



GRIT

Ransomware Report

APRIL—JUNE, 2024

Contents



Quarterly Ransomware Summary



June 2024 in Review



Quarterly Ransomware Trends



Taxonomy Breakout



Threat Actor Trends



Threat Actor Spotlight - Play



Industry Spotlight



Quarterly Wrap-up

Methodology

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

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

QUARTERLY



Ransomware Summary

Following an increased pace of observed ransomware operations in Q1 2024, Q2 saw a 9% increase in reported victims relative to Q1 2024; this presents a more modest seasonal adjustment when compared to Q1-Q2 of 2023, in which Q2 numbers increased 37%. We also observed a 9% increase in distinct active ransomware groups between Q1 and Q2, continuing the trend of diffusion of victims between a greater number of seemingly distinct groups. We assess that this increased number of distinct and active groups in Q1 is very likely driven in part by affiliates departing the Alpv and LockBit Ransomware-as-a-Service groups following disruptive multinational law enforcement operations. As such, while we continue to observe increased victim volume over time, we lack sufficient information to assess that increases between Q1 and Q2 are perennial in nature. We have and continue to note a typical increase in operational activity from the first quarter through to the second quarter, possibly influenced by expected decreases in activity over the summer season.

The Technology industry saw increased impacts from ransomware relative to other industries, becoming the second most impacted industry in Q2 2024 with 107 claimed victims, representing its highest relative placement among industries since Q3 2023. The increased impacts on technology organizations have been driven in part by relative newcomers RansomHub and DarkVault, which claimed 18 and 9 victims in the technology industry respectively. Meanwhile, the Manufacturing industry remains the leading industry by observed victim volume - a place it has held, uninterrupted, since Q1 2022.

In this quarterly report, we explore the continued operations of the insular ransomware group Play in our Threat Actor spotlight. Despite being comparatively “quiet” and avoidant of the spotlight in comparison to some of its Established peers, Play has remained one of the most prolific ransomware groups since late 2023, and we assess that its operational tempo will remain consistent in the near term.



QUARTERLY

Ransomware Summary (cont'd)

Later, we turn our attention to RansomHub, a Developing Ransomware-as-a-Service (RaaS) group first observed in February 2024. We explore assessments of the group's provenance, including as a potential rebrand of the now-defunct Knight ransomware group, or as a distinct group that has gained possession of the Knight ransomware source code and recruited veteran affiliates to its RaaS operations.

Finally, we review LockBit's discredited post claiming the United States Federal Reserve as a victim, later revealed to reflect the data of a financial organization. GRIT notes that LockBit has previously misled security researchers with similar antics in the past, including by claiming Fulton County, Georgia and the Federal Bureau of Investigation following earlier Operation Cronos disruptions in February 2024.

Throughout the remainder of this quarterly report, we outline trends, observations, and key takeaways pertaining to observed ransomware operations and events from April – June 2024.

	Q2 2024	Q1 2024	Q2 2023
Total Publicly Posted Ransomware Victims	1,117	1,025	1,177
Active Ransomware Groups	49	45	41
Average Daily Victims	12.3	11.3	12.9

June 2024 in Review

June 2024 presented a notable decrease in observed ransomware victim posts month over month, decreasing by 39.6% from 475 in May to 287 in June. This likely reflects the impacts of Alphv's departure and LockBit's continued degraded operations.

GRIT observed three new ransomware or data extortion groups in June: cicada3301, sensayq, and trinity. These three groups claimed minimal numbers of victims in line with most historical Emerging groups, accounting for 9 of the 287 observed June victim posts, or approximately 3.1%.

For this first time since Q1 2022, the Manufacturing industry fell from its position as the most impacted industry during the month of June 2024. In its place, the Technology industry emerged as the new frontrunner. This shift in impacts could reflect short-term or long-term changes in victimology amidst affiliate realignment as a result of recent law enforcement disruptions, though GRIT assesses that Manufacturing will almost certainly remain among the most impacted industries for the foreseeable future.



