GUIDEPOINT SECURITY

GRIT Ransomware Report

2023 ANNUAL REPORT

Contents


Annual Ransomware Summary


2023 Ransomware Activity
“by the numbers”


2023 Threat Group Breakdown


Ransomware in Depth: Major Events,
Observations, and Trends in 2023


Signposts of Ransomware Activity
and 2024 Outlook


Final Thoughts


Appendix

Methodology

Data collected for this report was obtained from publicly available resources, including information disclosed by threat groups themselves, and has not been validated by all alleged victims. As such, 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 or will remove posted details of the victims once a ransom has been paid. Additionally, some groups include incomplete information about their victim or claim an attack despite having successfully attacked 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 this variability, we still consider this report as an accurate representation of the 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.

In keeping with best practices in analytic tradecraft, we have we have made efforts to clearly distinguish between our assessments and the underlying factual evidence which supports it. Statements beginning with or containing the words “we assess” should be considered analytic judgments based on the expertise and experience of GRIT’s analysts coupled with the strength and corroboration of underlying sources. Statements of probability – such as “likely,” “almost certainly,” and “probably” reflect levels of confidence in an analytic assessment based on the strength and corroboration of underlying sources. “Unlikely” and similar terms reflect low confidence, “likely” and “probably” reflect moderate confidence, and “almost certainly” reflect high confidence within the scope of this report.

ANNUAL Ransomware Summary

In last year's Annual Ransomware Report, GRIT identified ransomware as "the most prolific and impactful threat to our networks, data, and operational capabilities," with more than 2,500 publicly posted victims observed in 2022. While we predicted a continuing steady increase in ransomware activity, 2023 outpaced our expectations, with year-over-year victim volume nearly doubling, driven in part by multiple mass exploitation campaigns impacting hundreds of organizations. In total, we observed 63 distinct ransomware groups leverage encryption, data exfiltration, data extortion, and other novel tactics to compromise and publicly post 4,519 victims across all 30 of GRIT's tracked industries, and in 120 countries.

Relative to the remainder of the year, Ransomware's operational tempo in 2023 began slowly, with a progressive increase in victim posting building up to a record high of 1,353 victim posts in Q3, followed by a comparatively mild 1,170 victim posts in Q4. As Q4's drop-off does not appear to correlate with any significant changes in the ransomware ecosystem, results from January 2024 may yet show whether victim volume will decrease, remain constant, or return to form by increasing in the new year.

Key Highlights

The United States was by far the most impacted country in 2023. Among posted victims, 2,199 were US-based organizations, accounting for 49% of all observed ransomware attacks in 2023. Eight out of the ten most impacted countries were within North America and Europe, with Brazil and Australia as the sole outliers. The same "top ten" most impacted countries were home to 76% of all observed victim organizations, of which 27% impacted non-US countries.

From an industry perspective, GRIT observed most impacts affecting a limited subset of industries. 62% of all observed victims belong to one of the "top ten" most-impacted industries, with Manufacturing and Technology remaining the two most-impacted industries; Manufacturing and Technology represented 12.9% and 7.9% of all victims, respectively.

In line with GRIT's taxonomy for classifying ransomware groups, long-term Established groups accounted for the overwhelming majority of observed victims (85%), followed by Developing groups (10%). Ephemeral and Emerging groups, as the newest and shortest-term entrants, lagged behind their maturing counterparts but still posed a significant threat to worldwide organizations, exacerbated by less "reliable" actors and frequently recycled malware. We note that for 2023, we have attributed only one Rebrand group in Black Suit, stemming from the now inactive Established group, Royal. Conversely, we have not definitively attributed any Splinter groups in 2023, though groups that we currently classify as Emerging or Ephemeral may, in time, show indications of having Splintered from other organizations.

ANNUAL Ransomware Summary (cont'd)

Tactically, 2023 presented repeated opportunities for new entrants in the ransomware ecosystem. This was achieved either through reduced technical barriers such as the recycling of leaked ransomware builders and commodity malware, or the recycling of previously leaked data for re-extortion and claims of attacks that never were. For those established groups with resources and technical expertise, exploitation of high-severity and zero-day vulnerabilities provided a reliable means of exploiting victims at scale, a trend we assess as likely to continue into 2024 as a means of overcoming improvements in security.

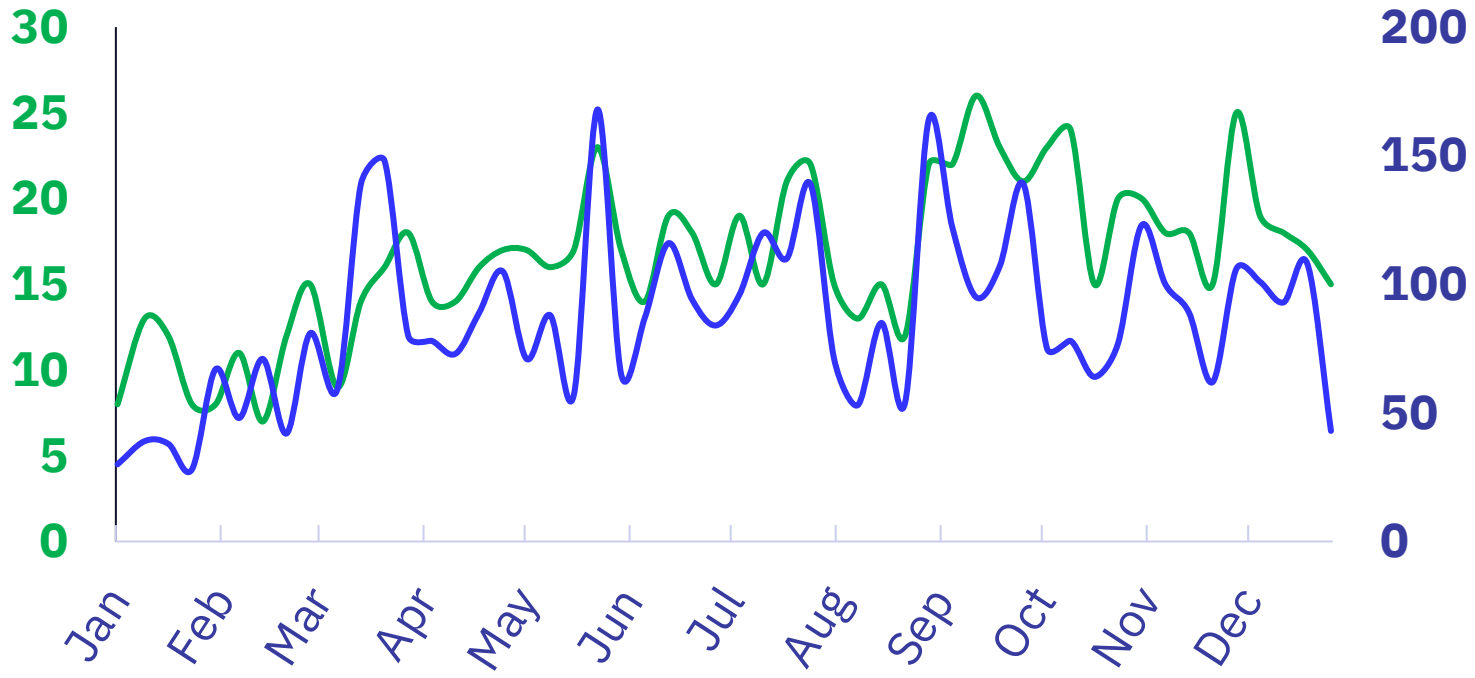
Law enforcement disruptions and rumors thereof circulated the ransomware community in 2023, culminating in a highly publicized takedown of Alphv's dark web leak site. Regrettably, Alphv chose not to go down without a fight, and its continued presence and operations highlight the resiliency of Ransomware's most entrenched groups. Targeting of victims previously considered "off limits", such as schools and hospitals, is expected to continue, as are attempts to attract additional attention to high-impact ransomware attacks. This brinksmanship, which aligns with several of the novel coercive techniques we observed in 2023, will likely attract the attention of both law enforcement and potential affiliates over time.

