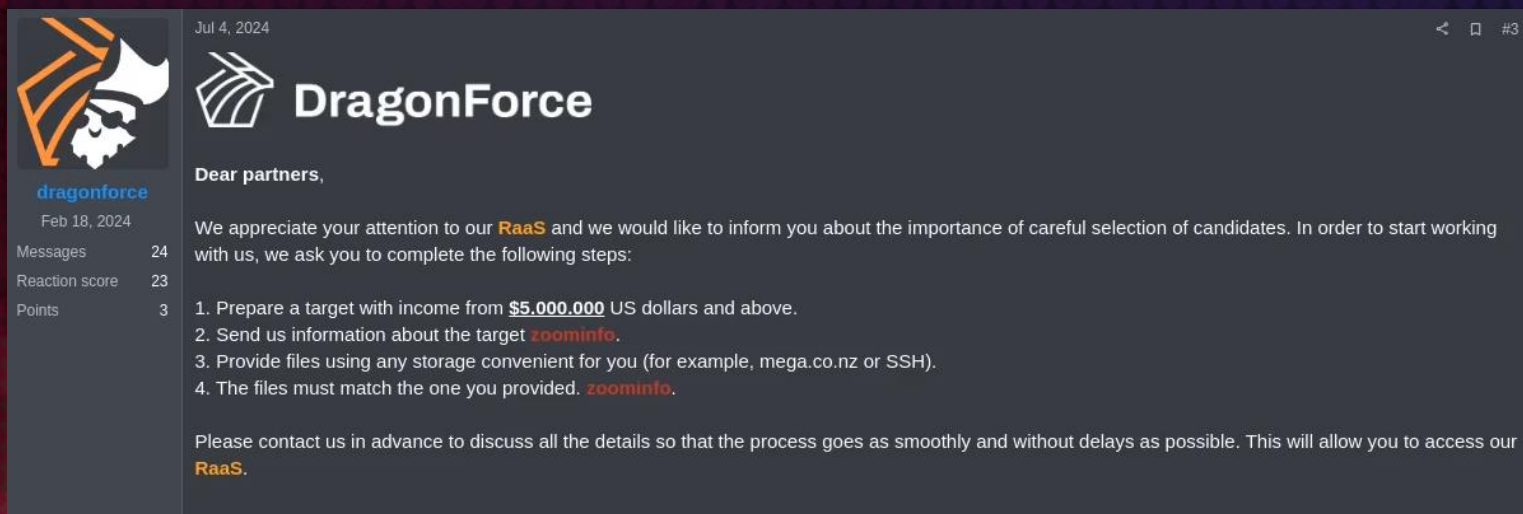


*DragonForce's data leak site showcasing victims and access to "published files."*

DragonForce's threat profile expanded significantly in 2024, both geographically and operationally. The group has claimed over 120 victims globally on its Data Leak Site (DLS), with confirmed victims in the US, Italy, Australia, and the UK. A notable spike in victim posts occurred in June 2024, when the group listed 20 new victims in a single month. These numbers, while not as prolific as the operations of BlackCat or LockBit at their height, indicate a growing operational tempo and impacts across a broad swath of industries. In one known case, the group demanded \$7 million from a single organization, suggesting the group may be pursuing a "big game hunting" approach to victim selection.



# Threat Actor Spotlight – DragonForce



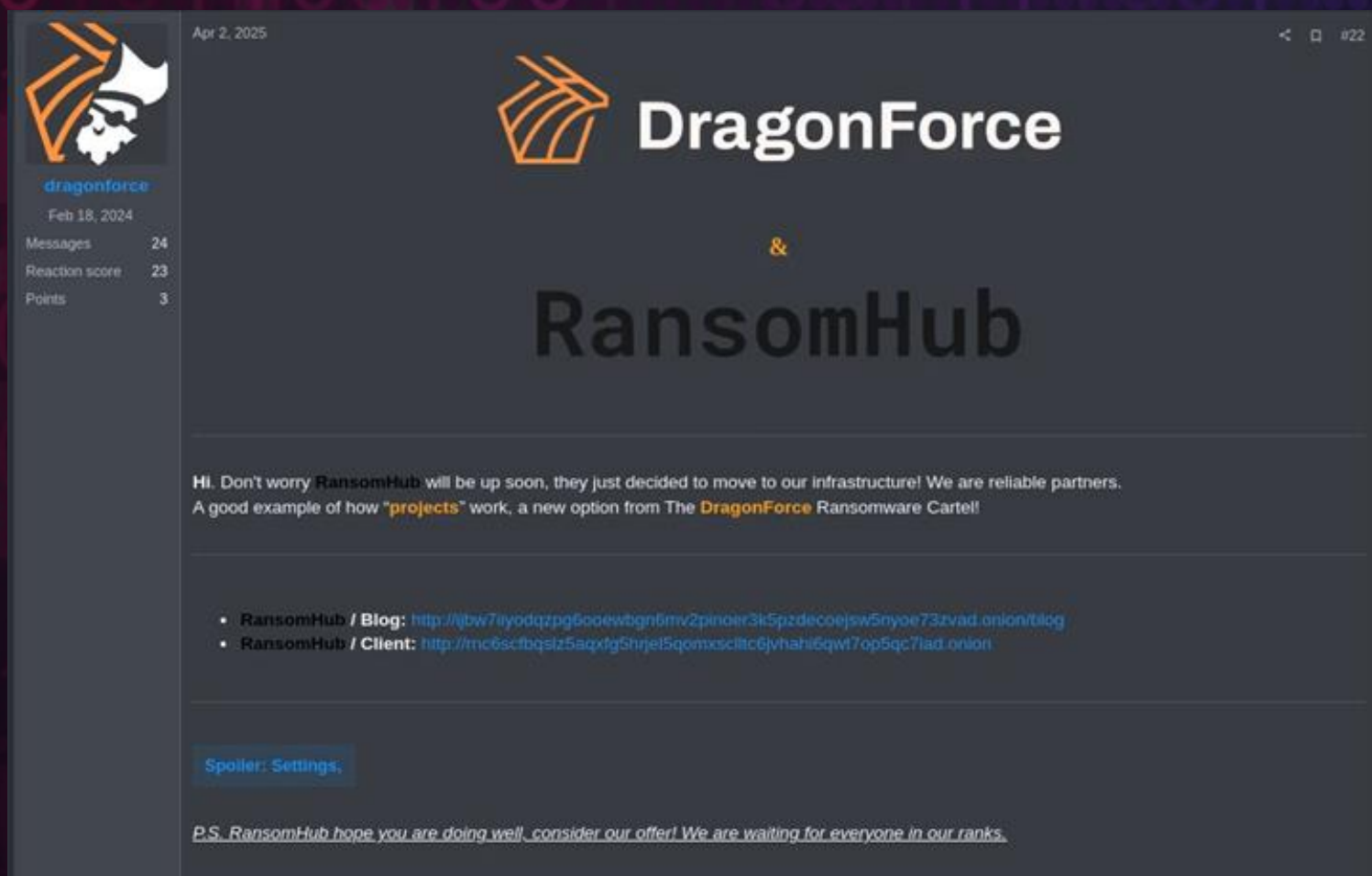
*DragonForce post on the illicit forum RAMP stating that affiliates must target entities with a revenue above \$5 million USD.*

