



GRIT

Ransomware Report

JANUARY – MARCH, 2024

Contents



Quarterly Ransomware Summary



Quarterly Ransomware Trends



Taxonomy Breakout



Threat Actor Trends



Threat Actor Spotlight - Qilin



Quarterly Wrap-up



Appendix

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.

QUARTERLY



Ransomware Summary

Following an increased pace in Q4 2023, Q1 of 2024 observed posts decreased slightly while still demonstrating a nearly 20% increase in victim volume year-over-year. Decreased activity in the first quarter of the year mirrors trends from 2021-2022, though we note that observed victim rates increased relative to the preceding Q4 during Q1 2023. As such, while we continue to observe increased victim volume over time, a repeated seasonal trend between Q4 and Q1 cannot be assessed beyond a low level of confidence. We have and continue to note a typical decrease in operational activity from the last week of December through to the first two weeks of January, likely driven by the holiday season and New Year's.

Q1 saw substantial shifts in activity from some of the most prolific Ransomware-as-a-Service (RaaS) groups. In particular, observed victims attributable to Alphv dropped off completely following an apparent exit scam in March, which the group claimed was the result of a law enforcement takedown. Open-source reporting and atmospheric reports from illicit forums indicate that Alphv's administrators may have instead absconded with a final large ransom in the tens of millions, pocketing the affiliate's share of the funds and offering to sell the remaining infrastructure.

Additionally, LockBit experienced an impactful law enforcement takedown resulting from the action of the Operation Cronos Task Force, helmed by the UK National Crime Agency (NCA). While LockBit would go on to recover and stand up new infrastructure, the widely publicized takedown almost certainly dealt a blow to LockBit's operations, raised uncertainty among the LockBit group and its affiliates, and resulted in the public revelation of unique intelligence and insight into the group's operations. In the wake of continued impacts on the most prolific RaaS groups, we have observed attempts by other smaller RaaS groups, including Medusa, Cloak, and Ransomhub, to recruit disaffected or displaced affiliates.



QUARTERLY

Ransomware Summary (cont'd)

Q1 2024 marks one year of continuing observed operations for the ransomware group, Qilin, whose methods and activity we explored in this quarter's TA spotlight. We also reflect on recent reporting regarding members of the so-called "Five Families" hacker collective, which has attracted attention in Q1 for alleged collaboration between two of the five groups, but which we assess is likely exaggerated or embellished.

Later, we turn our attention to Phobos, a RaaS group that does not operate a traditional ransomware leak site and has seen significant attention in recent reporting, as demonstrated by a February Joint Cybersecurity Advisory from CISA and the Multi-State ISAC. The group's affiliates typically communicate with victims over email, and their operations may follow either a single or double extortion approach, with some victims reporting exfiltration and others reporting encryption only. Importantly, Phobos affiliates have been observed attempting to re-extort victims for a secondary payment before providing a decryption tool.

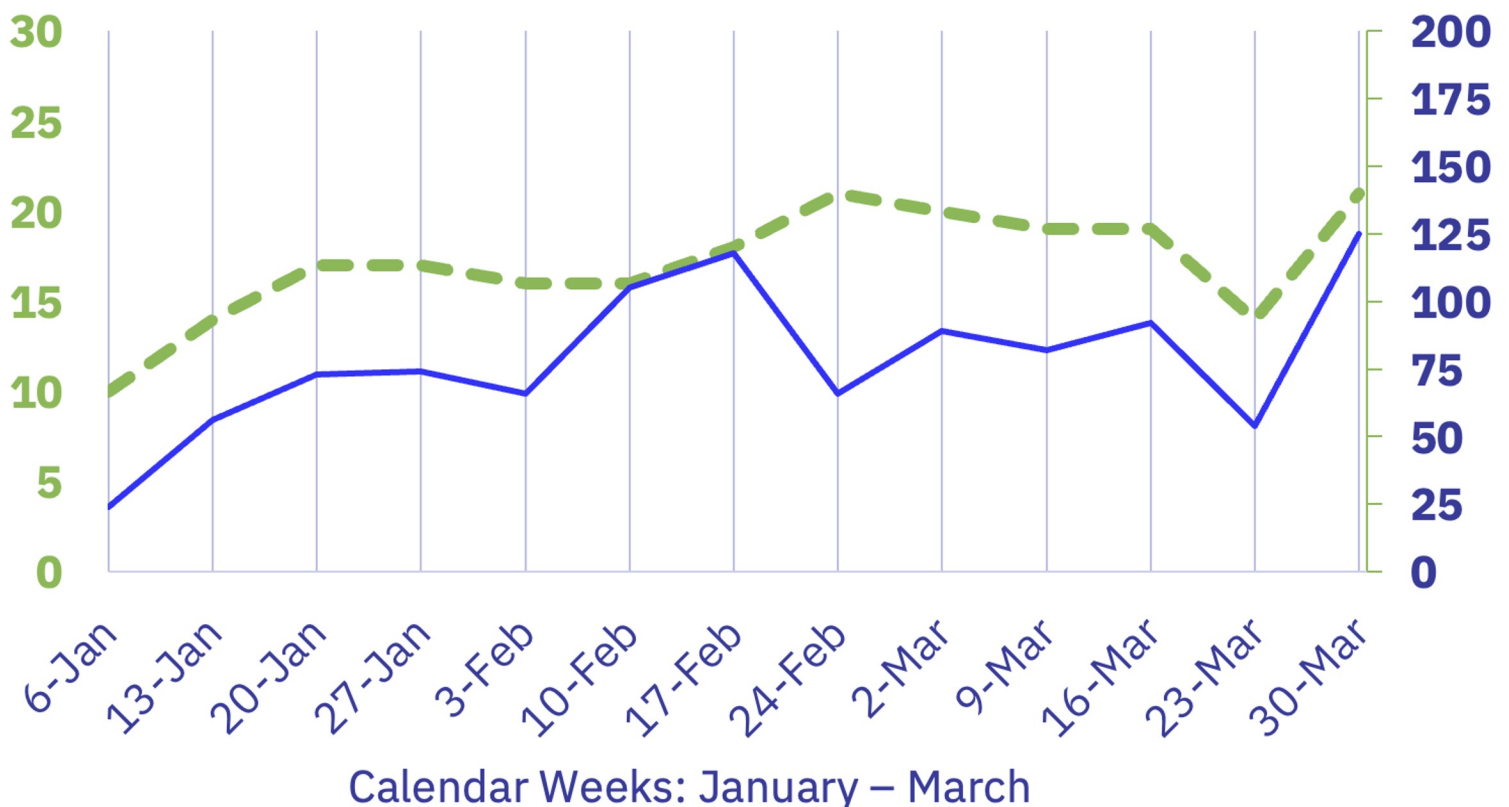
The remainder of this quarterly report outlines trends, observations, and key takeaways pertaining to observed ransomware operations and headlines from January – March 2024, including continued disproportionate impacts against western targets and recently observed attacks impacting the construction industry.