Total Publicly Posted Ransomware Victims	**4,519**
Number of Tracked Ransomware Groups	63
Average Posting Rate (per day)	12.4

2023 Ransomware Activity by the Numbers

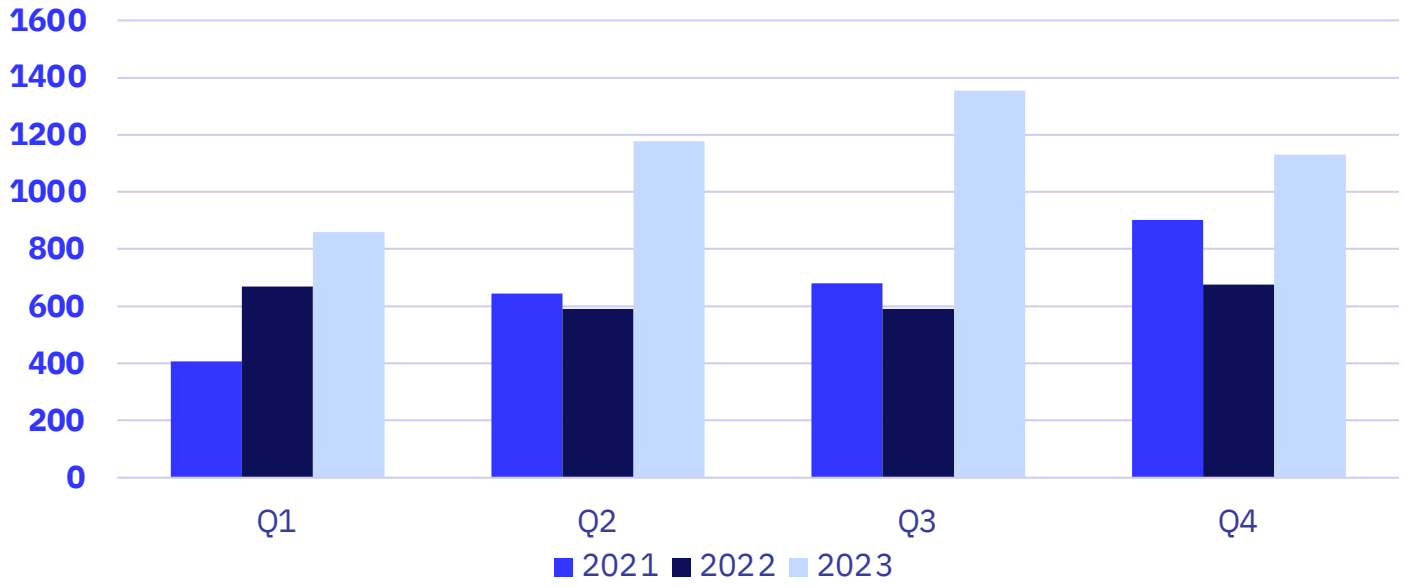
Activity ramped up considerably throughout Q1 into Q2, then held steady at around 100-140 posted victims per week for the remainder of 2023, with the exception of observable decreases in early August and October. An observable increase in victim volume in early September stems from a large "dump" of victim postings by the groups RansomedVC and Cactus.

Substantial increases in victim volume can be observed in March, June, and July following Clop's mass exploitation campaigns that impacted enterprise users of two distinct managed file transfer applications.

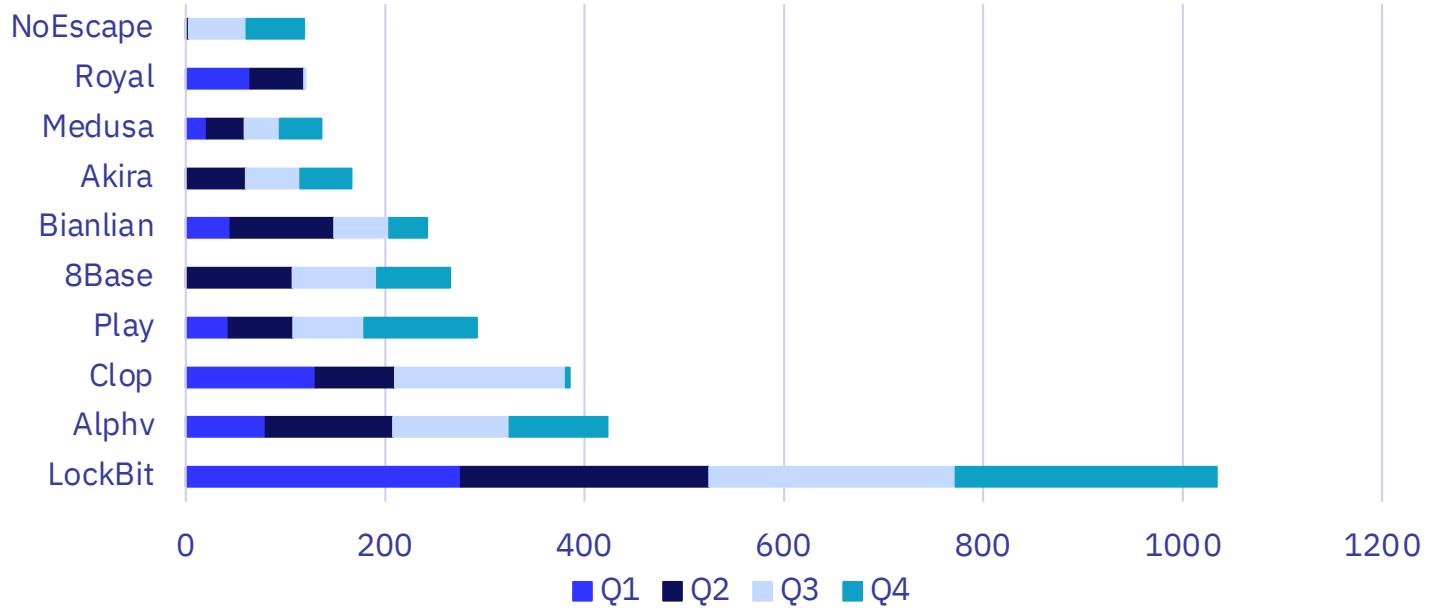


Total Posts	Average Posts / Week	Total Groups	Average Groups / Week
4,519	86.9	63	16.6