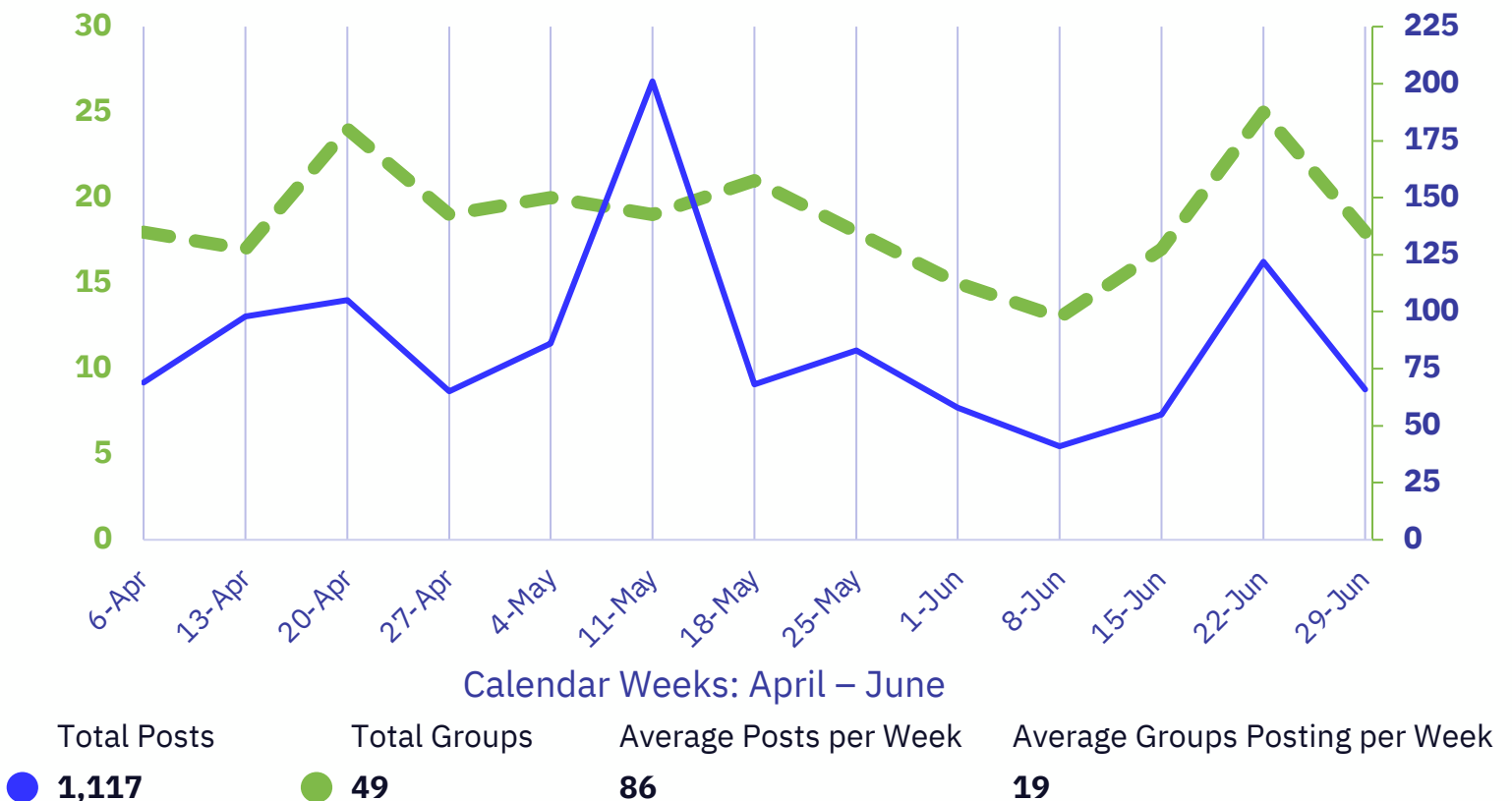
Quarterly Ransomware Trends

Rate of Publicly Posted Ransomware Victims

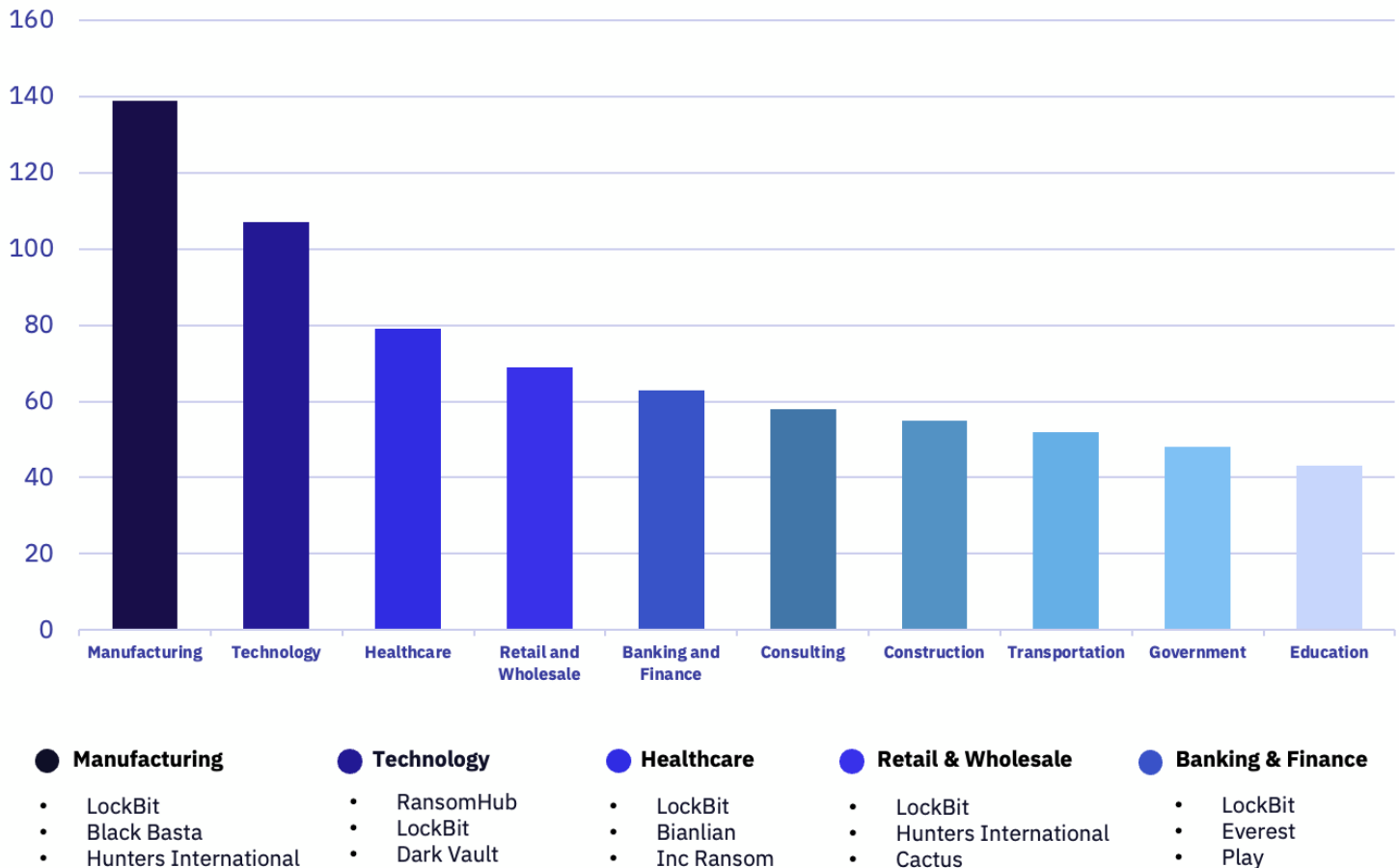
Q2 saw a 9% increase in reported victims relative to Q1 2024; this presents a more modest seasonable adjustment when compared to Q1-Q2 of 2023, in which Q2 numbers increased 37%.

We also observed a 9% increase in distinct active ransomware groups between Q1 and Q2, continuing the trend of diffusion of victims between a greater number of seemingly distinct groups. We assess that this increased number of distinct and active groups in Q1 is very likely driven in part by affiliates departing the Alphv and LockBit Ransomware-as-a-Service groups following disruptive multinational law enforcement operations.

We note that an observable spike during the week of May 11th was driven by LockBit's batch-posting of 76 victims. This event which may have represented the group's clearing of "backlog" victims rather than a temporary substantial surge in operations, as supported by a continuing decrease to the group's operations tempo thereafter. Other groups such as RansomHub and Play, by comparison, have increased their "market share" through June, likely enabled by former Alphv and LockBit affiliates.