While many ransomware groups operate quietly and seek to avoid unnecessary attention, DragonForce has been overt in its attempts to build influence within the cybercrime community. The group transitioned from traditional RaaS to a self-described “cartel” model in early March 2025, which allows for “partners” to maintain their own name and branding while working with DragonForce. At that time, DragonForce unveiled a revamped data leak site and a partner-based ransomware infrastructure offering affiliates up to 80% of ransom profits.

Their affiliate “cartel” model is advertised to potential affiliates as including not only malicious payload delivery and encryption tooling, but also administrative panels for managing “partner” blogs, exfiltrated file storage, 24/7 infrastructure monitoring for “partner” blogs, and even “client-facing support systems/client panels”.

# Threat Actor Spotlight – DragonForce

DragonForce's offerings rival those of legacy RaaS programs such as RansomHub and LockBit, but with a uniquely aggressive recruitment and control strategy, such as their defacement of the DLS and supplemental recruitment attempts of BlackLock and Mamona/El-Dorado affiliates. Additionally, in April, DragonForce capitalized on an opportunity presented by internal discord in RansomHub's RaaS community to appeal to new affiliates. Following RansomHub's sudden disappearance from the dark web in March 2025, DragonForce posted onion links on both their site and RAMP that linked to a rebranded RansomHub infrastructure under DragonForce control. The linked site displayed the message, "RansomHub will be up soon, they just decided to move to our infrastructure" implying a takeover of RansomHub infrastructure by DragonForce.



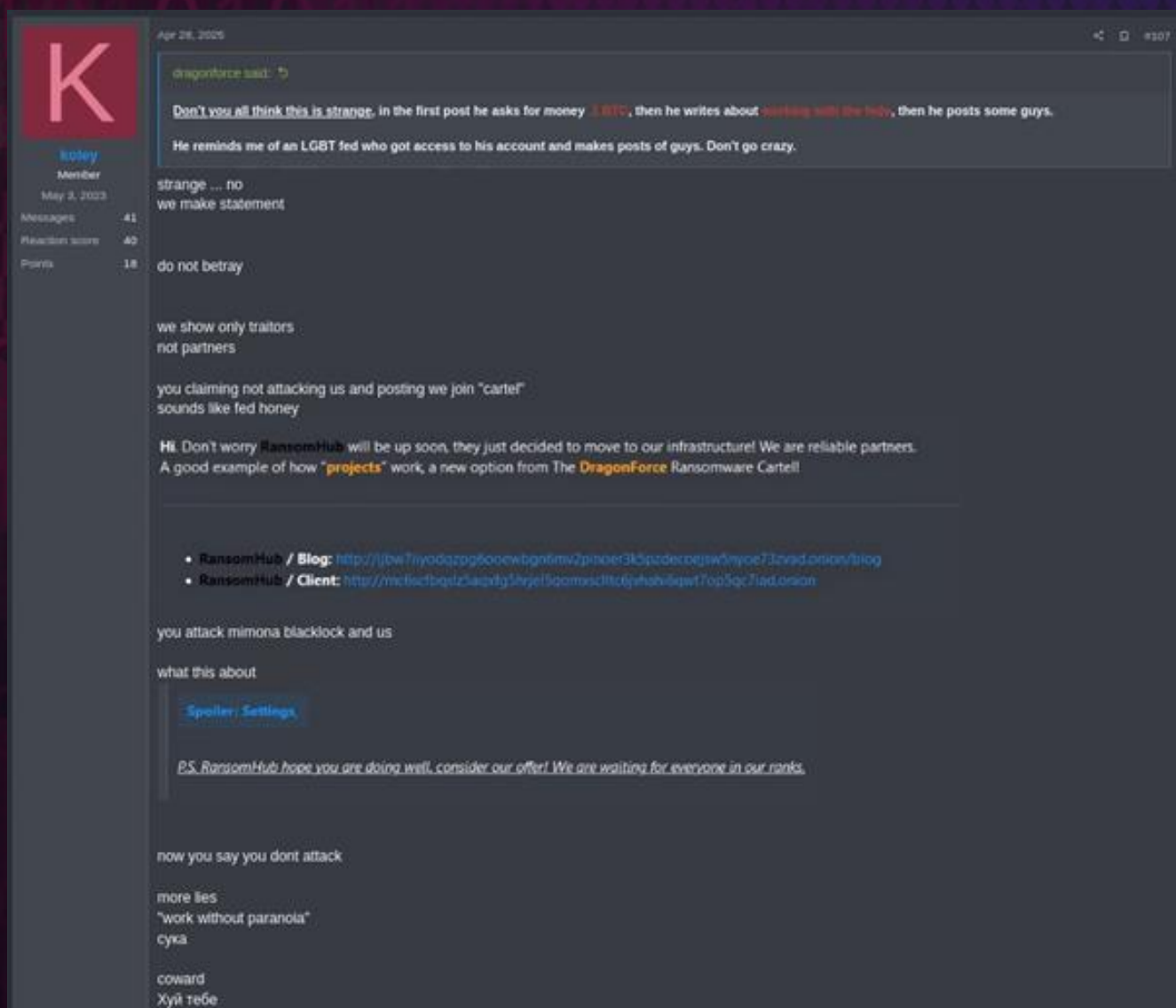
The screenshot shows a Discord chat window. On the left is a sidebar with the user's profile: a custom avatar of a dragon's head, the name 'dragonforce', and a timestamp 'Feb 18, 2024'. Below the profile are statistics: 'Messages 24', 'Reaction score 23', and 'Points 3'. The main chat area has a dark background. At the top, it says 'Apr 2, 2025' and '#22'. The header features the DragonForce logo (an orange dragon head) and the text 'DragonForce & RansomHub'. The message body reads: 'Hi. Don't worry RansomHub will be up soon, they just decided to move to our infrastructure! We are reliable partners. A good example of how "projects" work, a new option from The DragonForce Ransomware Cartel!'. Below this is a bulleted list: '• RansomHub / Blog: <http://qbw7iypdqzpg6ooewbgn6mv2pinoer3k5pzdecoejsw5nyoe73zvad.onion/tlog>' and '• RansomHub / Client: <http://mc6scfbqslz5aqxigShrjeI5qomxscIltc6jvnhai6qwl7op5qc7lad.onion>'. At the bottom, there is a 'Spoiler: Settings,' button and a footer message: 'P.S. RansomHub hope you are doing well, consider our offer! We are waiting for everyone in our ranks.'