Victim Posting Rates per Quarter



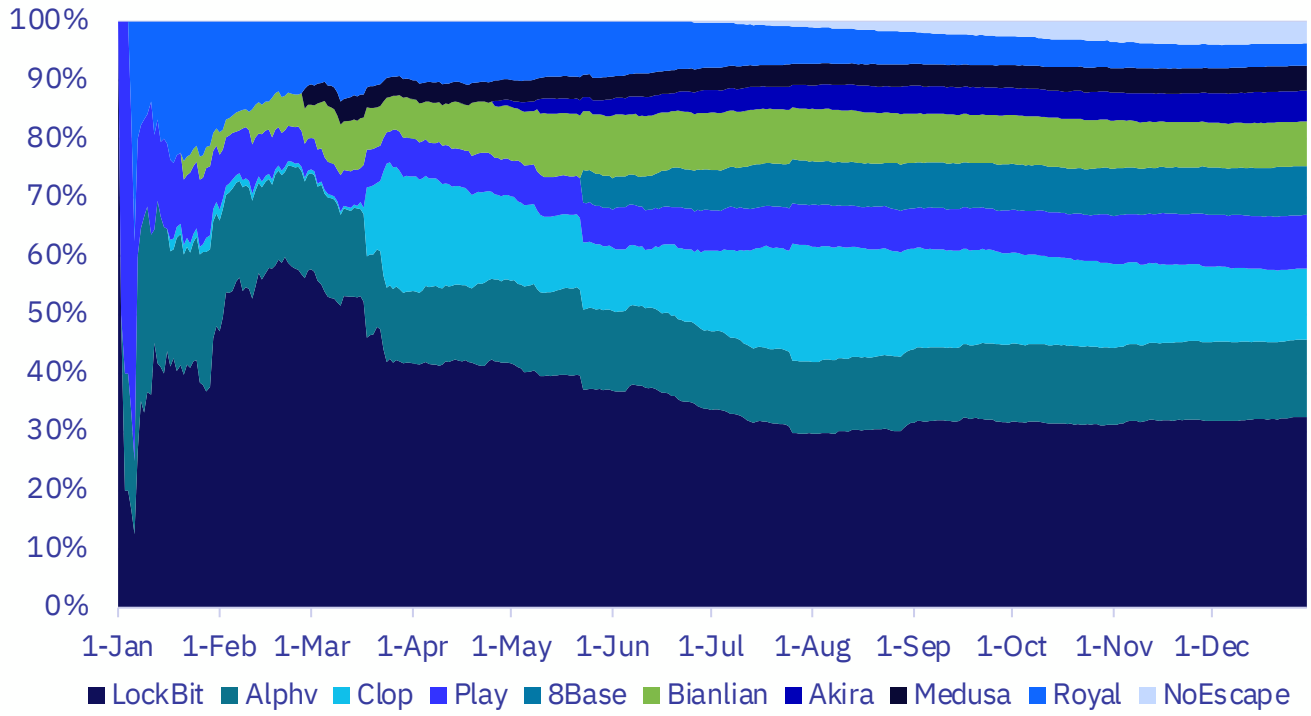
Most Impactful Ransomware Threat Groups - 2023



A quarterly breakdown of 2023's data shows a consistent and significant uptick in the volume of victims posted relative to the two preceding years. Emblematic of this increase, Q3 of 2023 resulted in a higher volume of victim postings than the Q3 totals of 2021 and 2022 combined.

The rate of publicly posted ransomware victims from 2021 to 2022 saw a 4.2% decrease in activity year over year. Comparatively, from 2022 to 2023, ransomware victim posting increased by a staggering 80.1%. While mass exploitation campaigns contributed substantially to this large increase, such attacks contributed just over 5% of the total victims for 2023, demonstrating this year's significant increase in ransomware activity overall.

Cumulative Victims by Threat Group - 2023



Following a slow close to 2022, LockBit's activity surged considerably in the first quarter of 2023, and the group maintained a steady pace of operations throughout the year, even during periods when other groups were far less active. GRIT observed a slower summer from LockBit compared to their average, possibly indicating conflicts with affiliates, processes, or or infrastructure, consistent with problems described in open security reporting. This may have contributed to LockBit's announcement in November, in which LockBit publicized a "policy" change that indicated the minimum acceptable ransom demand would be directly related to the victim organization revenue. Additionally, on November 15th, 2023, LockBit suffered an outage affecting all of it's known Dark Web infrastructure. The issue was resolved later that day, with no indications as to what caused the outage.

Including Clop's mass exploitation campaigns and the May 2023 bulk posting of victims by 8Base, LockBit's share among the "top 10" settled at 32% for the remainder of the year.

The Established group Royal began the year with a high and consistent volume of victims before a precipitous drop in Q3, when their leak site went dark. The group is believed to have since Rebranded as "Black Suit", which began continuing operations in Q4.

Play, a group responsible for only around 1% of observed victims in 2022, quietly and significantly increased their operations to become the fourth-most prolific group in 2023, in terms of observed victims.

GRIT observed the 6th- and 7th-most victims from Bianlian and Akira, despite the publication of ransomware decryptors which would degrade the effectiveness of encryption as leverage. Both groups appear to have quickly pivoted to extortion based solely on exfiltrated data and have maintained a significant operational capacity.

While retaining its place as the second-most impactful ransomware group, Alphv earned significant media coverage this Fall after claiming breaches against MGM Resorts and Caesars International through an elaborate social engineering campaign conducted by the prominent threat group, Scattered Spider.