	Q1 2024	Q4 2023	Q1 2023
Total Publicly Posted Ransomware Victims	1,024	1,117	859
Active Ransomware Groups	45	45	29
Average Daily Victims	11.3	12.1	9.54

Q1 2024 in Review

Q1 resulted in a 19.2% increase in reported victims over Q1 2023, despite the disruption of LockBit and the disbandment of Alphv. Q1 2024 similarly saw an increase in active ransomware groups, increasing by 55% from 29 in Q1 2023 to 45 distinct groups in Q1 2024. Overall, the ransomware economy's operational tempo maintained a minimum of 50 posted victims each week, with the exclusion of the partial week at the beginning of the year. At its highest rate, ransomware accounted for 125 victims within a single week at the end of March. Higher operational tempos may have been spread across distinct groups, as we observed at least 14 distinct ransomware groups posting victims each week, with two individual weeks resulting in posts from 21 distinct groups.

Rate of Publicly Posted Ransomware Victims



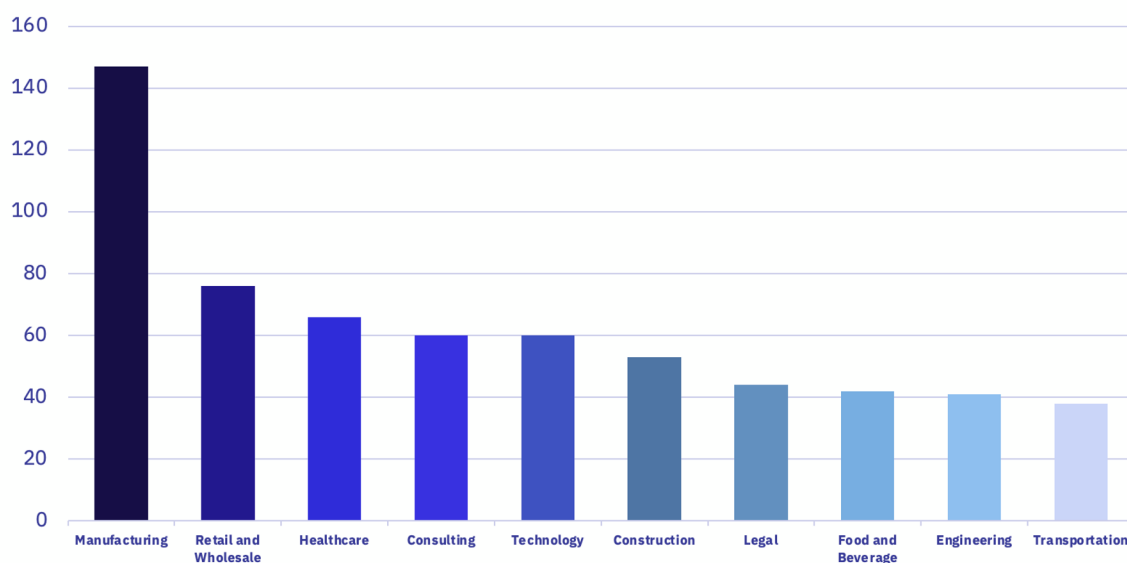
● Total Posts **1,024** ● Total Groups **45** Average Posts per Week **79** Average Groups per Week **17**

Q1 2024 in Review (cont'd)

Despite having previously decreased in terms of observed victims through Q4 2023, the Retail and Wholesale industry experienced a resurgence in observed activity during Q1 2024, accounting for 76 distinct observed victims. Retail and Wholesale subsequently increased to become the second-most impacted industry, accounting for 7% of all observed posts. Healthcare remains one of the most targeted industries, but it dropped to the third-most impacted industry with 66 posted victims, 14 fewer than in Q4 2023.

The most notable quarterly change in industry data is reflected in the number of impacted Government organizations. The number of posted victims dropped from 50 in Q4 2023 to 29 in Q1 2024, a 42% decrease. Technology saw a negligible increase in posted victims, from 58 to 60. However, with the drop in total victim posts, this slight increase in absolute terms resulted in the industry's relative level of impact escalating from sixth to fourth.

Most Impacted Industries – Q1 2024



● Manufacturing

- LockBit
- 8Base
- Blackbasta

● Retail & Wholesale

- LockBit
- Blackbasta
- Play

● Healthcare

- LockBit
- Bianlian
- Alphv

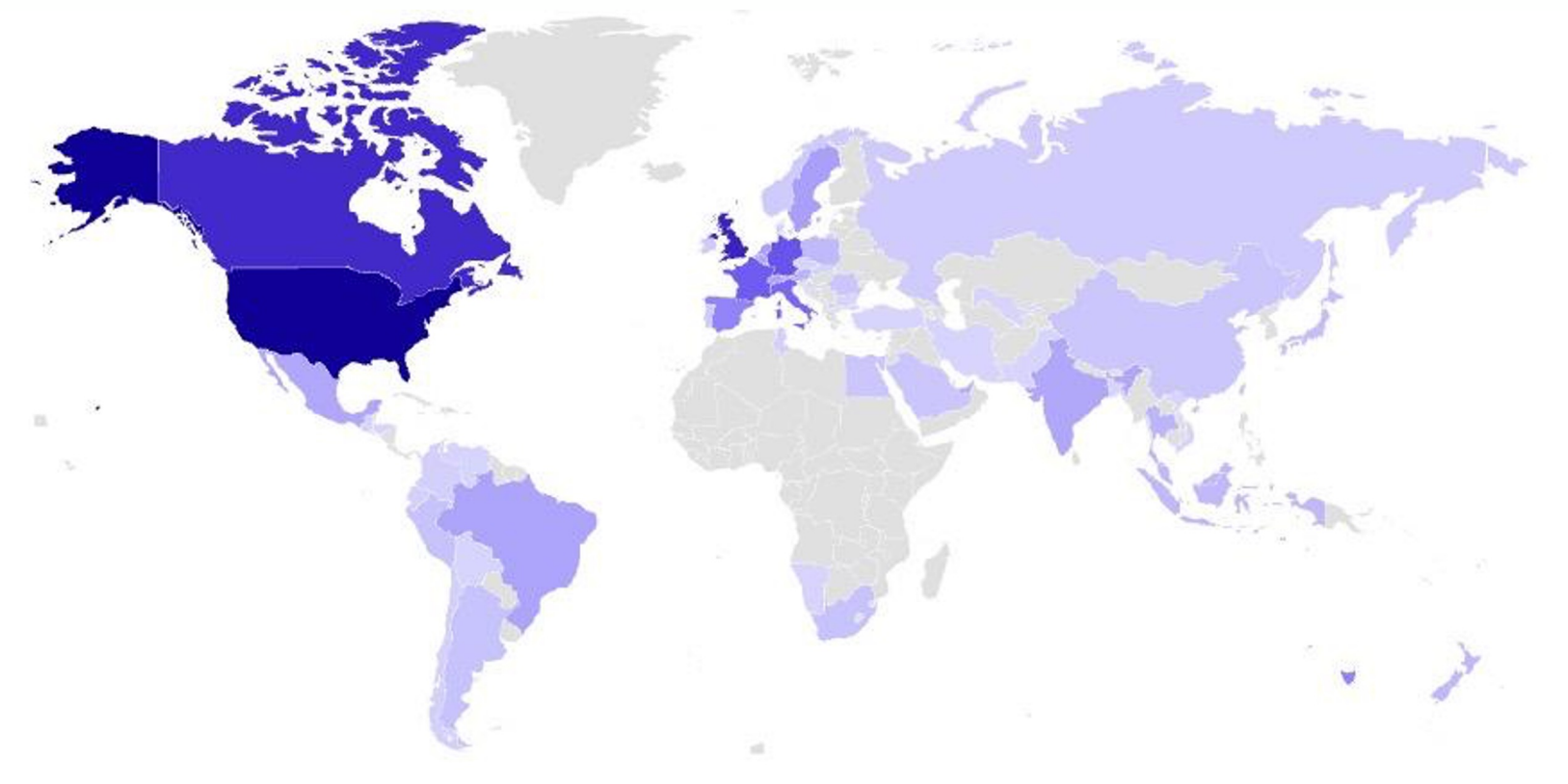
● Consulting

- LockBit
- Alphv
- Bianlian

● Technology

- LockBit
- Hunters
- Akira

Geographic Breakdown of Ransomware Victims (Q1 2024)