*DragonForce's initial "offer" to RansomHub, framed as a "takeover" announcement by DragonForce.*



# Threat Actor Spotlight – DragonForce

However, shortly afterward the announcement, DragonForce publicly clarified that this was not a consensual merger, but rather an invitation which had been rebuffed by the troubled RansomHub. RansomHub spokesperson "koley" later accused DragonForce of orchestrating the attack that took them offline via posts to RAMP forums, citing timing, infrastructure similarities, and alleged FSB connections as proof of the *fait accompli*.



*A RansomHub spokesperson "koley" blames DragonForce for the attack against them and the reason that they are currently offline.*

# Threat Actor Spotlight – DragonForce

Having utilized several RaaS strains in the past, including RansomHub and Qilin, the Scattered Spider threat group is likely now using DragonForce as a source to publish victims who do not comply with Scattered Spider's ransom demands. In early 2025, multiple UK-based retail organizations were shared on DragonForce's dark web blog. Reporting indicates that tactics attributed to Scattered Spider were used during these intrusions, including posing as internal IT support staff to gain initial access. As discussed, DragonForce's operators remain vocal on the dark web forum RAMP, predominately writing posts in the English language. Scattered Spider's members are assessed to be young English-speaking males, so the lack of potential language barriers with DragonForce could have attracted Scattered Spider to their affiliate program.

The group's aggressive efforts to dominate the RaaS market through both recruitment and sabotage mirror behaviors seen in previous power struggles among cybercriminal organizations, such as the LockBit-BlackCat rivalry and RansomHub's recruitment strategy after the LockBit takedown. Additionally, DragonForce adheres to a strict and explicit policy of avoiding critical infrastructure and former Soviet states, which suggests a deliberate effort to adhere to Russia-friendly operational boundaries.

Strategically, DragonForce's influence lies not just in victim count, but in the attempts at ransomware ecosystem manipulation. By offering infrastructure-as-a-service, DragonForce likely hopes to shape the operational landscape of lesser-known threat groups and even terminate services for those who oppose its directives. This centralized control model represents a consolidation of capabilities uncommon even among mature RaaS programs. The group has also adopted Graphics Processing Unit (GPU) assisted improvements following the exposure of Akira's decryption process in early 2025, indicating iterative improvements to the group's Linux and ESXi payloads.

DragonForce's rise coincides with a broader collapse of legacy Russian ransomware infrastructure. In addition to RansomHub's dissolution, BlackLock and Mamona Ransomware suffered a compromise in February 2025, wherein their DLS was defaced by DragonForce after being breached by a cybersecurity research firm. Though attribution remains unclear for the RansomHub problems, some personas commenting in cybercrime forums have speculated that DragonForce or its affiliates may have played a role, citing timing and strategic gain as well as contacts within the Russian government.





# Industry Spotlight – Manufacturing



# Industry Spotlight – Manufacturing

Manufacturing remains – unsurprisingly – the most heavily targeted industry in Q2 2025, with a continued string of ransomware incidents impacting operations, supply chains, and networks of manufacturing organizations across the globe. In Q2 2025, the manufacturing industry accounted for 200, or 12.6%, of the 1,591 victims we observed. This is the second highest volume of manufacturing victims we have recorded in a quarter, surpassed only by Q1 of 2025. These figures also reflect a 43.9% increase year-over-year (YoY) relative to the 139 manufacturing victims we observed in Q2 of 2024. While ransomware groups continue to evolve in their tools and tactics, their outsized impact on the manufacturing industry is likely rooted in two constants: high operational pressure and persistent vulnerabilities in IT networks.

While the drivers behind this sustained targeting may not necessarily be new, they remain relatively unresolved for many manufacturing firms. Many manufacturing environments still run legacy OT systems such as PLCs, SCADA servers, and HMIs that were generally designed for safety and uptime, not security. These systems are often decades old, built without basic protections like encryption, authentication, or access controls, and are difficult or impossible to patch without risking production downtime. This alone places them at a disadvantage. But the problem is compounded by the way many of these systems are integrated into flat networks, connected to the corporate IT environment via unsecured remote access tools or exposed services. It is not uncommon to see outdated Windows boxes with Remote Desktop Protocol (RDP) open to the internet, or Virtual Private Network (VPN) appliances with weak credentials acting as a bridge into the plant floor. Many threat actors know of this, and they continue to exploit it time and time again.

Like many other industries, human vulnerability is certainly another factor in the genesis of these attacks. While much focus is placed on exploiting system weaknesses, ransomware groups are increasingly turning to social engineering and manipulation of IT support channels to gain initial access. In multiple intrusions over the past two quarters, adversaries have used AI-generated voice phishing (vishing) and deepfake voice calls to impersonate employees and pressure IT staff into resetting MFA or credentials. In one observed case from late April, a threat actor impersonated a plant manager and convinced support to reset access to an industrial design repository, leading to both data exfiltration and eventual ransomware deployment. This trend represents a continuation of effective and evolving social engineering techniques while combining with traditional access pathways like RDP and remote monitoring tools.



# Industry Spotlight – Manufacturing

Ransomware groups such as Qilin, Play, Akira, and newer entrants such as Lynx and Safepay, have all impacted manufacturing organizations worldwide throughout Q2 2025. These actors likely understand that not only is the cost of downtime steep, but disruption to a production line does not just impact one company; it cascades through suppliers, distributors, and end customers. As a result, ransomware operators may perceive manufacturing victims as more likely to pay quickly to restore operations.

The manufacturing sector experienced several notable breaches this quarter. Lynx claimed responsibility for a notable double-extortion attack against R & M Manufacturing in late April, exfiltrating sensitive data before launching encryption across the enterprise. Nucor, one of North America's largest steel producers, was forced to shut down systems at multiple plants. Other incidents involving firms in Japan, Germany, and the US suggest that industrial ransomware is not only ongoing but also global and largely indiscriminate.

Q2 2025 has reinforced that manufacturing is not just a critical industry, but often a vulnerable one and a hot target for adversaries. Unfortunately, until more defenses are put in place and awareness in the industry spreads, ransomware actors will continue to exploit the gap in the manufacturing industry in the days ahead.