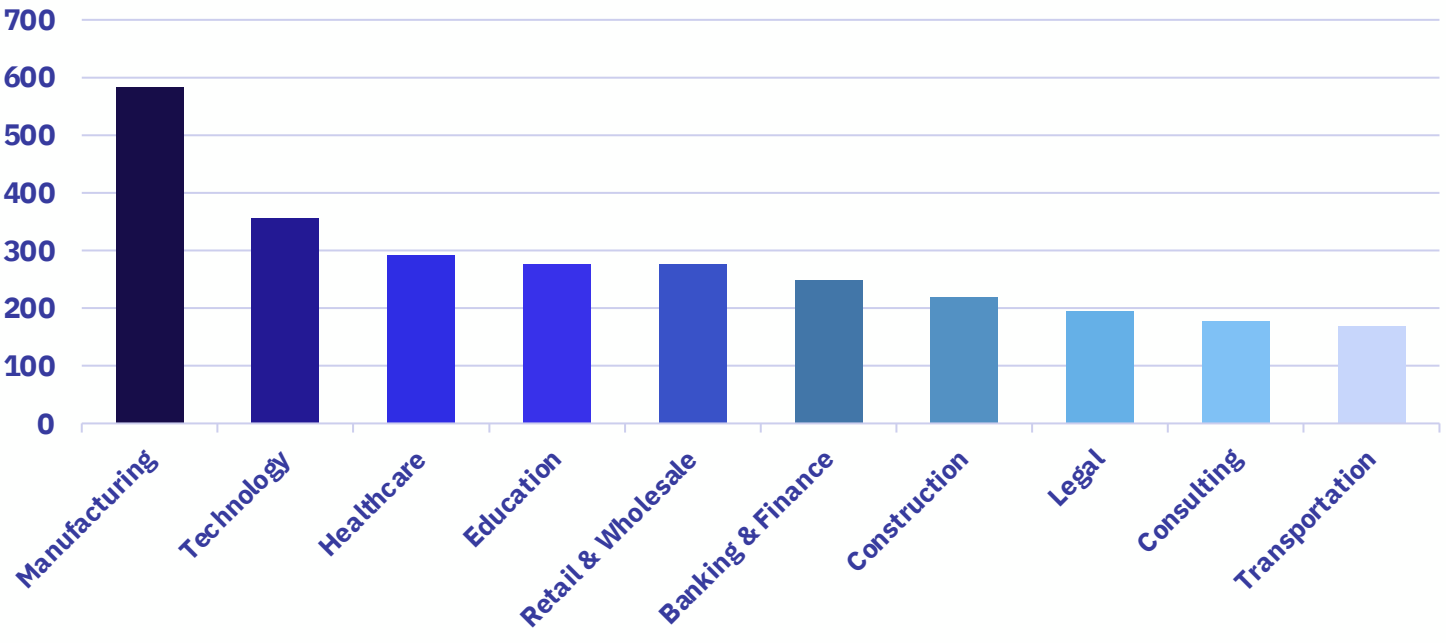
Most Impacted Industries - 2023

Interestingly, while Rhysida (Developing) was not a leading group in terms of total posted victims, coming in 13th amongst competing groups, the group caused disproportionate impacts on traditionally sensitive industries, including Education, Healthcare, and Government sectors. 46 of Rhysida's 74 posted victims belong to one of these three industries.

Among Manufacturing industry victims, the US was impacted five times as much as the next highest country, Germany. Specifically, the US saw 265 impacted Manufacturing victims, while Germany saw a significantly lower number of Manufacturing victims at 48. Manufacturing was the most impacted industry for almost every month in 2023, excluding May, when it placed behind Technology by a single observed victim.

The "top 10" most impacted industries accounted for 2,794 (62%) of all posted victims and were impacted by all but one of the groups tracked by GRIT – Free Civilian, a group with only two posted Ukrainian victims in late January 2023. Free Civilian, a self-proclaimed pro-Russian hacktivist group, has been reported as a Russian GRU persona by Microsoft and Mandiant. Given the typical diversity of impacted victims, limited victim diversity may serve as a future indicator for government-sponsored “faux-ransomware” operations.

Alphv's status as one of the leading ransomware groups impacting the Healthcare industry may continue after their response to law enforcement efforts to shut down their operations. After restoring operations, Alphv announced a change to affiliate rules, allowing the targeting of critical infrastructure. This may lead less scrupulous affiliates to disproportionately target hospitals and other healthcare providers using Alphv's ransomware.



1- Manufacturing
- LockBit
- Alphv
- Play

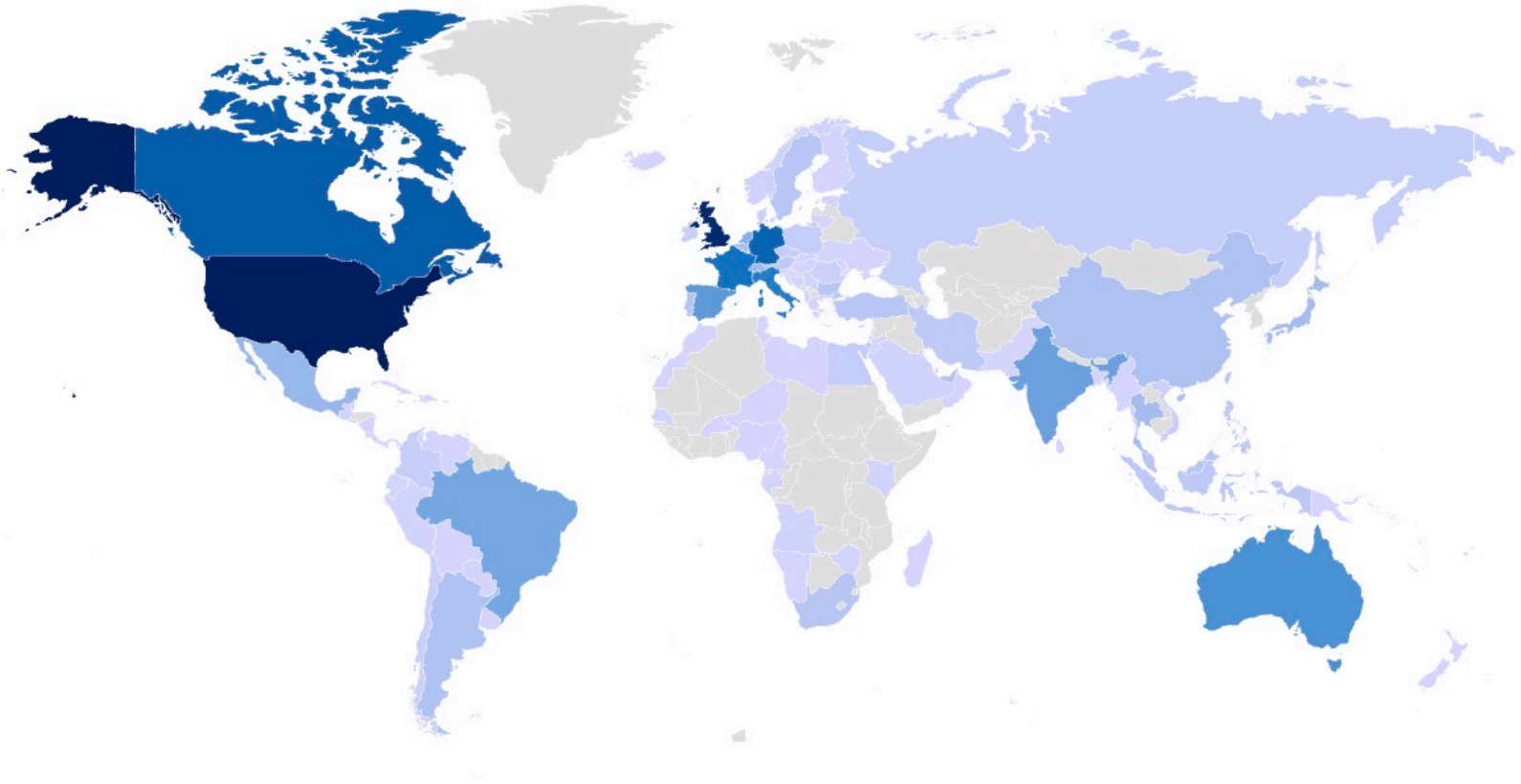
2- Technology
- LockBit
- Clop
- Alphv

3- Healthcare
- LockBit
- Alphv
- Bianlian

4- Education
- LockBit
- Rhysida
- Akira

5- Retail & Wholesale
- LockBit
- Play
- Alphv

Geographic Breakdown of Ransomware Victims (2023)



Most Impacted:

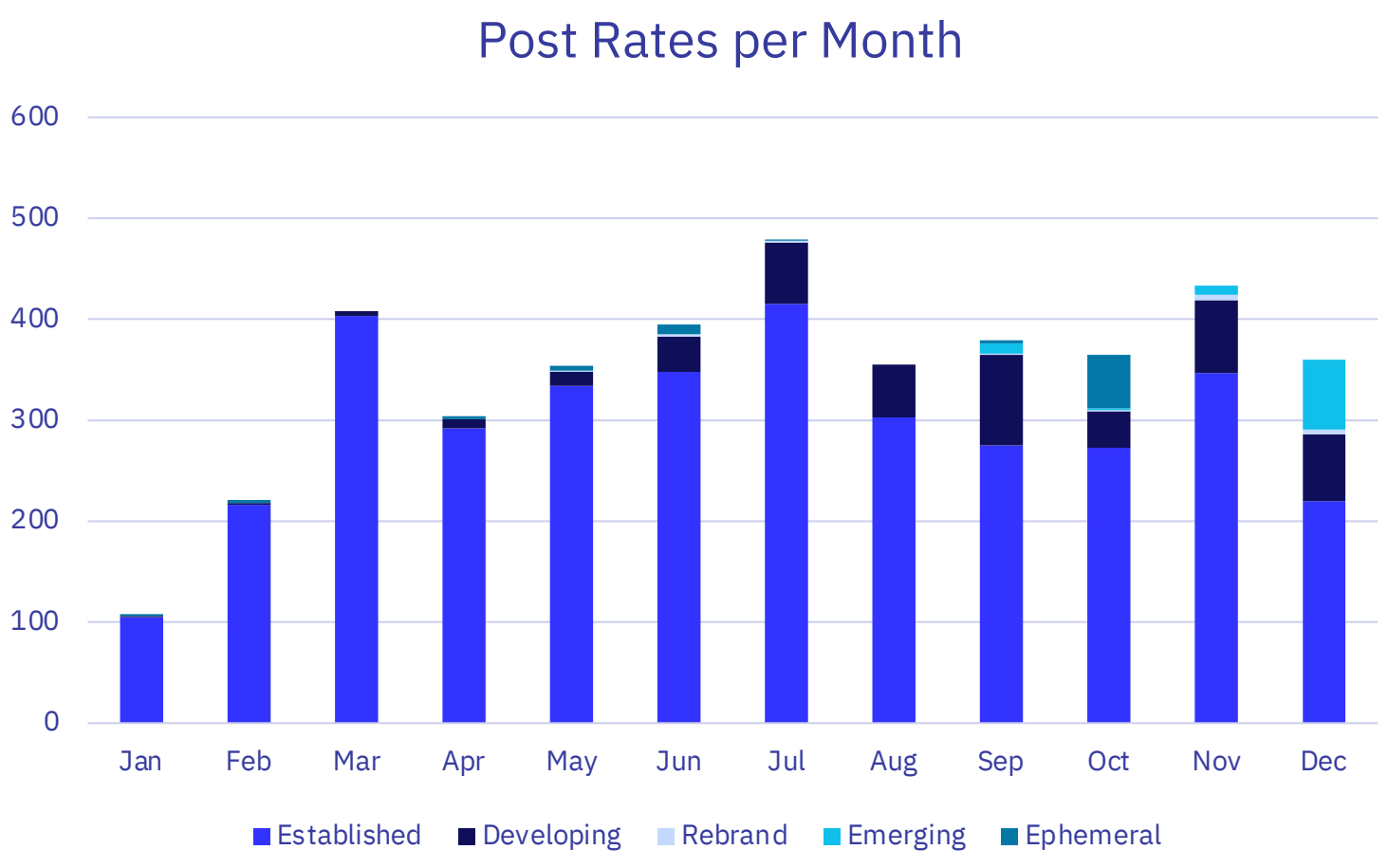
1. United States
2. United Kingdom
3. Canada
4. Germany
5. France
6. Italy
7. Australia
8. Spain
9. India
10. Brazil

2023 Threat Group Breakdown

Established ransomware groups dominated the ransomware ecosystem when compared to less mature groups as classified in our taxonomy. Despite representing less than a third of all distinct observed groups operating during 2023, Established groups generated a disproportionately high victim volume.

Established groups eventually ceded some of their dominant market share during Q4, with a greater portion of observed victims stemming from operations of Developing and Emerging groups. GRIT has previously observed a slight slowdown in the operations tempo of Established groups over the preceding two years. A portion of the decrease in activity could also potentially be attributed to law enforcement's temporary disruption of the Established group Alphv in December 2023.

Only one group, Black Suit, was classified as a Rebrand during 2023, whose victims account for a minute subset of the overall 2023 data. While other groups may be later determined by GRIT to be Rebrands or Splinter groups, only Black Suit's Rebrand was sufficiently attributable.



2023 Activity by GRIT Taxonomy Classification

GRIT Taxonomy Group Type	Days Active in 2023 (Across All Groups)
Established	353
Rebrand	14
Developing	160
Ephemeral	10
Emerging	19

The number of days in which each group type was active in 2023 paints a clear picture of the distinction between them within GRIT's taxonomy. “Days active” was measured by the number of distinct dates on which each group type updated their data leak sites with additional victims.

Established groups, which most frequently follow the Ransomware-as-a-Service model, generally have multiple affiliates acquiring victims at any given time, which allows them to post a near-continuous flow of victims to their data leak sites. Such groups also possess greater resources and staffing, which could support more timely and frequent updates.

Ephemeral groups, by contrast, are short-lived, resulting in minimal victim postings over short periods of time, as indicated by their minimal activity on data leak sites.

Developing groups – defined by GRIT's taxonomy as nascent groups focused on evolution, improvement, and TTP refinement – have demonstrated continuing operations and the ability to generate a consistent stream of victims. While not as well-resourced or entrenched as Established groups, we still expect to see higher levels of activity from these groups than short-term Ephemeral groups or newly arrived Emerging groups. The observable days of activity for Developing groups support this definition, presenting a substantial level of activity second only to Established groups.

Industry Victims by Taxonomy Classification

Established

Victim Industry	Number of Public Victims
Manufacturing	440
Technology	274
Healthcare	158
Banking and Finance	213
Retail and Wholesale	205

Emerging

Victim Industry	Number of Public Victims
Government	13
Manufacturing	11
Entertainment, Hospitality, & Tourism	8
Healthcare	8
Technology	5

Developing

Victim Industry	Number of Public Victims
Manufacturing	53
Healthcare	37
Education	35
Technology	30
Construction	25

Ephemeral

Victim Industry	Number of Public Victims
Manufacturing	12
Consulting	6
Legal	6
Construction	5
Education	5

Rebrand

Victim Industry	Number of Public Victims
Government	13
Manufacturing	11
Entertainment, Hospitality, and Tourism	8
Healthcare	8
Retail and Wholesale	205

Emerging groups were the only group type with Government amongst their most victimized industries, and Government victims were, in turn, the most impacted by Emerging groups. Emerging groups may be entirely new to the ransomware ecosystem and select targets differently than more mature groups, who may avoid government targets to avoid undesired attention from law enforcement.

Healthcare targets rose in popularity among both Established and Developing groups in 2023. Healthcare victims often hold a large amount of PII data, rendering them a high-value target for more mature ransomware groups capable of exploiting or extorting based on large volumes of data. While the Healthcare industry was once considered off-limits and less frequent as targets by Established groups, we have witnessed this norm eroding in 2023.