Most Impacted Industries, Q2 2024

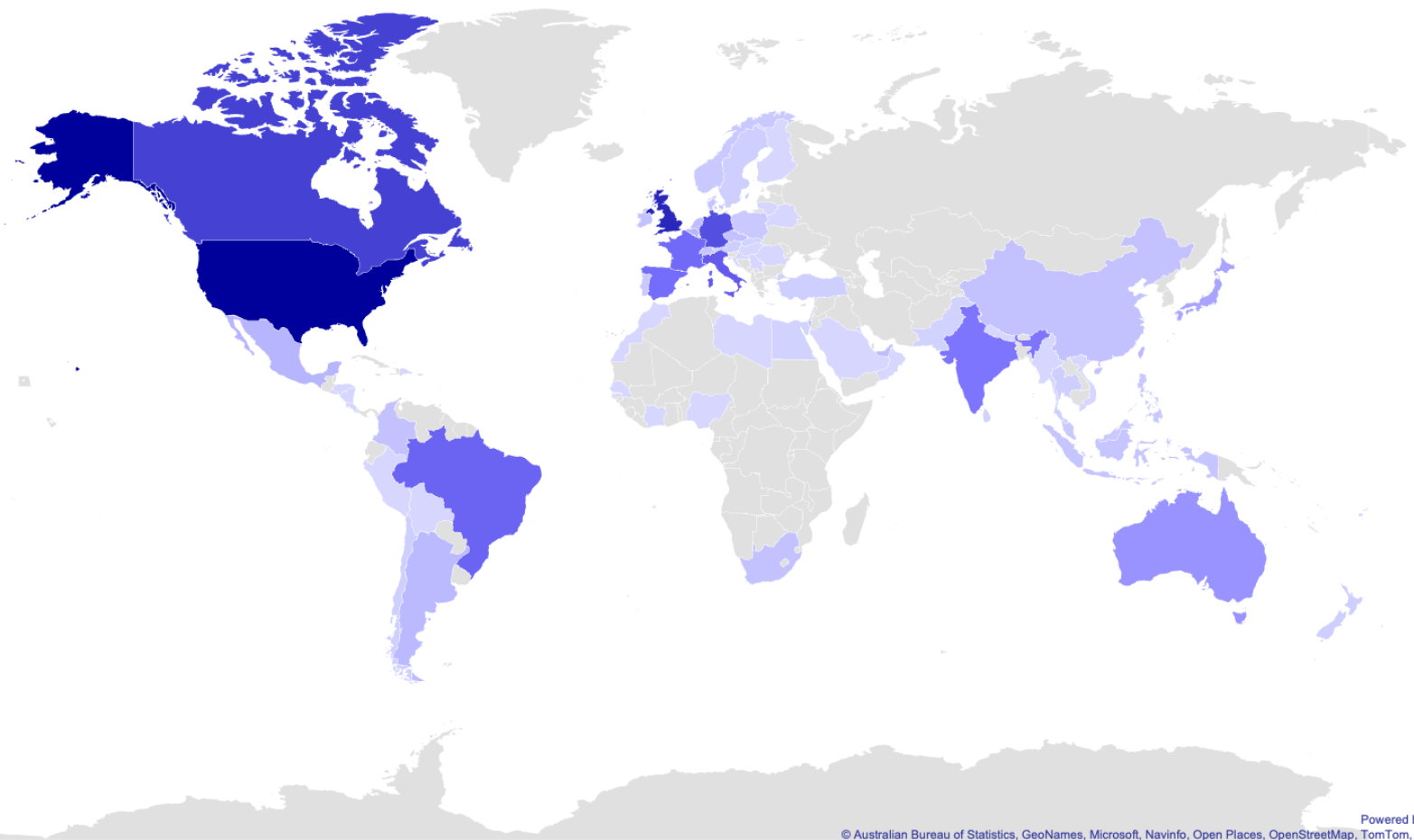


The Technology industry saw increased impacts from ransomware and was the second most impacted industry in Q2 2024 with 107 claimed victims, representing its highest relative placement among industries since Q3 2023. The increased impacts on technology organizations have been driven in part by relative newcomers RansomHub and DarkVault, which claimed 18 and 9 victims within the sector, respectively.

The Legal industry fell from the “top 10” most impacted this quarter after having been consistently present since Q1 2023. This change in impacts is likely driven in part by the disappearance of Alphv and the continued downward trajectory of LockBit, both of which were responsible for the majority of observed victims in the Legal industry through the first half of 2024.

Manufacturing remains the leading industry by observed victim volume, a position it has held uninterrupted since Q1 2022.

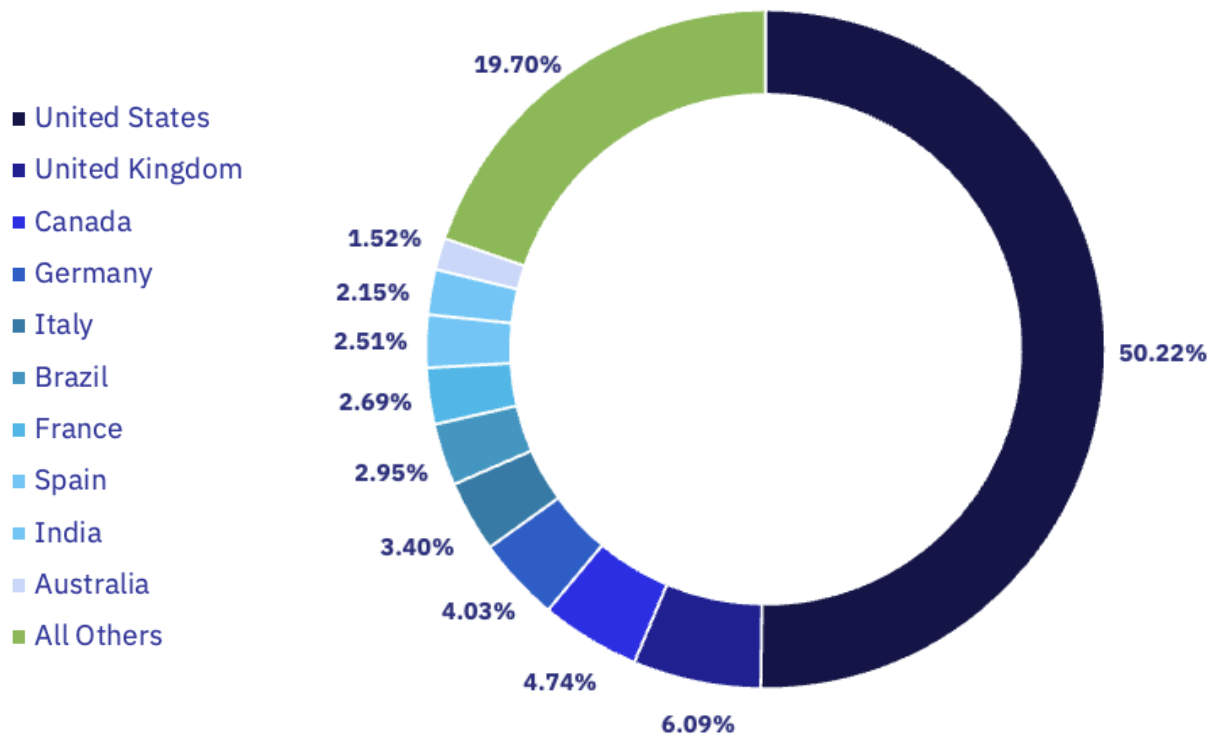
Geographic Breakdown of Ransomware Victims, Q2 2024



Top 10:

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

Observed Ransomware Impacts by Country, Q2 2024



The United States saw a modest increase in total observed victims (561) in Q2 relative to Q1 2024 (537). Despite the quarter-over-quarter increase, the United States' share of total victims fell 2.2% during that same timeframe, illustrating a slight shift of impacts towards non-US countries.