## Other Reporting and Events



# Law Enforcement Successes

Q2 2025 boasted a diverse and effective set of law enforcement activities aiming to disrupt various cybercrime actors and groups. These actions continue the uptick in publicly observable law enforcement operations targeting not only bad actors, but also their supporting infrastructure leveraged as a part of the cybercrime ecosystem. While it may not be possible or practical to arrest every cybercriminal in the world, these activities do introduce friction into daily cybercrime operations. This quarter, we have broken down the affected cybercrime groups into three pillars: dark web drug markets, hacker forums, and infostealers.

## **Dramatic Drug Market Disruptions**

In Q2, several major dark web drug marketplaces were significantly disrupted in law enforcement operations. First, on May 22, an international task force announced the success of Operation RapTor. Coordinated by Europol and arguably the largest law enforcement action against these dark web drug markets, police around the world arrested 270 individuals from 10 countries who are suspected of participating in the online drug trade. The main focus of this operation was deanonymization of drug vendors across multiple previously seized marketplaces including Incognito, Nemesis, Bohemia, and Kingdom Market. Using evidence gathered from previous seizures, along with blockchain analysis, more than 270 of the world's largest online drug distributors were identified and arrested. Much like ransomware, drug-based cybercrime is based on a level of trust between the purveyors and their customers. Large vendors are the backbone of the online drug marketplace and often go to great lengths to build and market their "brand," hoping to build a consistent customer base that persists in between markets which are often ephemeral in nature.



# Law Enforcement Successes

Less than a month later, international law enforcement agencies announced another victory, the seizure of Archetyp market and the arrest of its alleged administrator under Operation DeepSentinel. Before the June 11 seizure, Archetyp was arguably the largest dark web drug market in active operation. Archetyp was created in 2020 and outlived many of its predecessors, boasting thousands of vendors and hundreds of thousands of potential customers. The alleged administrator of this site, a German national using the monicker “ASNT,” was arrested in Barcelona, where law enforcement also seized millions of dollars in cryptocurrency and luxury goods. Notably, law enforcement did not immediately announce this operation. After the Archetyp market infrastructure was seized on June 11, its onion site was inaccessible without any announcement from its administrator, alarming vendors and customers alike. The next day, on the dark web forum Dread, a PGP-signed post explaining the sites unavailability appeared from ASNT. The post claimed that Archetyp’s administrator had not been arrested by law enforcement but had been performing maintenance on the market before identifying problems that required troubleshooting. The message concluded with a request that concerned parties not bother the administrator while they are working on the issues, encouraging users to go outside and “touch some grass.” Due to the timeline of the seizure, we now know that this post was made by law enforcement in possession of the Archetyp admin’s private key. After the operation was publicly announced, law enforcement disclosed the deception on June 16 through another post to Dread.

## **BreachForums Baddies Burned**

On June 25, French law enforcement announced the arrest of four operators from the embattled dark web cybercrime forum, BreachForums. The operators, known by the monickers ShinyHunters, Hollow, Noct, and Depressed, helped revive the market in the wake of a 2023 law enforcement seizure of the market and arrest of Pompompurin, its original administrator. Law enforcement also revealed that another individual associated with BreachForums management, known as IntelBroker, had been arrested in February. Together, these individuals have been responsible for or facilitated a significant number of high-profile breaches. Most notably, IntelBroker conducted the PowerSchool breach which affected schools and students across the United States and the SnowFlake data theft attacks that affected TicketMaster, AT&T and other organizations.



# Law Enforcement Successes

In both iterations, BreachForums has acted as a pseudo-marketplace where threat actors have bought, sold, and traded stolen data and illicit access to interested buyers. In some cases where threat actors could not find interested buyers, the actors opted to publicly leak the stolen data on the platform. Some smaller ransomware groups without traditional leak sites have threatened to leak data directly onto BreachForums. The disruption of BreachForums and the arrest of its key members removes yet another central gathering place for cyber criminals, which may curtail or impair such activity going forward.

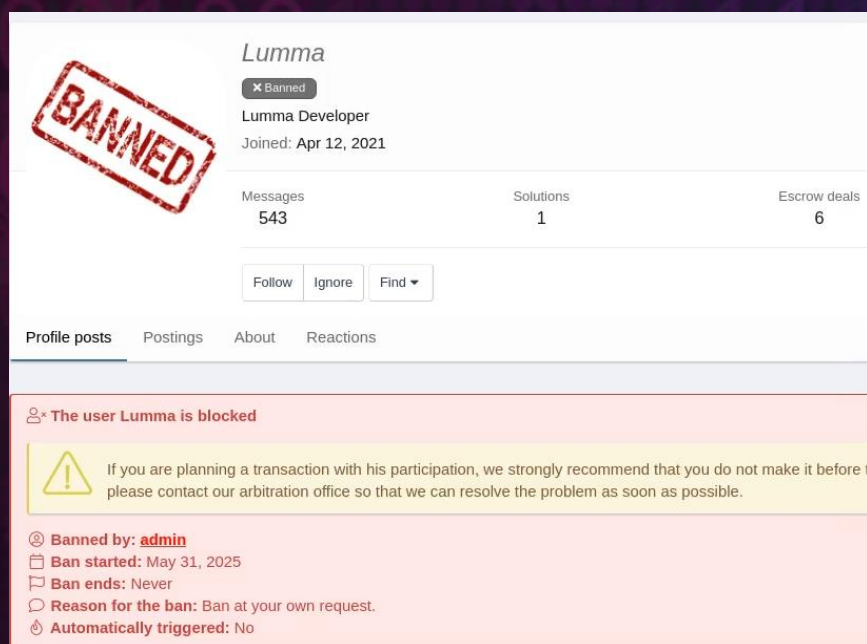
## **Lumma on Life Support**

On May 21, the US Department of Justice (DOJ) announced it had seized infrastructure used to support the Lumma Stealer infostealer malware. To the same end, Microsoft's Digital Crimes Unit aided law enforcement in the identification, takedown, and suspension of over 2,300 Lumma Stealer domains, sinkholing many domains to ensure TA Command and Control (C2) servers could no longer communicate with infected machines. This latest infostealer disruption comes on the heels of October 2024's takedown of both RedLine and META infostealers, previously among the most prevalent in the infostealer malware ecosystem. Consequently, and demonstrating the abundance of alternate options for cybercriminals, Lumma Stealer had risen in popularity among cyber criminals following Redline and META's takedowns. Based on the volume of credentials for posted for sale on the popular illicit marketplace Russian Market, which are attributed to specific stealer brands, it became the most widely used infostealer malware from the October 2024 takedowns until the May 2025 dealt Lumma a similar fate.