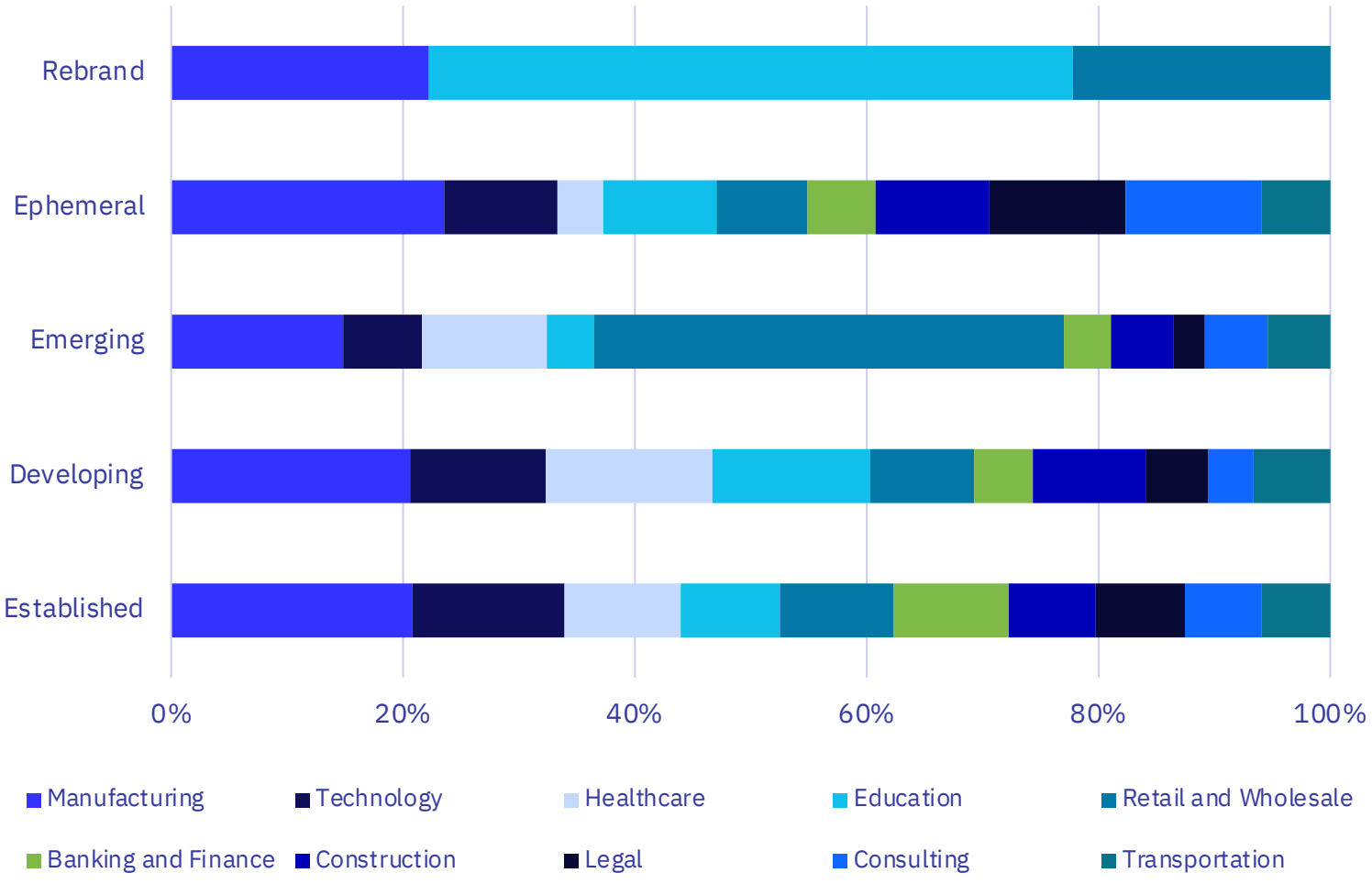
Manufacturing remains one of the most highly victimized industries across most group categories. This is likely driven in part by cybersecurity challenges within manufacturing organizations, as well as the fact that these organizations often suffer significant costs from operational disruption of manufacturing processes, potentially rendering them more likely to pay ransoms in support of a fast recovery.

Industry Victims by Taxonomy Classification

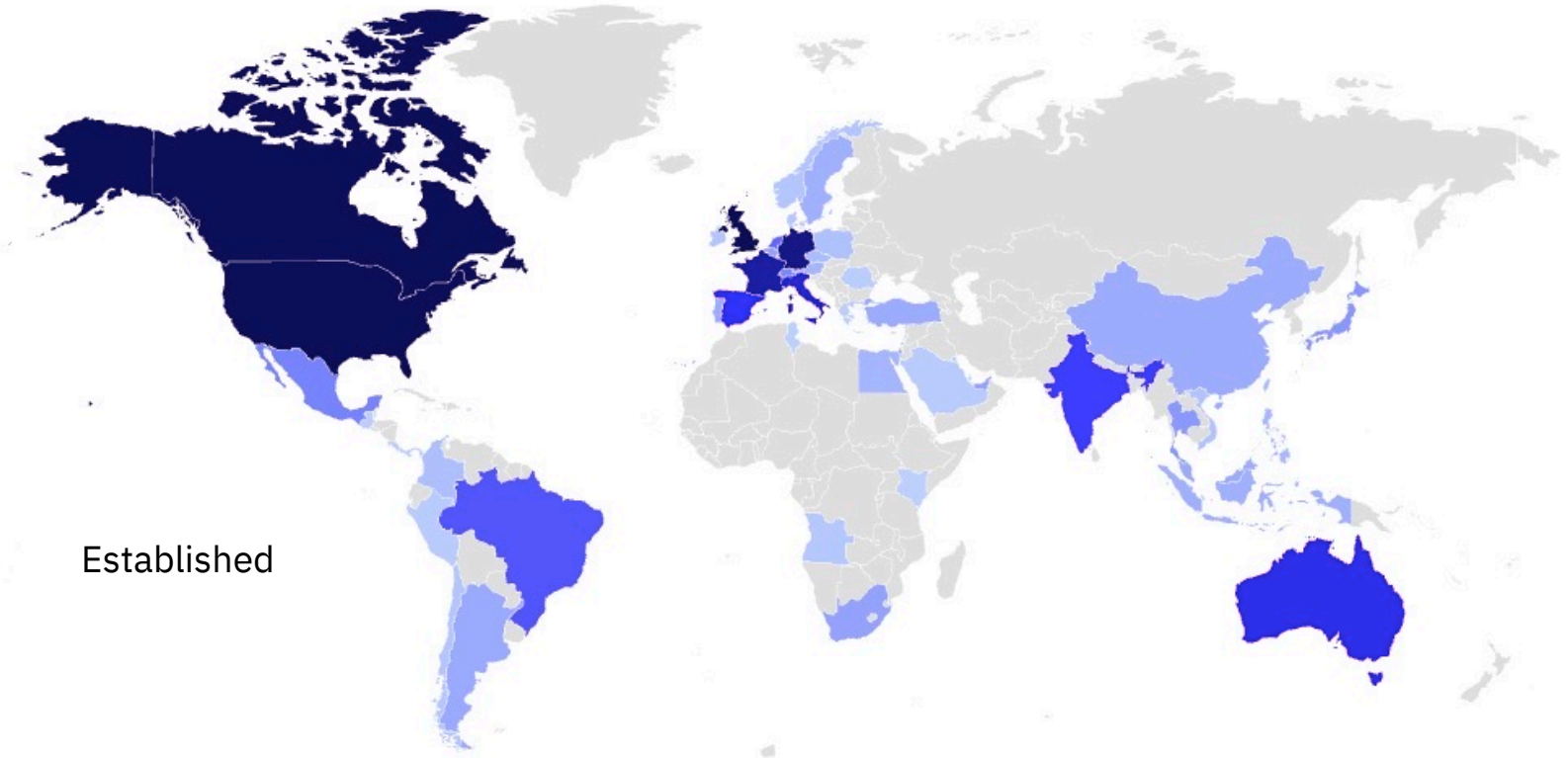
Relative to their share of the ransomware ecosystem, Developing and Emerging groups disproportionately impacted Healthcare organizations more often than Established groups. Healthcare has historically been considered “off limits” for some ransomware programs as this brings negative press coverage and extra attention from law enforcement agencies. Despite this, Established groups saw a relative increase in Healthcare victims from the previous year.