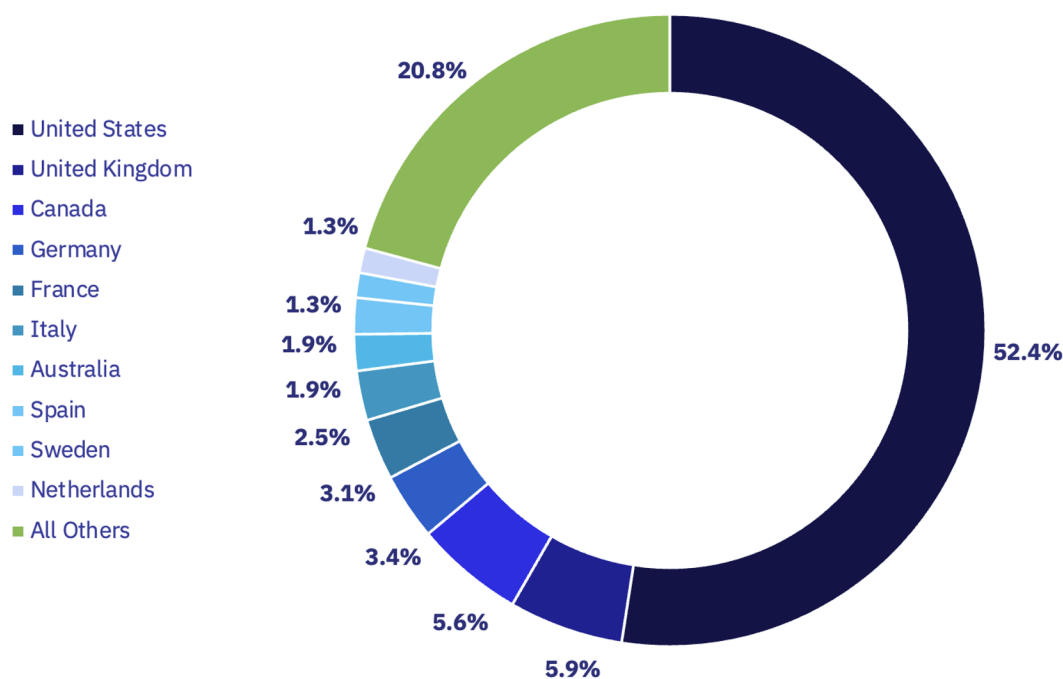


Top 10:

1. United States
2. United Kingdom
3. Canada
4. Germany
5. France
6. Italy
7. Australia (tied with Spain)
8. Spain (tied with Australia)
9. Sweden (tied with Netherlands)
10. Netherlands (tied with Sweden)

Q1 2024 in Review (cont'd)

Country Breakdown (All Threat Actors)



For the first time since Q2 2023, the United States absorbed over half of all observed victims, with 537 of the 1,024, or 53%, of all observed ransomware posts attributed to US-based organizations. A deeper analysis revealed that US-based healthcare organizations accounted for the majority of observed attacks against healthcare in Q1 2024, with 53 of 66 observed posts, or 80%, impacting US-based healthcare organizations.

The largest increase in reported victims was experienced by Sweden, with the number of observed victims attributed to Sweden-based organizations increasing from four in Q4 2023 to 13 in Q1 2024, a threefold increase. The largest decrease in observed victims by country was associated with the United Kingdom, which experienced a 26% decrease in total victims, down from 81 to 60 quarter-over-quarter. Unfortunately, the UK still absorbs the second-highest number of observed ransomware attacks, second only to the US.