The United Kingdom retains its place as the second most impacted country with 69 victims, or 6.09% of all observed victims in Q2. The UK's share of impacts has remained relatively consistent, and the country has stayed in the number two spot since Q1 2023.

India reentered the top 10 most impacted countries list for the first time since Q3 2023, and Brazil rose to the sixth most impacted country, demonstrating the continued impact of ransomware on emerging economies worldwide.



Taxonomy Breakout

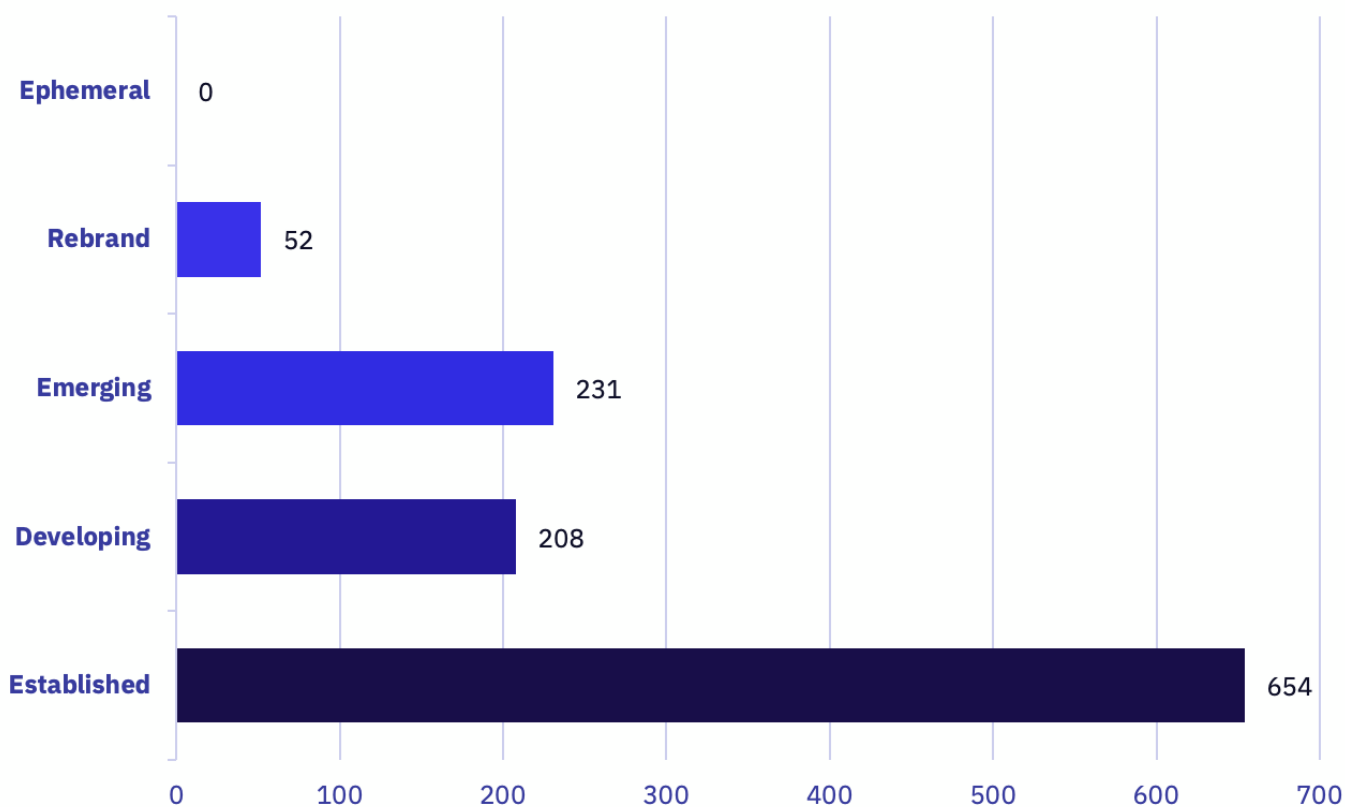
GRIT observed a dramatic increase in the number of victims posted by emerging groups in Q2, correlating with the appearance of 14 new ransomware groups during the same period.

Emerging groups claimed 21% of observed victims in Q2, a marked 6% increase relative to Q1 2024. Concurrently, the number of observed victims we attributed to Established groups fell by total volume and percentage in the same period. We attribute this shift at least in part to the realignment of affiliates following Alphv's exit scam and LockBit's disruption at the hands of Operation Cronos, at least some of which may have joined newer groups or formed their own groups.

Groups classified as Developing accounted for roughly the same level of activity in Q1 and Q2, with a marginal decrease of five observed victims in Q2.

GRIT did not attribute activity to any Ephemeral groups during the quarter, though we note that a number of Emerging groups that arrived late in Q2 may be later classified as Ephemeral following a period of dormancy indicative of short-term operations.