Emerging groups disproportionately victimized organizations within the Retail and Wholesale industry – an industry whose market value increased from $71.8 Billion to $77.2 Billion, according to the Business Research Company. This 7% increase in market value, coupled with a propensity for weaker cybersecurity postures among mid-size organizations, could make this industry a more appealing target for ransomware groups.

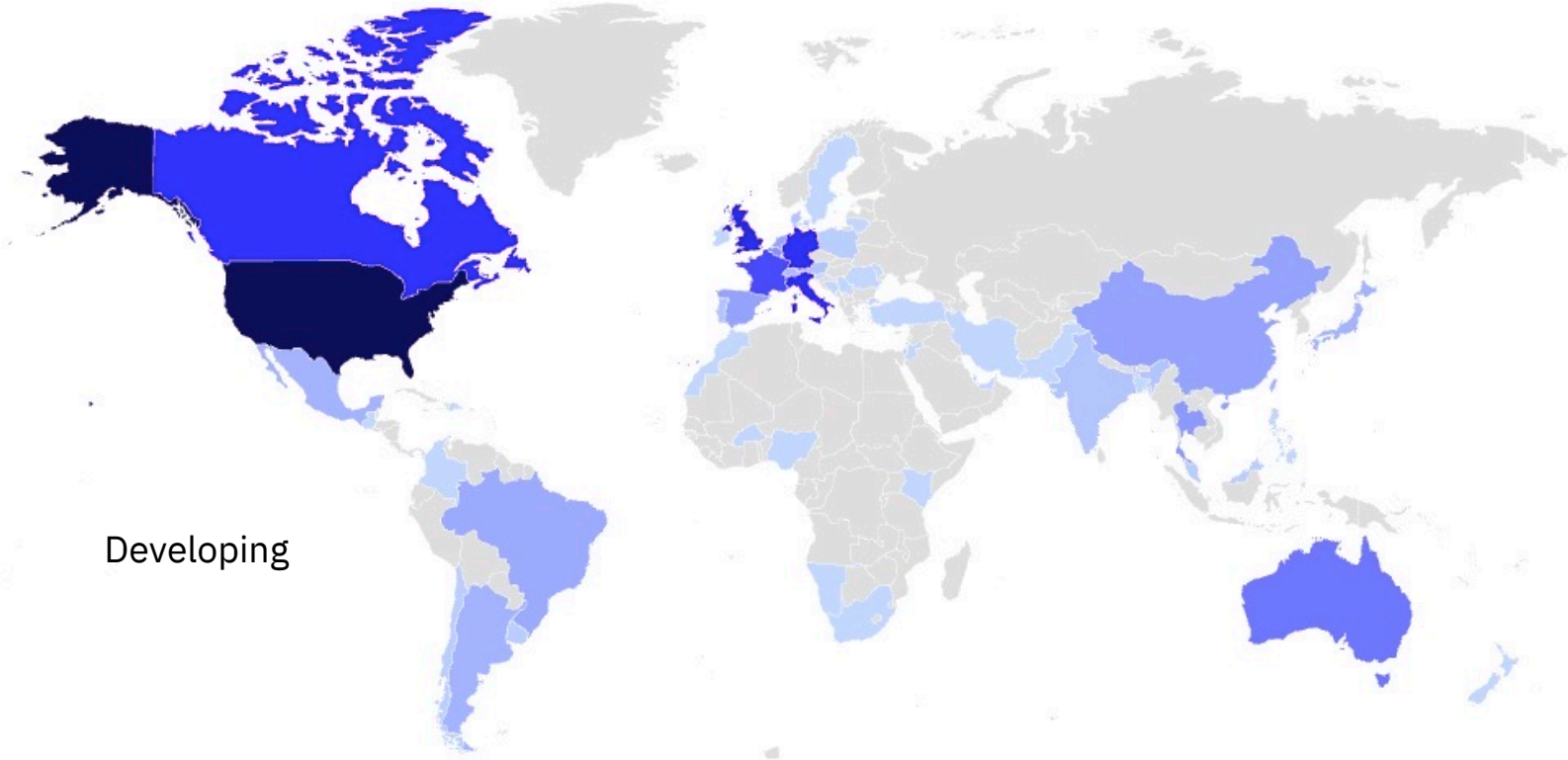
Manufacturing consistently remains the most affected industry across all group classifications. Over 20% of victims belong to the manufacturing industry across all group classifications except Emerging groups.