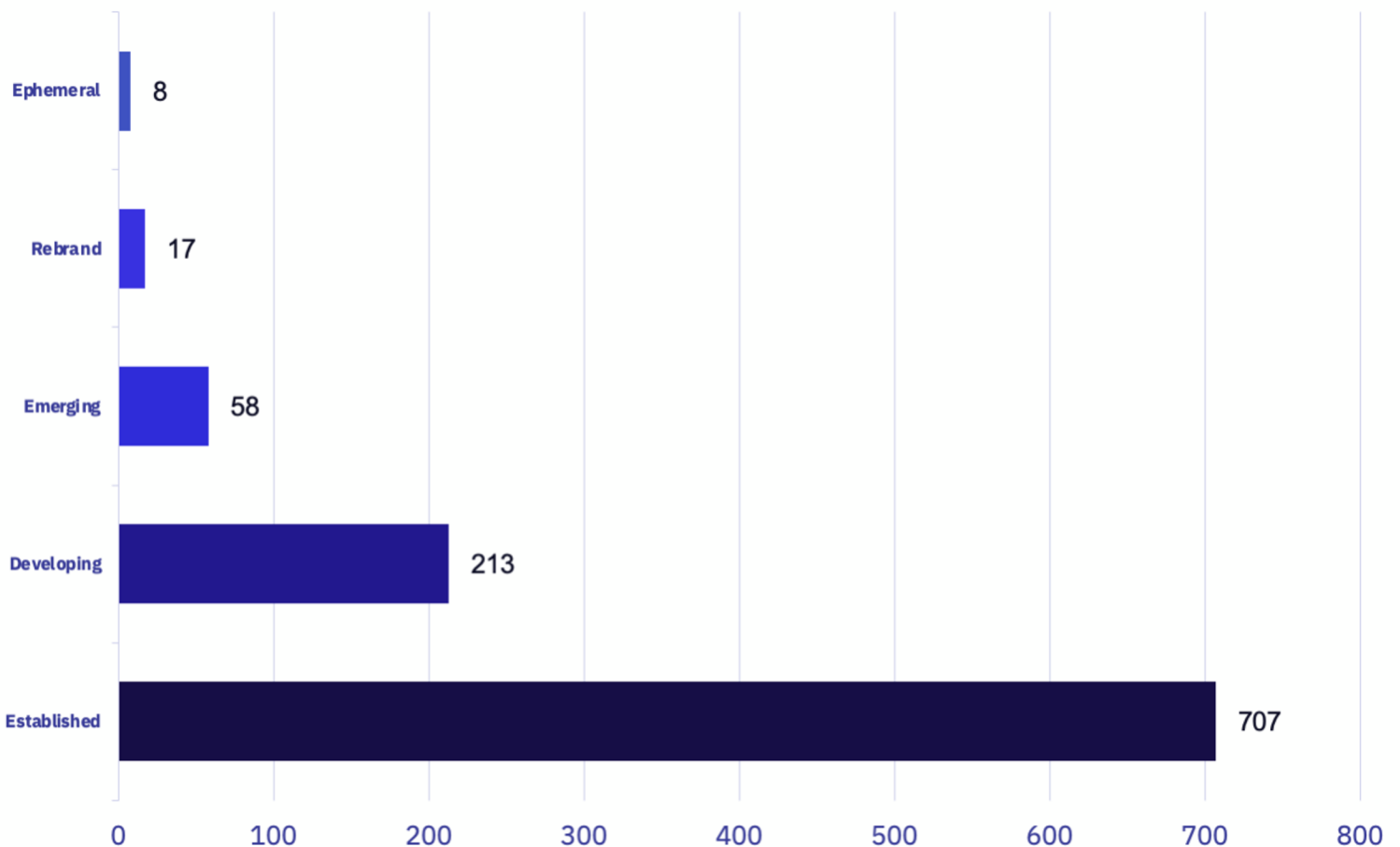
Taxonomy Breakout

Notably, short-lived Ephemeral groups represent the highest percent decrease in activity, dropping 68% from 25 posted victims in Q4 2023 to 8 in Q1 2024. This continues to reflect the minimal victim volume impacts of these short-lived groups within the wider ransomware ecosystem.

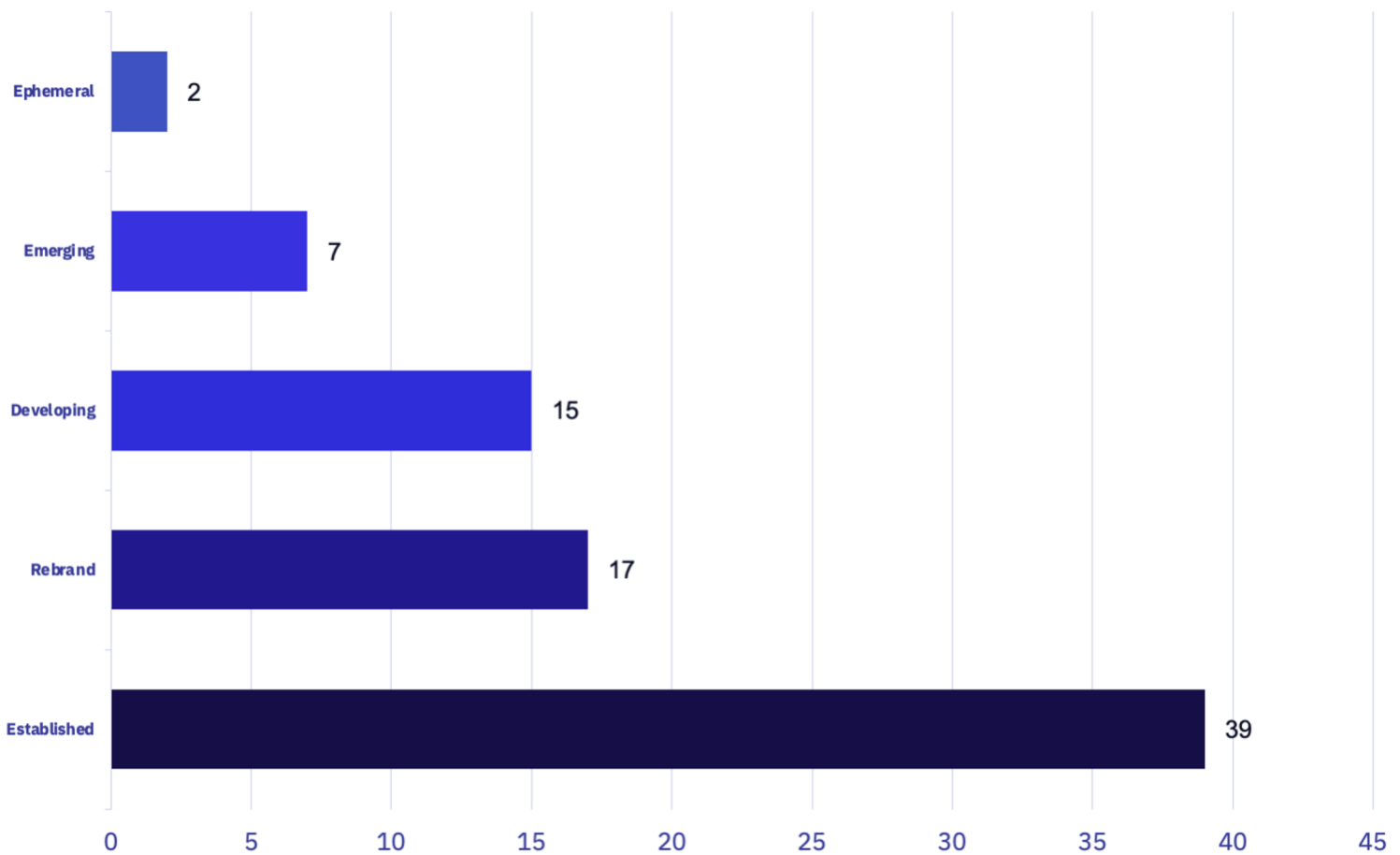
In fact, GRIT observed a decrease among all group taxonomies except Rebrand throughout Q1 2024 compared to Q4 2023, with an average decrease of 11.6%.

Blacksuit, the only confirmed active Rebrand group operating in both Q4 2023 and Q1 2024, increased its number of posted victims from 11 to 17, resulting in a higher rate of activity in the Rebrand classification.