# Law Enforcement Successes

The US DOJ reported that Lumma Stealer operators subsequently attempted to rebuild their operations after the seizures, before the government quickly detected and stopped their efforts. Law enforcement's swift interference may have caused the actors to willingly reduce their operations. Historically, Lumma Stealer has utilized the cybercrime forum XSS to conduct advertising and customer outreach, namely behind the group's spokesperson who acted under the moniker "Lumma." The user has since been banned on the forum "at [their] own request," suggesting that they are no longer engaging with potential customers under the moniker. The "Lumma" spokesperson was responsible for driving prospective users to purchase the stealer with advertisements and customer support, but this activity has seemingly ceased.



*Lumma's profile page on the illicit forum XSS.*

Law enforcement's successful performance now begs the question, what's next for Lumma Stealer? No arrests or indictments were disclosed in the DOJ's announcement of the seizure, meaning that the actors behind Lumma are currently still free to plan their next illicit business venture. In the absence of arrests or indictments of its facilitators, it is possible that the Lumma Stealer team could simply rebrand and create a new operation offering information stealing malware under a new brand. Some remnants of Lumma Stealer also remain unaffected, as their Telegram sales coordinator @lummaseller128 remains active and responding to customer inquiries. Even if the group continues to progress along at a diminished capacity, the reputational damage caused by the disruption will impact the group's "bottom line" for the foreseeable future.



# Tornado Cash Whirlwind

## **Tornado Cash Delisted from OFAC Sanctions**

On March 21, 2025, the United States Department of the Treasury's Office of Foreign Assets Control (OFAC) lifted economic sanctions against the decentralized cryptocurrency mixer, Tornado Cash. Tornado Cash was originally sanctioned by the Biden administration in 2022 as a direct result of the mixer's use for money laundering by the North Korean Lazarus Group. Shortly after sanctions were implemented, they were challenged in court by a group of plaintiffs in *Van Loon v. Treasury*, in which the district court sided with the government and upheld the sanctions. In November 2024, the US 5th Circuit Court reversed the district court's ruling, finding that OFAC had overstepped its authority. The Trump Administration did not appeal the court's ruling and instead chose to lift the sanctions, citing "novel legal and policy issues" while acknowledging the use of the exchange by North Korean threat actors and committing to continuing efforts to combat DPRK use of cryptocurrency exchanges. The lifting of sanctions likely reflects the current administration's more favorable view of cryptocurrency and its current "light-touch" approach to regulation in the space.

## **DPRK IT Worker Scams Disrupted**

As we discussed in our Q1 Ransomware Report, North Korean (DPRK) cyber operations heavily focuses on cryptocurrency theft and accumulation as a means to fund its weapons development programs and support the Kim regime. One of the DPRK's alternative efforts to gain cryptocurrency has come in the form of converted wages from North Koreans hired unwittingly by worldwide organizations to fill IT, AI, Software Development, and other tech roles. On June 30, 2025, the State of Georgia unveiled indictments against DPRK operatives accused of stealing cryptocurrency from their employers after concealing their identities to become remote IT employees. In the indictment, the State of Georgia outlines the operations the DPRK operatives undertook, including the alleged theft of nearly one million dollars in cryptocurrency and laundering it via a cryptocurrency mixer. While the mixer is not named specifically, DPRK operations have historically used mixers including Tornado Cash to laundry stolen cryptocurrency.



# Tornado Cash Whirlwind

## Forward Looking Assessment

The permissive regulatory stance of the current US administration towards the cryptocurrency industry will almost certainly reduce the likelihood of meaningful cryptocurrency regulations over the next four years. Law enforcement efforts to disrupt adversarial cyber operations which target cryptocurrency and associated infrastructure, however, are likely to continue. As mentioned earlier in the report, the disruption of BreachForums, the arrest of ShinyHunters and IntelBroker, as well as the sanctioning of Aeza, have had an observed effect on disrupting criminal activity. Nonetheless, it remains to be seen whether these efforts will have a lasting effect, or if the adage of cutting off one head of the hydra allows two more to pop up, remains true with regard to cybercriminal activity.

## Unknown Groups & RaaS Reputation

### Noteworthy Newcomers

Thus far in 2025, we continue to observe an increasing number of named ransomware groups. From Q2 2024, in which we observed 45 active ransomware groups, to Q2 2025, in which we observed 71 active ransomware groups, we note a 44.9% YoY increase by volume. When looking QoQ, the 69 active ransomware groups in Q1 2025 reflects a less pronounced but still increasing 2.9% growth.

In narrowing the aperture to focus only on new and Emerging groups, we have observed a similar increase in volume over time, with an 81.8% increase from 11 new groups in Q4 2024 to 20 new and Emerging groups in Q2 2025.



# Unknown Group and RaaS Reputation

We assess that this continued growth is likely driven in part by the scattering of affiliates and operators following the disruption of the most prolific RaaS group, RansomHub, as well as by other high-profile disruptions from law enforcement, which have fractured established ransomware ecosystems. As a result, a high volume of ex-RaaS affiliates or lower-level threat actors and developers have been forced to splinter off, forming their own operations or joining RaaS Groups, new and old. The observable increase in new groups could suggest a broader shift of affiliate interest away from the most prolific and Established RaaS groups, probably driven in part by the significant attention such groups garner from law enforcement and security efforts. Instead, 'free agent' threat actors may begin to opt for smaller, less prolific operations that can operate with a lower profile while continuing to reap the financial benefits of their operations. Together, these observations contribute to a more fragmented but highly active ransomware landscape in the first half of 2025.

In addition to this measurable increase in "traditional" branded ransomware operations, we have anecdotally observed an increase in unbranded, or "no name" groups, which use throwaway sobriquets or refuse to identify themselves or make any associations. Anecdotally, these actors often display less complex or sophisticated tactics and respond in a less structured fashion in negotiations, suggesting that such groups may often be populated by more junior ransomware or data extortion operators.

The "no-name" approach carries with it some inherent risks. Without a known identity, it is even more difficult to forecast adversary behavior or relative "trustworthiness" in honoring ransom payment agreements. Without a dedicated or branded Data Leak Site, "no-name" actors lack clear evidence to display the victims of their past crimes, as well as a dedicated location to post large volumes of data at a centralized location. Posting compromised data to illicit forums remains an option, though visibility, impact, and hosting restrictions may limit the impact of this approach. On the other hand, "no name" groups that refrain from hosting an open data leak site may be harder to track from a law enforcement perspective.

Overall, we have observed and assessed more widely that "no-name" or unbranded ransomware groups and data extortionists face lower rates of ransom payment amidst more limited impacts and greater difficulty in establishing their cybercriminal bona fides. In spite of this, we expect to continue to see such groups for the foreseeable future, complicating defender attribution and law enforcement disruption efforts in the space.