Overall Activity by Taxonomy Classification



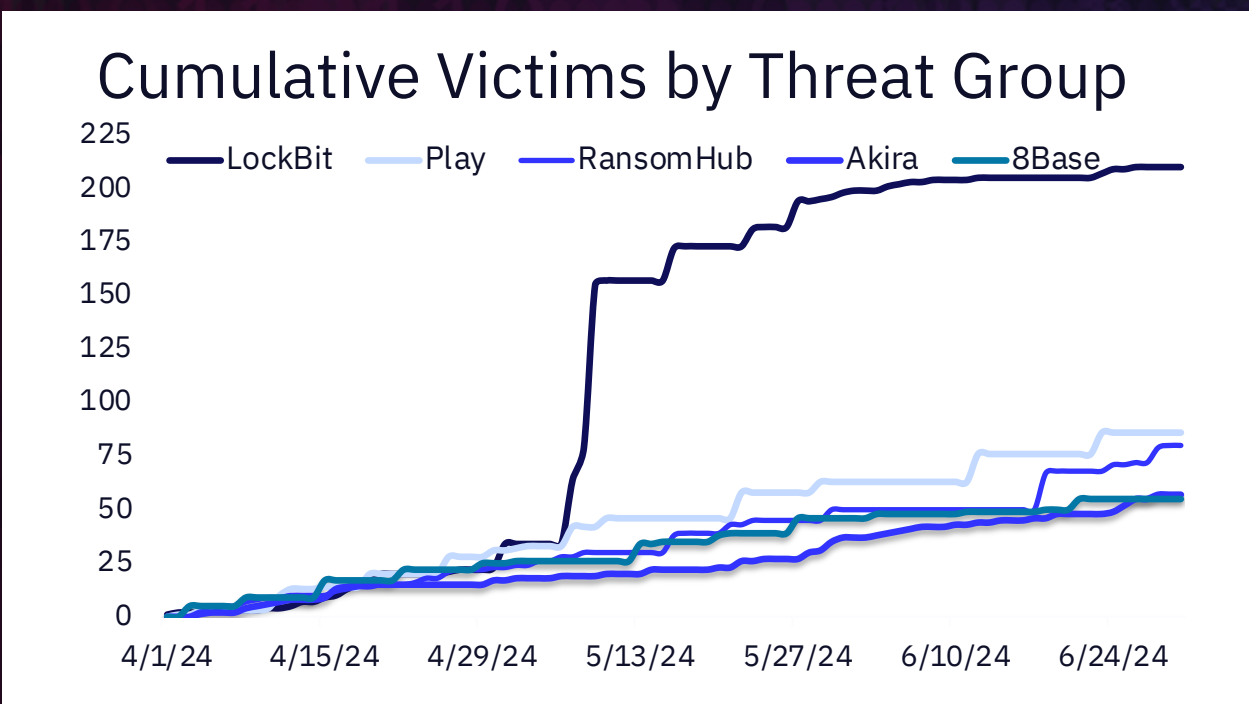


Threat Actor Trends

LOCKBIT In early May, LockBit claimed an apparent “batch” of 76 victims, in what we assess represents a “backlog” clearing in an attempt to demonstrate continued operations rather than a resurgence of the group and its affiliates. This assessment is supported by LockBit’s dramatic drop in operational tempo thereafter, resulting in 55 observed victims across the duration of the quarter. This marks a historically low operational tempo for the group, almost certainly driven by law enforcement disruption operations from Q4 2023 to Q2 2024.

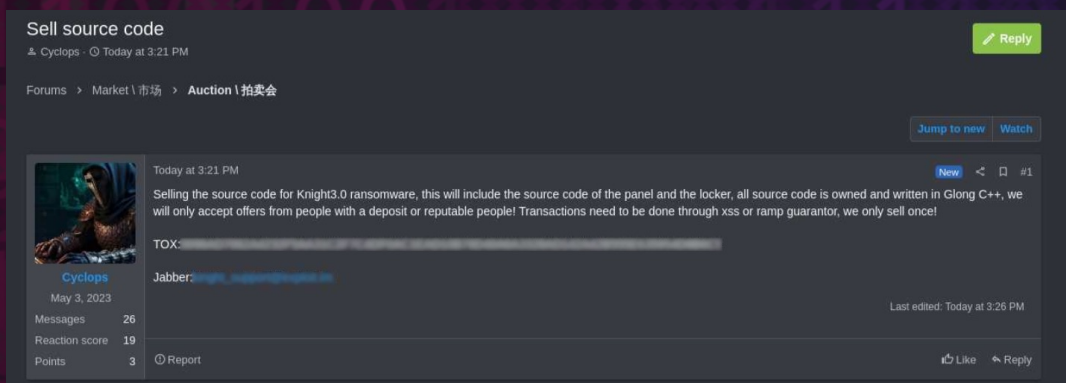
PLAY Despite being “quiet” publicly in comparison to its peers, Play has remained one of the most prolific ransomware groups since late 2023, and we assess that its operational tempo will remain consistent in the near term. We note that Play’s absence of a publicly advertised affiliate program and the group’s high number of claimed victims could indicate a more insular operating structure dependent on experienced operators and trusted referrals.

RansomHub Since emerging in February 2024, RansomHub has risen unusually quickly as one of the most prolific contemporary ransomware groups, capping June 2024 as the most active group by victim volume. The group's aggressive advertising for an affiliate program that favors affiliates, coupled with the alleged successful recruitment of seasoned affiliates from Alphv and other Established groups, has very likely contributed to RansomHub’s ascendance. We note that while RansomHub may have served as an attractive short-term alternative to displaced affiliates, its performance in the long term will serve as a greater indicator of the group’s attractiveness to the wider ransomware affiliate population, particularly as other competing and viable alternatives likely emerge.



Exploring RansomHub's Origin and Rise

RansomHub is a Developing Ransomware-as-a-Service (RaaS) group first observed by GRIT in February 2024. Rapidly increasing its operational tempo, the group has quickly established itself as a significant threat. Analysis by Symantec indicates that RansomHub's strain of ransomware may have originated from the older "Knight" ransomware, based on substantial code overlap between the two. To better understand the origin of the group and its potential similarities with known Tactics, Techniques, and Procedures (TTPs), we opted to delve into RansomHub's potential rebranding from Knight and its swift rise in the ransomware landscape, punctuated by RansomHub's position as the most active ransomware group by victim volume in June 2024.



Source: Bleeping Computer Article/ RAMP Forums

The similarities between Knight and RansomHub source code and operations are notable:

- Both are written in Go and use Gobfuscate (a tool that can compile Go binaries to or from obfuscated source code) for obfuscation.
- Both ransomware families have nearly identical help menus, with RansomHub only adding a sleep command.
- Both employ unique obfuscation techniques, encoding important strings with unique keys, decoded at runtime.
- Both can restart an endpoint in safe mode before starting encryption, a technique previously used by Snatch ransomware.
- Both ransom notes share many similarities, with exact wording in multiple places.
- The method and sequence of command execution are the same, with added execution in the RansomHub version.
- Both groups have implemented double extortion techniques.

Exploring RansomHub's Origin and Rise (cont'd)

The Knight ransomware group, itself a rebrand of Cyclops, allegedly sold its source code based on posts to the illicit forum RAMP in February 2024 after its creators shut down operations. This sale may have led to RansomHub's administrators obtaining and later modifying the Knight ransomware for rebranding and deployment under the RansomHub banner. We lack reporting to indicate any present or continuing relationship between RansomHub and former Knight affiliates.

RansomHub's rapid growth can almost certainly be attributed in part to its aggressive recruitment of experienced affiliates, particularly those displaced from other ransomware groups like Alphv (also known as ALPHV or Blackcat) and LockBit. According to Symantec, "the speed with which RansomHub has established its business and recruited affiliates suggests veteran experience and contacts within the cyber underground." RansomHub is one of several lesser-known RaaS groups that have ramped up recruitment operations in the aftermath of law enforcement disruption operations. As GRIT previously reported, RansomHub has offered generous terms for affiliates in its advertisements on illicit forums, such as a 90% commission on victim payments and direct payment processing for affiliates. These benefits are likely intended to attract affiliates wary of RaaS operations following Alphv's "exit scam" departure.

RansomHub has been successful in attracting former Alphv affiliates, as allegedly evidenced by the migration of an affiliate using the name "notchy," who previously claimed to work under Alphv's affiliate program. After claiming to have been robbed of a \$22 million ransom by Alphv's administrators, "notchy" joined RansomHub, bringing an impacted organization's data with them along with any past experience as an affiliate. This migration of experienced affiliates has likely reduced the amount of time necessary for RansomHub to "hit its stride" in terms of operational tempo and profile of victims.