Overall Activity by Taxonomy Classification



Average Activity by Taxonomy Classification



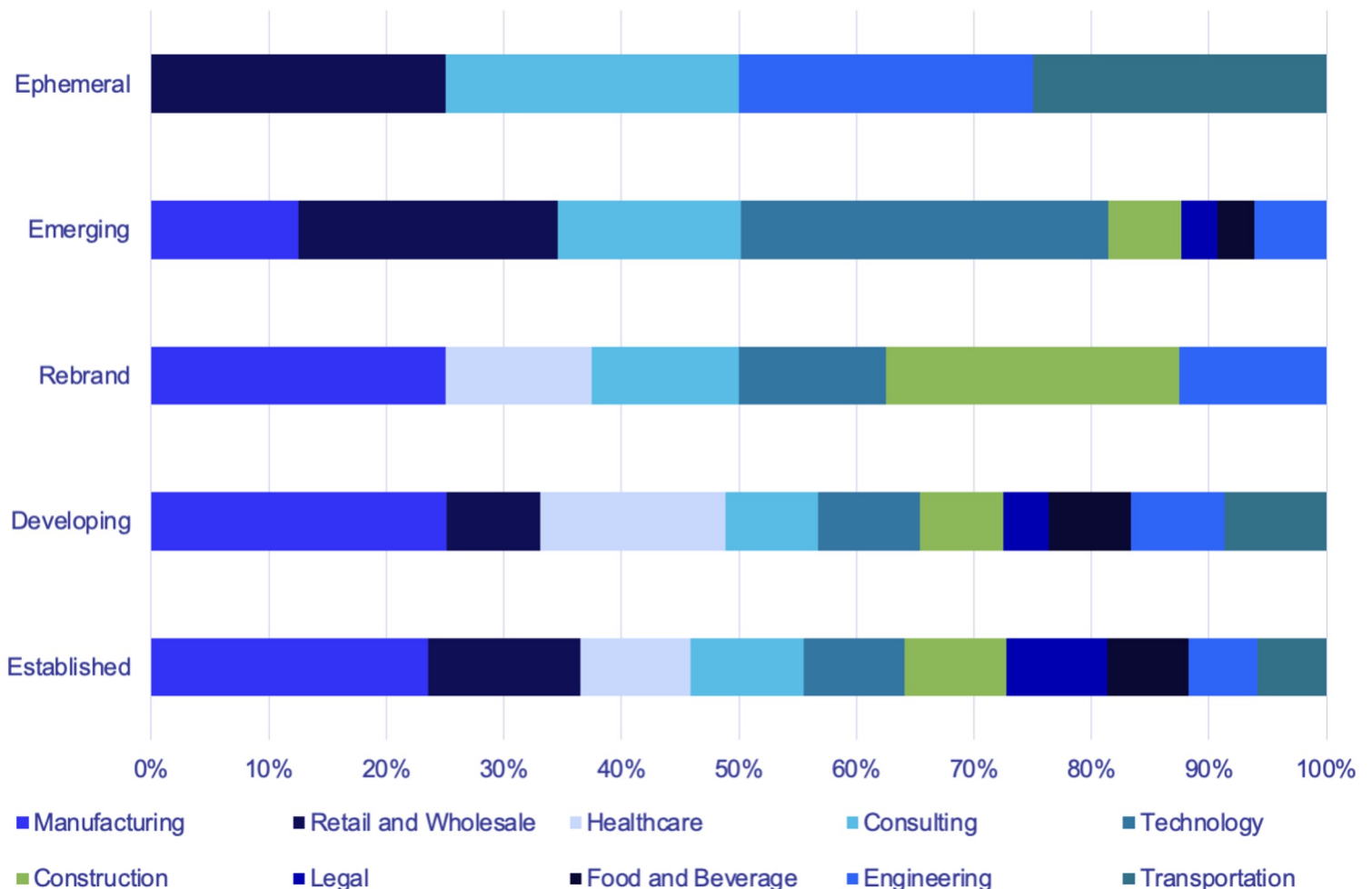
The average posts per group across taxonomies mirrors what we'd expect to see based on groups' technical capabilities.

In total, GRIT tracked 18 Established, 1 Rebrand (Blacksuit), 14 Developing, 8 Emerging, and 4 Ephemeral groups. Dividing the total posts per taxonomy by the number of groups tracked gives us the data represented above.

By aligning our group taxonomy against our top 10 impacted industries, we can see that the posted victims of more sophisticated and prolific groups are more evenly distributed across industry verticals. Extending our observation from GRIT's 2023 Annual Ransomware Report, Developing groups impacted Healthcare organizations at a disproportionate rate relative to Established groups, with 9.4% of all victims claimed by Developing groups attributable to the Healthcare industry, compared to 5.9% of all Established groups' claimed victims.

We expect continued and increasing impacts against the healthcare and critical infrastructure organizations based on declarations from LockBit and the now-defunct Alphv "opening up" such organizations to attack in the wake of law enforcement disruption operations. We expect these statements to further normalize attacking such organizations, which were at one point considered "off limits" by many groups.

Industry Impacts by Taxonomy Classification





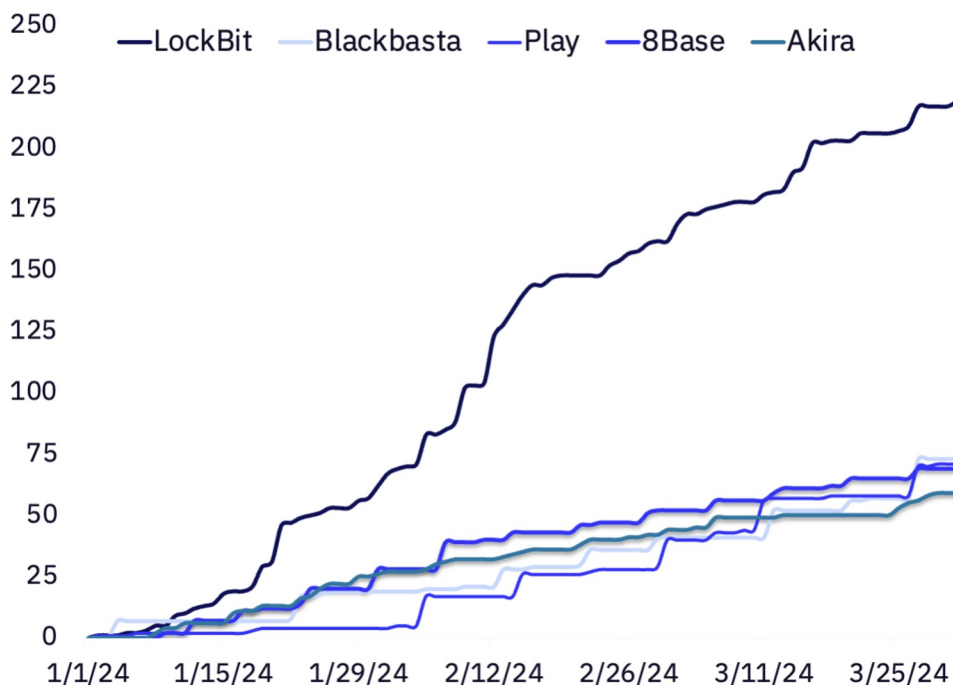
Threat Actor Trends

LOCKBIT - LockBit experienced significant law enforcement disruption during February 2024, but quickly recovered. The group has maintained the top spot among RaaS service operations with 219 victims, but with a lower operational tempo. LockBit claimed an average of 2.96 victims per day before the disruption occurred on February 20th (148 total), and only an average of 1.92 victims per day from February 24th to the end of March (71 total).

BLACKBASTA - Blackbasta started Q1 rather slow with 19 victims in January, but increased their operations throughout February and March with a claimed victims count of 22 and 32, respectively. This is a major increase from Q4 2023, during which Blackbasta claimed only 29 victims.

PLAY - Play's victim count during Q1 2024 (71) is noticeably lower than their Q4 2023 count (113). However, Play still managed to be the third most active ransomware group during Q1 2024. This is impressive when considering Play only claimed four victims during January, demonstrating Play's high operational cadence during the rest of Q1 2024.