# Unknown Group and RaaS Reputation

## **Increasing Coercive Tactics**

In addition to unknown groups, we have also experienced ransomware actors performing escalating coercive actions. In many cases, these threat actors decide to send email, faxes, texts, and even perform phone calls to certain personnel in an attempt to pressurize the victim further, all while already engaged in post-incident communications. It is often a tactic used to nudge the victim into speeding things up by sending threats to business leaders.

From unsophisticated threat actors to the more well-known and sophisticated actors, this activity has continued to occur, and unfortunately, may continue to occur as long as this remains an operation led by criminals. These coercive outreach efforts are seen across the board but are particularly common among mid-tier and smaller RaaS affiliates who may be under pressure to deliver results or close out an extortion quickly. In some cases, they appear to be operating independently or outside the guidance of the original ransomware group. The objective of these coercive tactics is unclear to the moral mind, as they almost never work and often cause reputational damage to a given ransomware group, even making payments less likely to occur.

GRIT has observed that this kind of harassment can erode any remaining trust or perceived professionalism, pushing victims further away from the idea of negotiating with the threat actor. Likely more of the same is still to come, unless the broader ransomware ecosystem begins to self-regulate, which seems unlikely. The correct response from defenders is to anticipate these escalation tactics, warn personnel not to engage with unsolicited threats, and maintain discipline by limiting all communications to the primary negotiated channel.



# Distraught Over Data Hosting

Throughout Q2, ransomware operators have encountered publicly visible technical challenges on their data leak sites, a trend that threatens to impact the leverage of affiliates in double extortion ransomware operations. Double Extortion attacks have become the norm among RaaS groups since 2019. It began in response to the rise of secure data backups as standard cybersecurity practice and reducing the effectiveness of extortion centered on decryption alone (original, or “Single Extortion” ransomware). As Double Extortion depends on the threat of data publication by threat actors, interruptions to this capability either removes or disrupts what may be the only remaining coercive lever at a threat actor’s disposal in the event a victim maintains viable backups.

Qilin, a Double Extortion RaaS group operating since late 2022, has demonstrated the most observable issues with data hosting. Over the past three months, GRIT has observed multiple instances of weeks-long gaps between Qilin’s announcements of new victims and the subsequent availability of victim data for download. We have considered the possibility that this approach could be interpreted as a negotiation tactic from Qilin’s perspective, in which victims are given a final warning prior to data release and extending the amount of time that victims have to pay a ransom demand. If this were the case, however, we would anticipate a much shorter time between announcement and leakage, measured in days instead of weeks. We assess that it is more likely that Qilin has struggled to house increasing volumes of victim data. Qilin has increased its operational tempo substantially in 2025 and claimed over 200 victims in Q2, potentially equating to tens of terabytes of data. In one instance, GRIT identified a victim claimed on Qilin’s data leak site, including advertisements for the compromised data. Upon inspection, the File Transfer Protocol (FTP) server supposedly storing the data was, in fact, empty.

Akira appears to have faced the same issues since the start of 2025, exhibiting substantial delays between publishing a victim’s name and its stolen data. Akira has seemingly attempted to combat the data storage issue by using torrents to crowdsource hosting. Torrents allow users to simultaneously download and upload files to prospective downloaders as long as at least one “seeder” has the full data set to share. This removes Akira’s burden of hosting data long term on their own servers, which can instead be done by other dark web users who house the files on their own systems for other users to retrieve.



# Distraught Over Data Hosting

Akira and Qilin have risen to become the top two most prominent RaaS groups following a drop off from Ransomhub, who had dominated the ransomware landscape for approximately a year and had successfully hosted vast amounts of victim data. Both Akira and Qilin's potential data storage issues could be described as "growing pains" as the groups' operations quickly expand beyond their prior capacity, absorbing displaced affiliates or new entrants. This increase in activity has likely strained its data storage infrastructure, which could mean more financial struggles for the group in the future if victims take note of this behavior and refuse to succumb to ransomware demands due to the lessened risk of data exposure.

Reporting from Coveware shows that ransomware payments have steadily declined since 2019, a trend that we assess will likely continue throughout the remainder of the year. Issues with data storage leading to issues with extortion leverage could cause ransomware affiliates to lose further revenue necessary to sustain their operations. In the near-to-mid-term, we expect to see efforts by prolific ransomware groups to address these storage issues through non-traditional means, including torrenting, use of FTP servers, and file sharing services such as MEGA, particularly if they struggle to obtain reliable dedicated storage tied to their data leak sites.

Victims of Akira and Qilin should consider the groups' data hosting issues throughout decision making and risk calculus. Historically, we have seen threat actors share victim data shortly after communications have broken down, but Akira and Qilin may wait weeks post-negotiation to share any data without any formal notice. This means organizations may have to monitor the threat actor's dark web site for an extended period of time, which in some circumstances could impact the timeline of disclosure notification requirements.



# A Little Bit of LockBit Leaks

## Overview

LockBit – once the most prolific Ransomware-as-a-Service group in active operations from roughly 2020-2024, before facing international law enforcement pressure and sanctions – cannot seem to catch a break of late. In mid-May, reports surfaced of a successful “hack” against the group’s infrastructure. It first manifested by a site defacement message reading “Don't do crime CRIME IS BAD xoxo from Prague,” and accompanied by a link to allegedly breached data. (For long time watchers of the space, the same wording was used on an April 2025 site defacement of the ransomware group, Everest).

The linked data, which took the form of a compressed 26MB SQL database, appeared to reflect data from December 2024 to April 2025 dumped from LockBit’s backend affiliate “panel,” the web application used by affiliates to generate encryptors and communicate with victims. Researchers quickly coalesced around the data’s authenticity, and we opted to take a look.

The leaked data included nearly 60,000 Bitcoin addresses and credentials for 75 administrators and affiliates. As researchers began diligently examining these, we opted to focus on the 4,492 chat messages reflecting contact between victims and LockBit affiliates, which yielded the following data points and anecdotes of interest:

- In terms of victims and victim volume, we identified at least 208 unique chat IDs corresponding to distinct chat rooms, though several appeared to be continuations or resets of historical or existing correspondence between victims. Victims appeared to be based in a wide range of geographic locations, including Brazil, China, Egypt, France, Germany, Iran, Peru, Poland, Taiwan, and the United Arab Emirates.