LockBit's Reserve of Lies

On June 23rd, 2024, the LockBit ransomware group listed the United States Federal Reserve on their Data Leak Site (DLS), with a claim that the group was able to exfiltrate 33TB of data holding “juicy banking information containing Americans’ banking secrets.” The initial post contained no exfiltrated data as proof, only a promise that information would be leaked on June 25th. When additional data was later uploaded, cursory review tied the data not to the Federal Reserve, but a distinct US banking institution. The released data was split into 21 separate hyperlinks; the first link led to a June 14th Press Release made by the Federal Reserve, which issued an enforcement action against Evolve Bank “for deficiencies in the bank's anti-money laundering, risk management, and consumer compliance programs.” Other links provided in the post embedded Evolve Bank's URL within the file hosting URL; as LockBit has historically published the victim's website as the title for their blog posts, the inclusion of Evolve Bank's URL likely indicates that the posted data actually belonged to Evolve Bank. (GRIT has not and does not download or attempt to access the data of unaffiliated victims on ransomware data leak sites).

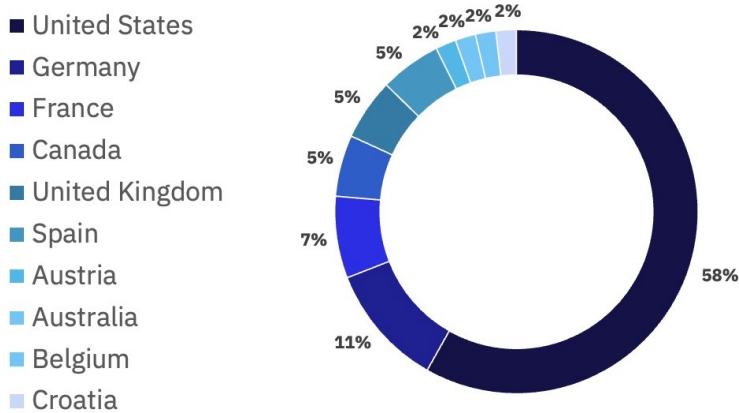
LockBit has misled security researchers with similar antics in the past. In February 2024, LockBit successfully encrypted the network of Fulton County, Georgia, but the group would extend their claim to alleged data exfiltration which the County denied. LockBit set multiple deadlines for the publication of this allegedly exfiltrated data, but ultimately relented without any evidence to support their claims. As we have observed from other ransomware groups, LockBit likely lied about having exfiltrated data in order to conceal an operational failure, coerce a ransom demand, or to attract public attention.

GRIT assesses that LockBit's issuance of false claims about sensitive targets is an attempt by the group to signal continued relevance and efficacy concurrent with declining victim posts and recurrent law enforcement disruption operations. GRIT assesses that LockBit may repeat this tactic in the future in an attempt to project strength and cause panic within private and public sector organizations.

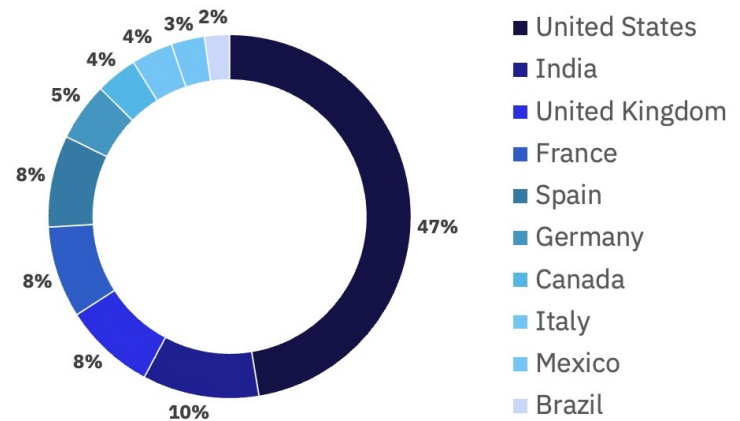
International Encryption

Following the imposition of multinational sanctions against LockBit ransomware's administrator on May 7th, GRIT developed a comprehensive overview of the group's impact on foreign countries based on data leak site information. In seeking to identify relevant patterns, we observed a shift in the proportion of LockBit's attacks from principally impacting US-based organizations towards those in Brazil, Spain, and India.

Lockbit Reports by Country Prior to May 7th



Lockbit Reports by Country After May 7th



Charts displaying LockBit victims by country.

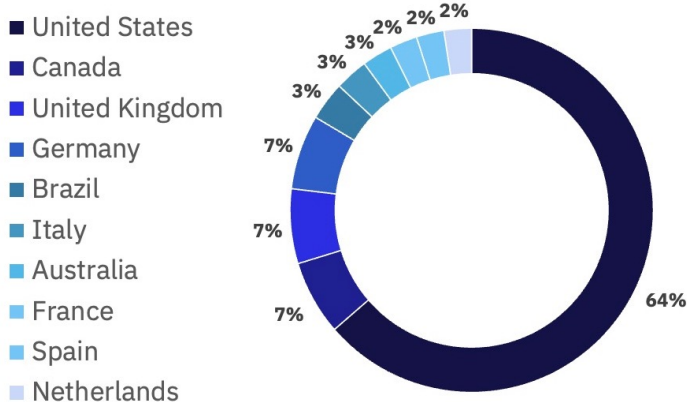
Prior to the U.S. sanctions on May 7th, the United States was LockBit's primary focus, accounting for 56% of the group's ransomware attacks in the 90 days leading up to the sanctions. Post-sanctions, this proportion dropped to 45%, indicating a significant shift in LockBit's targeting strategy. This decrease suggests that the sanctions and subsequent unmasking of Dmitry Yuryevich Khorshev, identified as the primary operator of the LockBitSupp persona and member of the LockBit ransomware group, and his affiliates disrupted their operations and may have deterred their strategic targeting focus on the U.S. The strategic shift is further evidenced by the increased attacks on other countries, particularly Brazil. The data indicates that, while the U.S. remains a significant target, ransomware groups like RansomHub, BlackBasta, and newcomer ArcusMedia are diversifying their attack vectors and regions. Countries like the United Kingdom, France, and Germany also saw considerable numbers of attacks both before and after the sanctions. The targeting of a wider range of countries may be a strategic move to distribute risk and evade international law enforcement efforts.

International Encryption (cont'd)

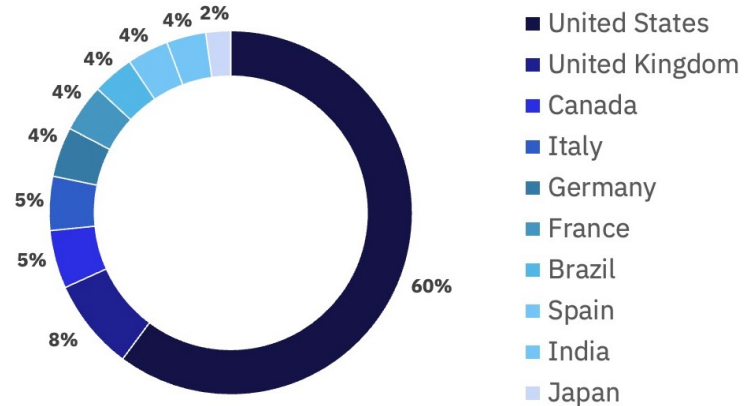
While the impact of U.S. sanctions on LockBit has been significant, the broader landscape of ransomware attacks reveals emerging trends that extend beyond the immediate consequences for the United States. A particularly noteworthy development is the increased focus on Brazil, Spain, and India by various ransomware groups. This trend highlights the shifting dynamics in cybercrime as ransomware actors adapt their strategies to exploit new opportunities and evade enhanced security measures in traditional target regions.