Cumulative Victims by Threat Group





Threat Actor Spotlight

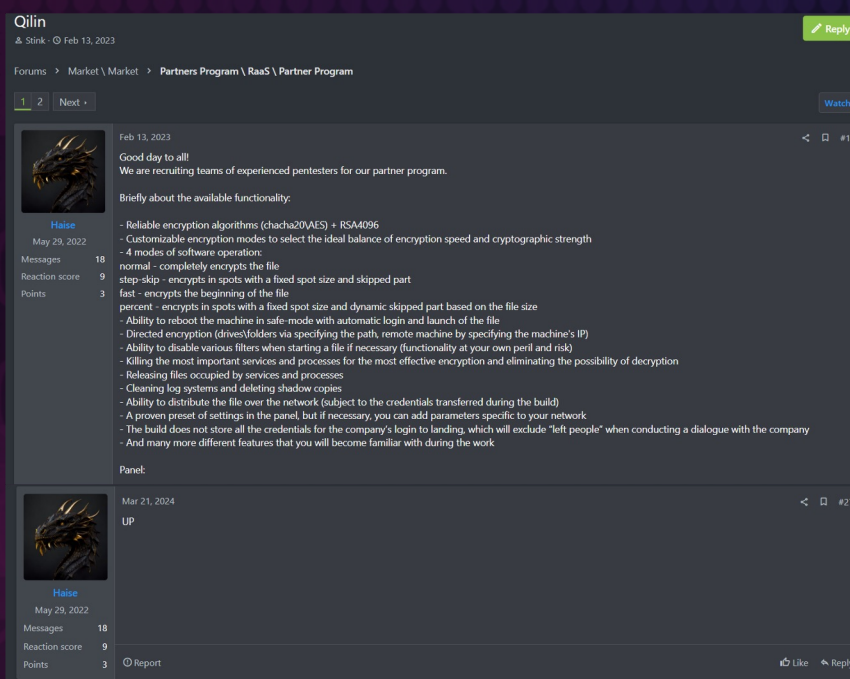
QILIN

QILIN, formerly known as

Agenda, is an Established, double-extortion ransomware group that has been active since at least mid-2022. Ransomware variants associated with the group have been observed "in the wild" as programmed in Rust or GoLang, with Rust variants applying intermittent encryption as a means of defense evasion and increasing the speed of encryption.

The group is on pace to surpass its 44 victims claimed in 2023, having already claimed 34 victims in Q1 of 2024.

Similar to most Established RaaS operations, Qilin's activities disproportionately affect Western organizations or those based in the "global north." Since their first observed operations, 26% of Qilin's victims have been based in the United States, 10% in France, and 7% each in Germany, Italy, Malaysia, Saudi Arabia, and the United Arab Emirates, indicating a worldwide impact. Victims claimed by Qilin have spanned the Agriculture, Fishing, & Forestry; Construction; Engineering; Food & beverage; Banking & Finance; Consulting; Media & Advertising; and Technology industries, among others. On March 21, 2024, we observed a user under the moniker "Haise" promoting Qilin's RaaS affiliate program on the illicit forum RAMP. The post was originally made in February 2023 by Haise but was "bumped" by the actor to gain visibility. The advertisement lists features of the encryption malware, including the ability to partially encrypt files for increased speed. The advertisement fails to list benefits for affiliates, which we would typically expect in such advertisements based on similar posts by RaaS groups during Q1. According to researchers from Group-IB, for payments totaling \$3M or less, affiliates earned 80% of ransom payments; for payments of more than \$3M, affiliates earned 85% of the ransom.



Qilin
Stink · Feb 13, 2023

Forums > Market \ Market > Partners Program \ RaaS \ Partner Program

1 2 Next · Watch

Feb 13, 2023

Good day to all!
We are recruiting teams of experienced pentesters for our partner program.

Briefly about the available functionality:

- Reliable encryption algorithms (chacha20/AES) + RSA4096
- Customizable encryption modes to select the ideal balance of encryption speed and cryptographic strength
- 4 modes of software operation:
 - normal - completely encrypts the file
 - step-skip - encrypts in spots with a fixed spot size and skipped part
 - fast - encrypts the beginning of the file
 - percent - encrypts in spots with a fixed spot size and dynamic-skipped part based on the file size
- Ability to reboot the machine in safe-mode with automatic login and launch of the file
- Directed encryption (drives/folders via specifying the path, remote machine by specifying the machine's IP)
- Ability to disable various filters when starting a file if necessary (functionality at your own peril and risk)
- Killing the most important services and processes for the most effective encryption and eliminating the possibility of decryption
- Releasing files occupied by services and processes
- Clearing log systems and deleting shadow copies
- Ability to distribute the file over the network (subject to the credentials transferred during the build)
- A proven preset of settings in the panel, but if necessary, you can add parameters specific to your network
- The build does not store all the credentials for the company's login to landing, which will exclude "left people" when conducting a dialogue with the company
- And many more different features that you will become familiar with during the work

Panel:

Mar 21, 2024

UP

Report Like Reply

Other Notable Ransomware Events

Ransomware-as-a-Service Recruitment Efforts Observed in Wake of Law Enforcement Operations

In January and February of 2024, GRIT observed efforts by the RaaS groups Medusa, Cloak, and RansomHub to advertise their affiliate programs on deep and dark web forums, likely in an attempt to recruit threat actors to join their affiliate programs. The advertisements coincided with a temporary Law Enforcement disruption of LockBit's operations and an apparent exit scam orchestrated by Alphv, and thus may have been aimed to attract affiliates displaced or disaffected. In the case of Medusa and Cloak, analysis of our available data resulted in no indications of increased operational activity. However, in the case of RansomHub, we have observed potential indicators of increased operational activity.

- Medusa claimed 42 victims in Q4 of 2023, which marginally increased to 45 in Q1 of 2024.
- Cloak's data leak site was dormant from approximately August 28th, 2023, to March 26th, 2024, making assessments of the group's operational cadence difficult. The group has posted 15 victims since the resurgence of their data leak site.
- We observed RansomHub's advertisement for affiliates just one week before the group's data leak site was discovered on February 10th, 2024. As a result, assessments of the group's advertising campaign are difficult to validate. We note that RansomHub has been the 11th most active ransomware group by victim volume during a limited timeframe of February to March, accumulating 22 victims despite its Emerging classification. The group finished March as the fifth-most prolific ransomware group for the month and has continuously updated their advertisement on the illicit forum RAMP. Updates have included notifications on alleged improvements, such as "Rewritten ESXi locker in Golang. Compatibility is strong, Faster," and "Update Bypass 95% AV." GRIT assesses that RansomHub intends to further refine their capabilities and recruit additional affiliates, and, if successful, will impact higher volumes of victims in the near-to-mid term.

GRIT intends to continue monitoring the aforementioned groups for signs of additional capabilities or increased operational tempo, in anticipation of at least some degree of affiliate realignment post-law enforcement disruption.

Bloody But Unbowed: LockBit Stays Alive

In the wake of the group's disruption by law enforcement in February, the future of LockBit, the largest ransomware group tracked by GRIT, very much appeared to be in flux. Despite arrests of several affiliates and seizure of production infrastructure, LockBit leadership was quick to attempt a show of strength in their public statements. In a long and, at times, rambling message posted to a new onion site just days after the takedown, LockBit's administrator, LockBitSupp, gave credit to law enforcement for their work but vowed to rebuild and resume operations as fast as possible. Just four days after the disruption, LockBit had rebuilt a functional data leak site and resumed posting alleged victims.

The question remains as to the long-term effectiveness of Operation Cronos in attempting to shutter the most prolific ransomware group of the modern era. Surface-level analysis of LockBit's victim claims post-disruption appear near baseline, though the group removed several victims after attention was called to several as historical, not new, victims. Since March, LockBit appears to have resumed operations and posting of new victims, claiming 97 in March alone. New impacts on victim organizations, coupled with continuing public communications from the group, suggest that operations have continued unabated, though a deeper analysis suggests that the group may not yet have returned to full strength. LockBit's operations have decreased by over 20% year-over-year, having claimed 219 victims in Q1 2024 and 276 in Q1 2023. While we lack insight into the inner workings of LockBit's daily operations, the most plausible explanation for decreased victim volume in RaaS operations is either a decrease in efficacy or a decrease in the core group's number of affiliates.