# A Little Bit of LockBit Leaks

- In terms of payment information, despite the very large number of cryptocurrency wallet addresses featured in the dataset, we confirmed only 15 instances of payment issuance and receipt on the blockchain.
  - Those observed payments totaled less than \$500,000 USD in aggregate, with the lowest observed confirmed payment a modest \$6,000 USD, and the highest at approximately \$60,000 USD.
  - Initial demands we observed from affiliates were almost always substantially higher, averaging out to \$150,000 USD before negotiations brought the average final demand down to a more modest \$44,000. Dozens of observed demands were in the low thousands (\$4,000-\$8,000), though we observed three outlier demands of \$1.2 million, \$2 million, and \$4.5 million USD. We were unable to confirm payment of these high-sum ransoms, though separate reporting [from Trellix](#) has reflected one \$2 Million ransom was paid.
- Multiple victims self-identified as China-based or Taiwan-based, a notable departure from LockBit's historical focus on mostly western victims. This introduced friction into the equation, as several such victims expressed an inability, whether real or exaggerated, to obtain the Bitcoin, which LockBit affiliates demanded, due to local restrictions or controls. Several victims instead requested to pay instead in Tether (USDT, a stablecoin pegged to the US Dollar). Over time, at least some affiliates impacting China-based victims seemed to accept this and began making demands or offering payment in USDT in lieu of the typical Bitcoin.



# A Little Bit of LockBit Leaks

- In multiple instances, affiliates appear to have been afforded limited autonomy and faced substantial delays while pending approval or decryptor generation from an unidentified “boss”.
  - In a mid-March 2025 chat, the affiliate explains that they had been waiting for three days for their “boss” to provide a decryptor, opining to the victim in the process that the “boss” “doesn't trust to nobody the private keys from the decryptor” and “hasn't answered anyone for 3 days.” The affiliate remained unable to proceed for an additional two days afterwards.
  - In two separate chat instances, an affiliate communicated to a victim that “The boss is very busy and often [sic] responds to messages for 3-5 days,” and a victim complained that “the boss” had been unavailable for 10 days.
  - In multiple other instances, the affiliate appears to have required approval to accept offers or propose counteroffers in negotiations, responding to victims that they will “tell the boss”
- In one unique instance, the affiliate references themselves as part of a partnership between LockBit and the ransomware group Hellcat. Hellcat is a seemingly insular data extortion group which emerged and sharply declined early this year. It was comprised of a handful of seemingly juvenile operators which sought attention through informal interviews and general trolling, at one point demanding a French victim pay their ransom in baguettes. While we cannot independently confirm a genuine connection between the two groups outside of this singular claim, it is noteworthy in that no such connection had been previously observed or reported prior to the leak.



# A Little Bit of LockBit Leaks

- In at least two instances, the victim or negotiator on the receiving end of the extortion effort expressed interest in joining LockBit's affiliate program. In both cases, the affiliates appeared dismissive of the request, demurring and providing a short explanation that membership could be obtained by paying \$777 for panel access. **We do not recommend this as a lifestyle or career choice.**
- In one instance, we observed an alleged RansomHub affiliate who had seemingly opted to transition their negotiation with a victim to LockBit's infrastructure in April 2025. This coincides with GRIT's reporting from the same time frame of internal discord among RansomHub's affiliates. **This appears to have backfired for the affiliate, as the victim or negotiator on the other end proceeded to explain that they could no longer pay the affiliate due to their ties to LockBit as a sanctioned entity.**

## Key Takeaways

- LockBit's offering of "lite" panel access via self-registration at a cost of \$777, which may have begun in December 2024, likely reflects the group's status as a diminished power and efforts by LockBit's administrators to generate revenue outside of ransom payments. Compared with former LockBit operations at the hands of seemingly experienced affiliates, the leaked chat logs reveal a number of apparently newer and relatively inexperienced affiliates, with lower demands and success rates of extortion.
- Ransomware remains a global problem, with diminishing "safe" global targets. Although Russian targets appear to remain off-limits for Ransomware-as-a-Service groups including LockBit, Chinese targets appeared to pose no issue for multiple LockBit affiliates within this period.
- LockBit's administrators, including potentially "LockBitSupp", appear to be consistently inconsistent and unreliable throughout messages in this leak, with affiliates facing substantive delays in their operations as a result. We do not know the cause of these delays but assess that a lack of responsiveness and independence suffered by affiliates will reduce retention of LockBit affiliates with "better options" at other RaaS groups.
- The above takeaways and LockBit's sinking status in the RaaS ecosystem can be directly attributed to the effectiveness of western sanctions against the group in the wake of the UK National Crime Agency's 2024 Operation Cronos. While US/UK/Australian organizations may still face attacks from LockBit affiliates, we observed no instances in the leaked chats of successful negotiations and payment from such organizations. Whether immediately or over time, LockBit affiliates have almost certainly determined that victim organizations from the US, UK, or Australia are unlikely to pay a ransom to affiliates overtly leveraging LockBit infrastructure.



# Iranian Cyber Threat Activity

## Post-Strike Activity Outlook

On June 22, 2025, the US military struck Iranian nuclear facilities at Fordow, Natanz, and Isfahan as part of the current Israel–Iran conflict. While kinetic operations historically correlate with increased cyber activity, we have not yet observed a major surge in cyberattacks from Iran in public reporting. However, the Department of Homeland Security anticipates that Iran's cyber forces will target US networks following the nuclear facility strikes, aligning with established patterns observed in previous regional conflicts.

Iranian state leadership most frequently uses cyber operations to project political messaging and conduct intelligence collection. These operations typically focus on regional targets, particularly Israeli infrastructure, while maintaining capabilities against high-value targets, including politicians, key decision-makers, and directly involved entities. Supply chain targeting remains a consistent methodology, with Iranian actors targeting vendors, providers, and critical infrastructure dependencies.

Iranian cyber threat actors have previously demonstrated their ability to conduct both opportunistic and sophisticated operations against victims either deliberately targeted or seized upon as timely opportunities have arisen. The scope and intensity of state-directed or state-endorsed responses from these actors to date, however, appears measured. Assuming this trend continues, this suggests that Iranian leadership recognizes the limitations of cyber retaliation against its adversaries' superior kinetic capabilities. Consequently, we assess that Iran-sponsored cyber activity will likely focus on Middle East regional infrastructure, its traditional focus area, rather than large-scale attacks against US homeland targets in the near term.

## Hacktivism

Initial but limited retaliation has included Distributed Denial of Service (DDoS) campaigns, such as those of the Iran-aligned 313 Team, which claimed responsibility for attacks on the social media site Truth Social within hours of the strikes. There are reportedly over 120 Iran-affiliated hacktivist groups that have been observed actively operating in relation to the current conflict with Israel; with DDoS attacks and destructive malware operations being the primary attack methods for these operations. Other operations attributed to these groups include data breaches targeting energy and utility companies, hijacking and cyberespionage directed against Internet of Things (IoT) and Operational Technology (OT), including the hijacking of home security cameras and hack-and-leak operations designed to damage adversary credibility.