In the wake of these strategic shifts, Brazil has emerged as a prominent target for ransomware attacks, reflecting a broader trend of cybercriminals targeting regions undergoing rapid economic and technological growth.

Reports by Country Prior to May 7th



Reports by Country After May 7th



Charts displaying victims by country before and after May 7th, ransomware group agnostic.

GRIT observed a significant increase in claimed ransomware victims located in Brazil, moving from tied for 7th place to 5th in the ranking of most impacted countries from April to May of 2024, and a fall to joint 7th in June of 2024 again. Reports per day for Brazil increased from 0.229 in the six-month period from September 2023 to February 2024, to 0.363 in the last three months (April 2024 to the end of June 2024). This uptick can be attributed to Brazil's growing digital infrastructure and economic development, making it an attractive target for ransomware groups seeking new opportunities.

International Encryption (cont'd)

Brazil has emerged as one of the top countries impacted by ransomware, most likely becoming a victim of its economic success and burgeoning tech sector. The country's economic landscape is marked by substantial investments in technology, innovation, and digital transformation. Major cities like São Paulo and Rio de Janeiro are rapidly becoming tech hubs, attracting startups and multinational corporations. The rapid digitalization of services, expansion of internet connectivity, and proliferation of smart devices have created a fertile ground for cybercriminals looking to exploit vulnerabilities in new and expanding networks.

Brazil was impacted by 11 unique ransomware groups during Q2, emphasizing the diverse and persistent threat landscape facing the country. The increased number of Brazilian victims aligns with the global trend of cybercriminals shifting focus towards regions experiencing rapid technological growth and digital transformation. The following points highlight Brazil's attractiveness as a target:

- Brazil's rapidly growing economy, particularly in the tech sector, presents lucrative opportunities for cybercriminals seeking ransom payments from financially stable organizations.
- The extensive digitalization of services and infrastructure increases the potential attack surface for ransomware groups.
- As Brazil continues to expand its digital infrastructure and, thus, their attack surface, there may be inherent vulnerabilities that cybercriminals can exploit.

While Brazil has clearly become an attractive target for ransomware groups, similar trends can also be observed in Spain and India, albeit with some differences in context and magnitude.

Spain has been undergoing a significant digital transformation, with substantial investments in digital infrastructure, smart cities, and technology-driven industries. Major cities like Barcelona and Madrid are recognized for their smart city initiatives, integrating IoT, AI, and other advanced technologies into urban planning and services.

International Encryption (cont'd)

Spain hosts several technology hubs, innovation centers, and multiple global technology conferences and summits, all of which attract both startups and established tech companies. These hubs inherently increase the attack surface for cybercriminals. Additionally, Spain has shown steady economic growth over recent years, recovering from past economic crises and making significant strides in sectors like tourism, renewable energy, and technology.

India, like Spain and Brazil, is globally recognized for its robust IT sector, with cities like Bangalore, Hyderabad, and Pune being major IT hubs. This sector is a significant contributor to the country's GDP and a major driver of employment. The government's Digital India initiative aims to enhance online infrastructure, increase internet connectivity, and make the country digitally empowered. The Smart Cities Mission is an urban renewal and retrofitting program aimed at developing smart cities across the country, incorporating modern technology in urban development. Additionally, India has one of the fastest-growing economies in the world, with significant growth in sectors such as technology, manufacturing, and services. There has been substantial investment in infrastructure, including digital infrastructure, making India an attractive target for cybercriminals looking for vulnerabilities in rapidly expanding systems.

Like Brazil, both Spain and India have seen significant economic growth and technological advancements, which have made them attractive targets for ransomware attacks. The expansion of digital infrastructure and the proliferation of smart technologies in these countries increase the potential attack surface for ransomware groups. Companies in these countries are perceived to have the financial capability to pay ransoms, making them lucrative targets for cybercriminals.

While Brazil has seen a particularly sharp increase in ransomware attacks post-U.S. sanctions, the increase in Spain and India, though notable, has not been as dramatic. The specific nature and tactics of ransomware attacks may vary, with different groups targeting different sectors within each country based on perceived vulnerabilities and potential payoffs. It's worth noting, however, that the full extent of the follow-on effects of the sanctions may not be apparent for several months to a year.

International Encryption (cont'd)

Additionally, data trends from Spain and India indicated by data from April 1, 2024, to June 30, 2024, provide insights into the specific activities of ransomware groups across these countries:

Spain:

- Pre-Sanctions: Spain experienced consistent attacks from groups such as LockBit and Cactus.
- Post-Sanctions: The number of attacks on Spain remained steady, with notable activity from RansomHub and BlackBasta. The overall trend indicates a sustained level of attacks, with Spain ranking consistently high among targeted countries.
 - Moderate increase in post-sanction activity, indicating steady targeting.

India:

- Pre-Sanctions: India was impacted by several groups, including DarkVault and KillSecurity.
- Post-Sanctions: The frequency of attacks increased, with LockBit being particularly active. Other groups like DarkVault and RansomHub also impacted India, indicating a persistent and growing threat landscape.
 - A noticeable increase in the number of incidents post-sanctions.

Overall, the combination of economic growth, technological advancement, and expanding digital infrastructure makes Brazil an increasingly attractive target for ransomware attacks. This trend is also representative of the affects being seen in India and Spain as well. These countries' rise in the ranking of most impacted nations underscores the need for robust cybersecurity measures and international cooperation to mitigate the threat posed by ransomware groups.



Threat Actor Spotlight

PLAY

Threat Actor Spotlight: Play

PLAY NEWS

CONTACT

FAQ

PLAY FAQ

- What happened?

- We infiltrated your network, thoroughly investigated, stole all important, personal, private, compromising information, including databases and all documents valuable to you, encrypted your data, making them inaccessible for use.

- How can i get my organization back to normal?

- The first thing you need to do is leave your contact in the feedback form, after that we will contact you and discuss the terms of the deal.

Deal scenario:

1. You send several small files for decryption, we decrypt them and send it back to you, thus proving our technical ability to decrypt your network.
2. Right before payment, you must again send several small files for decryption, after receiving the decrypted files, you pay the price we indicated to our wallet.
3. Within a one hour after receiving the payment, we permanently delete your files from our storage, and send you a decryptor* with detailed instructions.
4. You decrypt your systems, and return to normal operation.

*The speed of the PLAY Decryptor is comparable to the speed of the PLAY, also, if during the encryption process you urgently de-energized your network, this will not affect decryption, PLAY Decryptor uses the validation of encrypted sections.