The lifeblood of a RaaS operation is the codependent relationship between the group's operators and their affiliates. As GRIT observed in February's Ransomware Report, Operation Cronos targeted LockBit's infrastructure and affiliates not just through direct action but through public statements and information releases likely designed to erode confidence in the group's continued viability and profitability.

Bloody But Unbowed: LockBit Stays Alive (cont'd)

Law enforcement hinted at their awareness of LockBitSupp's identity and indicated that they were able to identify several affiliates based on data held by the core group, factors seemingly designed to raise concerns of future identification and arrest among LockBit affiliates as a result of LockBitSupp's actions or security failures. We assess that more risk-averse or loosely-tied affiliates may seek alternative RaaS groups with which to associate, whether as whole substitutions or as a hedge against future law enforcement disruption. We further assess that reduction in the skill level or volume of LockBit affiliates would degrade the group's operations in the near term.

LockBitSupp has continued to act in ways that suggest instability within LockBit proper. On March 29th, a Tox account associated with LockBitSupp updated their public status to indicate that the group was "looking into violence-as-a-service," or VaaS operations. VaaS is a cybercrime model that connects individuals willing to commit physical acts of violence against targets "in the real world" with those willing to finance and direct such actions. Customers of this type of service range from those seeking revenge for perceived slights to more complex extortion operations, and may range in severity from physical harassment, to assault, or even homicide.

When asked about their public status on the topic of VaaS by researchers at VX-Underground, LockBitSupp iterated that they have no intentions of using VaaS to intimidate victims of ransomware directly, but hinted that recent actions by individuals in the cybercrime community had led them to consider resolution via physical force. We lack insight into the truthfulness of this commentary or any planned use of VaaS by LockBit, whether as a retributive action against perceived adversaries or as an additional extortive lever in future operations. We note that LockBitSupp has long held a reputation for being outspoken and brash, even when interacting with other members of the ransomware community, and that LockBitSupp's statements may point to internal anxiety and instability within the group post-disruption.

The Five Families

"The Five Families" is a cybercrime collective that announced its establishment in August 2023 and has attracted renewed attention in recent weeks based on widespread security reporting of collaboration between two of the component groups. In total, "The Five Families" was allegedly formed with leadership representing five distinct cybercrime and hacktivist groups:

- **ThreatSec**
- **GhostSec**
- **Stormous**
- **BlackForums**
- **SiegedSec**



The group claims to have been created "to establish better unity and connections for everyone in the underground world of the internet, to expand and grow our work and operations."

Recent security reporting on collaboration between Stormous, an extortion or ransomware group, and GhostSec, a nominal hacktivist organization, has brought the group, which primarily communicates to the public via Telegram, to wider attention.

The group's Telegram has primarily been used to amplify the attacks or announcements of its component groups and for occasional announcements about affiliation or non-affiliation with other cybercrime groups. On one occasion, the Telegram was used to sell alleged VPN access to a University in Taiwan and both an Internet Service Provider (ISP) and an Insurance company in the United States.

The Five Families (cont'd)

Primary media attention in recent months has focused on the alleged use of GhostSec's "GhostLocker" ransomware by Stormous, and on a string of worldwide ransomware attacks claimed collaboratively by the groups. Despite the widespread attention, we do not assess that "The Five Families" or its component groups pose a sophisticated or persistent threat to most organizations.

- We note that the reported victims to date are largely small- to medium-sized organizations in the Global South and that there have been no reported GhostLocker attacks against US Organizations. Both Stormous and GhostSec have an established history of embellishment, exaggeration, and fabulism.
- Members of the "Five Families" have frequently ascribed implausible or impossible levels of complexity and impact to their attacks, which have been cited as part of propaganda videos.
- We are unaware of any technical analysis of the alleged ransomware, and have no information on its efficacy beyond statements from the group.

While "hactivist" groups and other "hacker" groups do not represent a sophisticated or well-funded threat to most organizations, their operations can be disruptive or extortive to victims.

- **Most operations claimed by the "Five Families" groups appear to be data breaches rather than attacks**, which were likely the result of misconfigurations, unsecured services, or poor baseline security measures rather than novel or complex intrusion TTPs.
- Members of "The Five Families" have been accused in Telegram channels of posting public breaches as their own, and of relying on "combo lists" of compromised credentials as a primary means of access.

The Five Families (cont'd)

We assess with moderate confidence that "The Five Families" collective does not presently function as founded and declared publicly, and that the name is principally used to amplify the claims and statements of the two remaining active groups: Stormous and GhostSec. Despite the seeming disbandment of the organization "behind the scenes," we note continuing references to the collaboration in security reporting.

- SiegedSec's membership as part of the Five Families was announced on the group's Telegram as "terminated" on December 20th, 2023, based on unspecified "heavily uncomfortable subjects" that had been promoted by SiegedSec.
- BlackForums' administrator announced that they would cease operations in January 2024, eventually turning over the organization to "USDoD," a known threat actor persona. BlackForums rebranded as BlackSec, and later SparrowCorp, and now claims to operate in pursuit of children's safety. We are not aware of any claimed or acknowledged affiliation between SparrowCorp and "The Five Families."
- We are not aware of posts, claims, or operations attributable to ThreatSec since January 2024, following the alleged "doxing"—or public identification—of ThreatSec's leader. Subsequent hearsay indicates that the community believes ThreatSec has, for all intents and purposes, disbanded.

In support of our assessment, we note the primary use of the "Five Families" Telegram channel as amplifying information and attacks attributed to Stormous and/or GhostSec, including the "GhostLocker" ransomware allegedly developed by GhostSec. We do not know whether Stormous and GhostSec currently operate as two truly distinct groups, two groups with overlapping membership, or a single group operating as two personas.

Phobos in Retrograde

On February 29th, 2024, the Cybersecurity and Infrastructure Agency (CISA) and Multi-State Information Sharing and Analysis Center (MS-ISAC) released a Joint Cybersecurity Advisory (JCA) "to disseminate known TTPs and IOCs associated with the Phobos ransomware variants." We have observed and corroborated an apparent increase in Phobos operational activity in Q1, though we lack the quantitative data necessary to understand broader impacts.



Phobos is nominally a RaaS operation, operating since 2019, with access to the Phobos ransomware available at an affordable price point (\$100-\$150) across a number of illicit forums. Phobos may reference several “splinter” groups, and encompasses a number of different “variants” that are classified under the larger Phobos umbrella, including Eight and Elbie. Data exfiltration may or may not occur during Phobos intrusions depending on the operating affiliate responsible. (Note: According to Cisco Talos, Phobos has also been deployed by 8Base, a considerably more prolific group than most Phobos operators, which maintains a data leak site.)

Phobos does not maintain a central data leak site or chat infrastructure, and victim communications most frequently take place over email, with the operating affiliates using “throwaway” accounts with secure email services such as Proton Mail and Onion Mail. Some ransom notes left by affiliates reference the group name or sub-brand, but many do not and remain unnamed. Affiliates demand payment in Bitcoin and promised “deliverables” are generally limited to a decryptor unless otherwise specified by the victim and agreed upon by the threat actor.