# Iranian Cyber Threat Activity

## Ransomware

Iranian cyber operations increasingly blur the lines between state-sponsored and cybercrime activities. Recent investigations from the US Cybersecurity and Infrastructure Security Agency (CISA) and the FBI have identified an Iranian cybercrime group dubbed Pioneer Kitten—also known as UNC757, Parisite, Rubidium, and Lemon Sandstorm—as targeting US and foreign organizations across multiple sectors. These obtain and develop extended network access and collaborate with third-party affiliates such as NoEscape, Ransomhouse, and AlphV (aka BlackCat) to deploy their ransomware.

Iranian actors conduct computer network exploitation activity in support of the Government of Iran, including intrusions enabling the theft of sensitive technical data against organizations in Israel and Azerbaijan. This approach provides operational flexibility while maintaining plausible deniability for state leadership. The ransomware ecosystem demonstrates Iranian actors' ability to monetize network access while supporting broader state intelligence objectives.

## Russia-Ukraine Conflict Comparison

The Russia-Ukraine cyber conflict offers valuable lessons for understanding contemporary cyber warfare dynamics and provides an instructive framework for analyzing Iranian cyber operations. Russia's invasion of Ukraine is the most recent conflict in which large-scale cyber operations functioned as an integral component of kinetic operations. It has involved large-scale cyber operations that demonstrate several key characteristics: extensive pre-positioning of malware, coordinated destructive attacks synchronized with kinetic military operations, and sustained targeting of civilian critical infrastructure, including power grids and communications networks.

However, in the case of Ukraine and Russia, cyber operations have played a shaping role rather than a decisive one. Despite extensive engagement and massive involvement of cybercrime groups, cyberattacks have not been a deciding factor in the conflict. This outcome is the result of several factors, including Ukrainian cyber resilience, international support, and Ukraine's lessons learned from earlier Russian cyber campaigns.

When examining Iranian cyber operations through this lens, several distinct patterns should be considered. Iranian cyber activities typically demonstrate more surgical precision and escalation management compared to the comprehensive degradation approach seen in Ukraine. While Russian operations have sought systemic disruption of critical infrastructure, Iranian cyber responses focus on symbolic targets and proportional disruption designed to signal resolve while avoiding triggers for disproportionate retaliation. This reflects both different strategic objectives and operational constraints.

This case study comparison highlights how cyber operations serve different strategic functions depending on the broader conflict context, from signaling and deterrence in limited engagements to comprehensive warfare support in existential conflicts.



# Iranian Cyber Threat Activity

## Forward-Looking Assessment

Iranian cyber retaliation could manifest in several forms over the coming months. CISA recommends that defenders stay aware of changing conditions. These threat categories may also warrant further monitoring:

1. Espionage by Iran-controlled nation-state actors
2. Spear-phishing campaigns by Iranian actors against diplomatic targets with ties to the US seeking to deploy destructive wiper malware
3. Disruptive DDoS attacks and social media influence operations by Iran-aligned hacktivist groups

Following trends in past behavior demonstrated against Israeli critical systems, Iran-linked threat actors may again target regional infrastructure. Recent targeting of IoT and OT, including home security systems and industrial control networks, indicates Iranian actors maintain sophisticated capabilities for infrastructure disruption. However, attacks against US homeland targets will likely prioritize symbolic rather than strategically significant objectives to avoid escalatory responses.

Interconnected networks and supply chains increase the potential for supply chain compromises targeting IT providers and critical infrastructure vendors. Iranian actors, particularly Tortoiseshell (APT456, Devious Serpens), have demonstrated capabilities for supply chain campaigns against Middle Eastern IT providers since 2019.

Iranian actors may continue leveraging generative AI for enhanced social engineering operations, building onto previously observed capabilities such as the use of fake documents and customized impersonation techniques. The integration of AI-enhanced phishing alongside the exploitation of known vulnerabilities is an evolving threat that should be monitored as this conflict continues.

## Recommendations

CISA confirmed on June 22, 2025, that no specific credible threats from Iran currently target US critical infrastructure, though the agency encourages continued review of DHS threat bulletins. Organizations should prepare business continuity plans addressing cyberattack scenarios while developing protocols to validate and respond to breach claims or data leak allegations, as threat actors frequently use false claims for harassment and political messaging.

The ongoing conflict warrants increased vigilance to cyber threats from Iran. Organizations may consider enhanced monitoring for threat signals associated with internet-facing assets, including websites, VPN gateways, and cloud infrastructure. Critical priorities include ensuring all internet-facing infrastructure maintains current security patches and hardening configurations, while implementing comprehensive employee training on evolving phishing and social engineering tactics, incorporating AI-enhanced techniques.





# Quarterly Wrap Up

While we are hopeful at the sight of reduced victim volume in Q2, we do not yet have sufficient evidence to assess that the quarter's reductions are indicative of a longer-term trends; rather, indications to date suggest Q2's figures could largely be the result of temporary headwinds.

Seasonality almost certainly plays a factor in the activity levels of ransomware groups of all sizes, particularly as we enter the summer months when, as ridiculous as it sounds, many threat actors are believed to be on vacation. We expect to see continued lulls in activity into and through August, with an increase in operations tempo in the latter half of Q3 into Q4, largely consistent with historic norms.

We continue to assess that the impact of disruption to large RaaS groups – whether from international law enforcement or internal disunion – is not a substantial drop off in ransom activity but a realignment of operational capacity amongst other RaaS groups, as other RaaS groups absorb displaced affiliates.

This does not mean that disruption of RaaS groups serves no purpose; introducing friction and imposing costs on administrators reduces the net gain that cybercriminals benefit from and introduces uncertainty for those “on the fence.” Development of new encryptors, standing up of new infrastructure, onboarding of new affiliates, increasing capacity of existing infrastructure – these all take time and negatively impact active or emerging groups, a net positive for would-be victims. However, the problem remains larger than any one group, an enduring and unfortunate advantage of the RaaS model. Ransomware victim volume is still likely to be highly polarized among a small number of “leading” RaaS groups, though the specific groups will change over time.

With 2024 and 2025's disruptive events, we are only beginning to see the downstream impacts on the wider ecosystem, and in addition to redistribution of affiliates in longstanding RaaS groups, it is also apparent that the number of unique named groups continues to increase in parallel, likely reflecting splintering of affiliates into new organizations. We expect to see many of these groups using leaked builders, such as those from LockBit in 2022, or eschewing encryption altogether, affording easier standup of distinct RaaS or insular ransomware groups.

GRIT continues to monitor the ransomware and cybercrime landscape, that we might better observe these trends and changes as they occur. We encourage Defenders to remain educated on the most prolific groups operating today and their tactics, which eventually trickle-down even to new groups. As the second half of the year begins, old tactics continue to merge with new names, keeping us all busy but presenting the same opportunities for detection and disruption.

-Happy Hunting.