- How can i trust you?

- We monitor our reputation. We are not an affiliate program, this guarantees the secrecy of deals, there are no third parties who decide to do otherwise than their affiliate partners.

Play is an Established double-extortion ransomware group that has been active since at least June 2022. The group claims to not operate as a Ransomware-as-a-Service group, as supported by a message on their data leak site stating, "Play ransomware HAS NEVER PROVIDED AND DOES NOT PROVIDE THE RaaS." The inclusion of this statement is likely in response to late-2023 reporting alleging the group's ransomware being distributed as-a-service, based on nearly identical TTPs across multiple operations. GRIT respectfully dissents from the late-2023 reports and notes that the presence of highly similar TTPs would be more likely to indicate an insular group of operators than highly decentralized RaaS operations. Further, in a December 2023 Joint Cybersecurity Advisory, CISA, the FBI, and Australian federal agencies noted that Play is "presumed to be a closed group."

Threat Actor Spotlight: Play

Play's alleged non-RaaS operating model makes it an outlier among prolific ransomware groups, many of which depend on high volumes of affiliates to achieve a comparably high number of successful attacks. Late-2023 reporting of nearly identically sequenced attack patterns in Play operations could indicate highly standardized "playbooks" that enabled attacks to scale even with lower numbers of insular operators.

Play is believed to have originated with members of the Hive and Nokoyawa ransomware groups, as noted by Trend Micro; Tactics Techniques and Procedures (TTPs) demonstrated by Play ransomware operators have overlapped with those of historical Hive and Nokoyawa attacks. The group has also demonstrated novel and distinct TTPs, including its use of the active directory query tool, AdFind.

Play's operational tempo has seemingly increased since Q3 2023 when it first emerged as one of the "top three" most impactful ransomware groups, continuing through its most recent place as the second most impactful group in June 2024. We note that Play's observed victims are almost entirely based in the United States and, to a much lesser extent, Canada and western Europe, accounting for 93% of Play's victims in Q2. Manufacturing and Construction, industries that have historically been highly sensitive to operational disruption caused by ransomware, also represent the two industries most frequently impacted by the group, accounting for 22% of Play's observed victims in Q2.



Industry Spotlight

TECHNOLOGY

Industry Spotlight: Technology

This quarter's Industry Spotlight highlights the recent increase in observed ransomware attacks impacting organizations within the Technology industry. Tech companies have always been a target of ransomware gangs, particularly those that emphasize data exfiltration and data extortion. A majority of organizations in the Technology industry depend upon the development and protection of intellectual property, sensitive data, and service availability, all of which have been effectively disrupted by contemporary ransomware operations.

In Q2 2024, 107 victims in the Technology sector were posted to ransomware data leak sites, second only to Manufacturing with 139. The Technology sector made up 9.6% of the total posted victims in Q2 vs a 7.8% share in Q1; However, we note that while the share of victims from technology organizations increased, the absolute number decreased from Q1 to Q2. This shift to a greater share of observed victims may be driven in part by the realignment of affiliates to new groups following the disruption and exit of LockBit and Alphv respectively and continues a recent trend of higher impacts on the industry.

Ransomware groups are not the sole cyber threat actors impacting the Technology industry disproportionately. Other cybercriminals are also focused on compromising Technology company source code repositories to later sell the code on illicit marketplaces or bolster their reputation in illicit forums and communities.

Industry Spotlight: Technology (cont'd)

Other industries, such as Manufacturing and Construction, suffer at the hands of ransomware groups due to impacts on the availability of IT networks, resulting in degraded operations and the subsequent financial costs from lost production. By comparison, Technology companies often feature no exploitable assembly lines or production facilities, with ransomware impacts targeting the confidentiality of sensitive data or integrity of sensitive source code, which could support downstream supply chain attacks if effectively compromised. Technology companies are often expected to maintain near-perpetual availability, resulting in financial and reputational impacts for even incomplete or temporary disruption from ransomware attacks.

Take, for example, a recent high-profile ransomware attack allegedly carried out by BlackSuit and impacting a multinational automotive technology company; The attack left the automotive software company's services unavailable to car dealerships nationwide. Without the ability to process sales, service requests, and other transactions, many of these third parties were left unable to do business as the result of the downtime of a single software provider. The victim organization faced immense pressure to restore services, despite their exemplary transparency and the provision of near-daily updates on restoration progress, all of which can be expected and leveraged by ransomware actors as coercive leverage to encourage compliance. Facing pressure to quickly restore not just internal operations but the downstream operations of their customers, Technology organizations may face above-average pressure to pay ransomware groups as a business and financial decision. In the wake of potentially successful or highly visible public disruption from ransomware operations, we may expect to see imitation and increased targeting by other ransomware groups hoping to attract similar attention and cause similar levels of disruption.



Quarterly Wrap Up

While Q2 looks relatively indistinct by comparison from a quarter-over-quarter and year-over-year perspective, major shakeups continue to unfold amidst the greater ransomware ecosystem. LockBit's takedown and Alphv's "exit scam" have shown signs of significant impacts on adjacent RaaS groups which will likely continue to play out through the end of 2024. Law enforcement's disruption of LockBit, as described in detail during GRIT's [February](#) and [April](#) Ransomware reports, has almost certainly driven a massive decrease in the number of impacted victims claimed by affiliates of the group since May, accompanied by the concurrent ascendancy of RansomHub to the "top" of the current ecosystem. As evidenced throughout this report, the vacuum left by departures and disruption of the most prolific ransomware groups has also potentially led to the expansion of targets and industries deemed "acceptable" for groups to target, an aspect that we assess is more likely to continue to expand rather than contract.

Curiously, the power vacuum generated by Alphv's departure and LockBit's disruption has seemingly been filled by aggressive recruiting by relative newcomers RansomHub, as previously reported by GRIT. This potential Knight rebrand is leading the ransomware ecosystem into the post-Alphv, and potentially post-LockBit, "new normal." Additionally, we're seeing continued threats from persistent, and quieter, ransomware groups such as Play, which are in some cases increasing operations.

In Q2 we observed changes to the distribution of impacted countries, shifting slightly from heavily U.S.-focused to more widespread across the globe, with Brazil, Spain, and India becoming mainstays in the top impacted countries. The shift is exemplified by Brazil's swift rise toward the middle of the rankings compared to other countries starting as early as February of 2024, and remaining consistent throughout Q2. The increase in Brazilian ransomware victims could potentially be a result of its budding economy and booming technology sector creating a target-rich environment.

Focusing on the rest of 2024, GRIT expects to see significantly more volatile activity from ransomware operators and groups, as previous norms fall by the wayside in the wake of LockBit and AlphV's disruption and destruction, and new groups emerge as leaders in ransomware. 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 will likely seek to expedite this evolution by recruiting motivated affiliates from competing RaaS organizations.