Phobos in Retrograde (cont'd)

Observed Phobos encryptors often depend on unique encryption keys for each impacted device or directory, complicating decryption efforts. We have observed limited troubleshooting support and instructions provided by affiliates. Anecdotally, we have observed a higher frequency of re-extortion by Phobos affiliates, with the ransomware affiliate demanding additional payment before providing decryption tools in whole or in part.

In Q1, security researchers announced a new variant of Phobos, dubbed Faust. Security researchers have discovered propagation of the variant via VBA script macros embedded in Microsoft Office documents. When the Office document is opened by a victim, the VBA script initializes and triggers PowerShell, which downloads Base64-encoded data leading to an executable downloader and second-stage file encryption, according to Fortinet. Phobos ransomware intrusions, including those linked to the new Faust variant, primarily depend on phishing or Remote Desktop Protocol (RDP) abuse for initial access, as highlighted in the CISA/MS-ISAC JCA and open-source security reporting. These low-sophistication access methods can be hampered through security best practices, such as the following:

- Microsoft Office macros have been disabled by default since December 2023. Changes to these settings should be alerted on and investigated, and users should be prevented from enabling macros without approval or authorization in advance.
- Flag emails sent from external networks to alert users to apply additional scrutiny.
- Closing RDP Port 3389 unless absolutely necessary for a business purpose. In these instances, providing "just in time" minimal access is recommended.
- Block RDP connections between user devices on-network; this behavior is anomalous of typical users and should be alerted on by organic tooling.



Quarterly Wrap Up

While Q1 2024's figures appear largely unremarkable save for an anticipated increase in victim volume, metrics alone risk obfuscating the impact of substantial law enforcement disruption operations that took place and may shape the ransomware ecosystem for the duration of 2024 and beyond. The LockBit takedown, as described in detail during GRIT's February Ransomware report, has led LockBit administrators to direct affiliates to operate at will against previously off-limits organizations and industries, including hospitals and critical infrastructure. Alphv issues similar "fire-at-will" edicts prior to their exit from the scene, which may leave a vacuum that smaller groups, including Medusa, Cloak, and Ransomhub, could seek to fill. The continued expansion of "acceptable" targets for ransomware groups is more likely to expand than contract in the near term.

So-called "hactivist" and cybercrime groups such as "The Five Families" continue to operate and call attention to their attacks while almost certainly inflating the breadth and depth of their access and capabilities. These groups and their tactics reflect the relatively low barriers to entry in cybercrime and the untrustworthiness of their mouthpieces, but these factors do not negate or cancel out the real-world impacts of data breaches and publicized leaks for everyday citizens who are impacted. While the term "hactivist" has traditionally been used to imply ideological drives and purpose, an objective view of accomplishments by the "Five Families" and the data breached therein reflects opportunistic and indiscrete attacks that may be more accurately described as criminal. Recent pivots by GhostSec to ostensibly embrace extortion and ransomware further reflect the separating line between hactivism and conventional cybercrime blurring with time.



Quarterly Wrap Up (cont'd)

In Q1, 23 distinct Developing, Rebrand, and Established ransomware groups claimed responsibility for 95.5% of observed victim posts. Alternatively, 12 distinct ransomware groups classified as Emerging or Ephemeral accounted for the remaining 2.4% of victim posts, at 25. These numbers demonstrate the continued dominance of ransomware groups that have developed higher operational tempos, greater capabilities, and a commitment to long-term operations, as opposed to more junior or novice groups.

Focusing on the rest of 2024, GRIT expects to see significantly more volatile activity from ransomware operators and groups, as previous norms and guidelines preventing the targeting of critical infrastructure and life-saving organizations fall by the wayside. At least some portion of Emerging and Developing groups stand to maintain a steady increase in operations and become new long-standing Established groups, and may seek to expedite this evolution by recruiting motivated affiliates from competing RaaS organizations.

Appendix: March 2024 in Review

The month of March 2024 marked a significant shift in the number of ransomware victim posts observed. There was a 7.4% increase from February, with the number of posts escalating from 363 to 390. This increase predominantly affected the Technology, Retail and Wholesale, and Financial industries, contributing to 74 of the March victim posts. This represented 18.9% of the total for the month, a noticeable jump from February's 46 posts, which was 12.6% of that month's total.

Conversely, the Healthcare and Legal sectors experienced a welcome decline in posts, with a combined total of 30 victims, down from 53 in the preceding month. Breaking these numbers down, Healthcare saw a decrease from 32 to 20 posts, and Legal incidents were halved from 20 to 10.

Geographically, Germany and Canada experienced the most significant increases, with victim numbers rising by 16 and 14 respectively, culminating in totals of 23 and 27 for March compared to 7 and 13 in February. This contrasted sharply with France, where organizations experienced a significant decrease in ransomware posts—plummeting 79% from 14 in February to a mere 3 in March.

In addition to these fluctuations in ransomware activity, GRIT identified the emergence of three new malicious entities—Killsec, Donex, and Redransomware. These groups were responsible for 22 of the 390 victim posts in March, accounting for approximately 5.6% of the total incidents.



Appendix: GRIT Ransomware Taxonomy

By subdividing ransomware groups, GRIT can obtain more detailed insights into how ransomware groups progress in their level of operational maturity and can classify and identify potential rebranding activity.

We distinguish ransomware groups by placing them into these six categories:

EMERGING

This category is reserved for new ransomware groups within their first three months of operations. These organizations may be short-lived, resulting in an Ephemeral group; may be determined to have Splintered or Rebranded from an Established group; or may move on to further develop their operations and TTPs over time.

EPHEMERAL

These groups are short-lived, with varied but low victim rates. Observed victims are usually posted in a single or short series of large postings rather than a continuous flow over time. Ephemeral groups, by definition, terminate operations, spin-off, or rebrand within three months of formation. These groups may or may not have dedicated infrastructure (i.e., data leak sites and chat support) as part of their operations.

DEVELOPING

These groups have conducted operations for three months or longer, resulting in a recurring flow of victims. Developing groups do not appear to be directly linked to other ransomware groups as a Splinter or Rebrand but may include some experienced ransomware operators. Developing groups generally improve their people, processes, or technology over time by recruiting additional members, refining TTPs, or improving the quality of their associated ransomware and encryption. These groups generally have dedicated infrastructure (i.e., data leak sites and chat support) as part of their operations.

SPLINTER

These groups consist of a plurality of members from previously Developing or Established groups and may have formed either by choice or due to exclusion. These groups may be identified by very similar or overlapping TTPs and tooling or through HUMINT gathered through interactions with personas on the deep and dark web. Splinter groups differ from Rebrands by the continued existence of the original organization as the Splinter group operates.

REBRAND

These groups consist in whole, or in part, of former Developing or Established groups. Rebrands often maintain the same people, processes, and technology as the original group. Rebrands are generally undertaken in order to minimize attention from law enforcement or intelligence officials or to avoid negative publicity.

ESTABLISHED

These groups have operated successfully for at least nine months and have well-defined and consistent tactics, techniques, and procedures. Established groups often possess functional business units that enable sustained ransomware operations, with specialists focused on areas such as personnel, encryption, negotiations, etc. These organizations successfully employ technology and redundant infrastructure to support their operations.

There are multiple routes a group can take through the various classifications, and no one route is standard. While one group may begin as “Ephemeral” and move their way through the ranks to “Full-time,” another group may enter as a “Rebrand” as part of a larger obfuscation strategy to avoid attention from law enforcement.