Geographic Victims by Taxonomy Classification

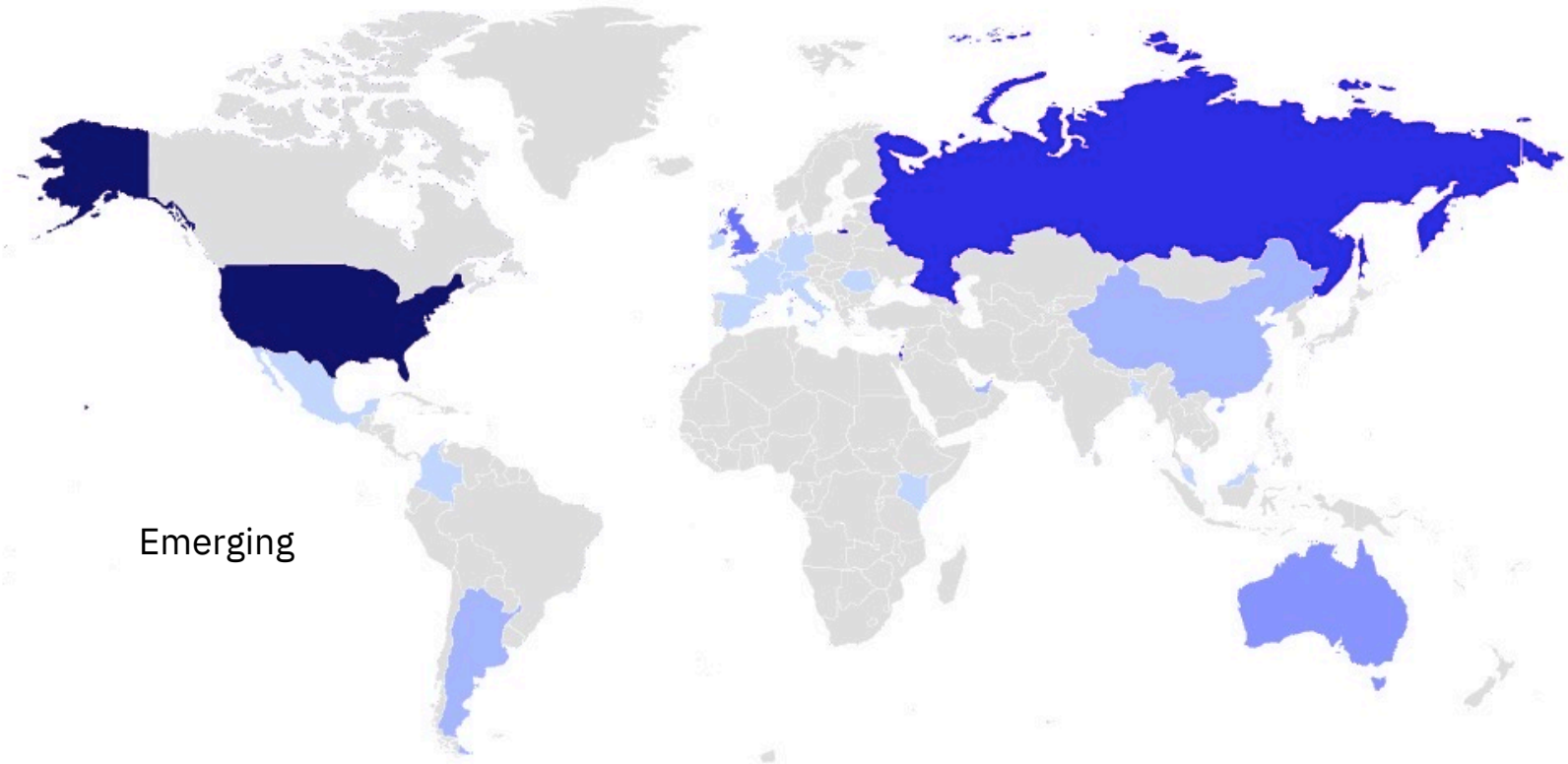


Established

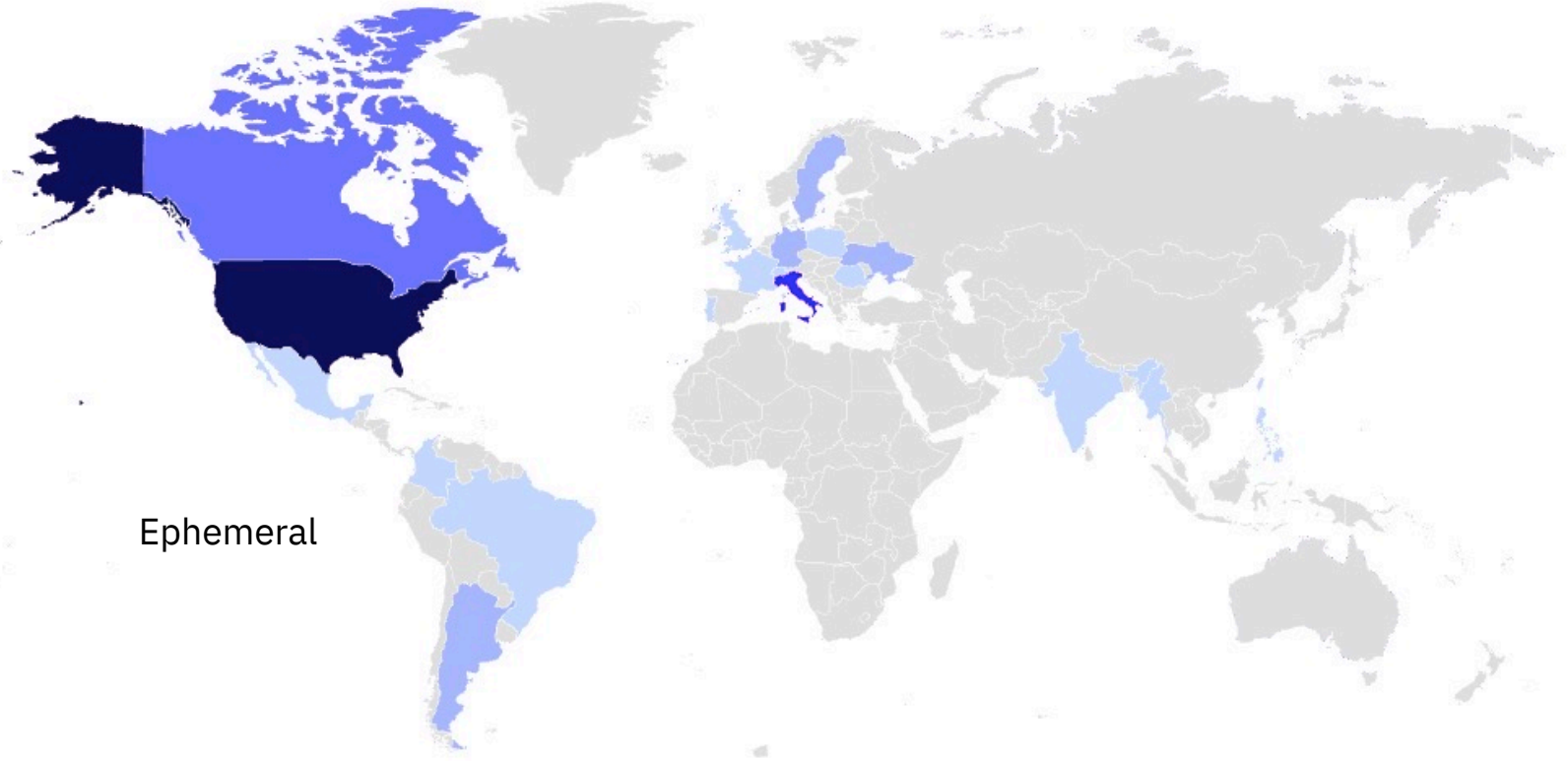


Developing

Geographic Victims by Taxonomy Classification (cont'd)



Emerging



Ephemeral

Top 5 Countries By Taxonomy Classification

The United States was the most impacted country across all group classifications, reflecting its status as an attractive target for ransomware groups from inception through maturity. This is likely due to the perception of victim organizations in the US as more likely to pay ransoms and the profit-maximizing nature of ransomware operations.

Emerging and Ephemeral groups appear to target more victims outside of the Global North, potentially limited by language barriers or technical proficiency, or to maintain a lower profile while beginning operations. As groups progress across the maturity spectrum, victim concentration appears to shift towards North American and Western European targets.

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

Developing
1. United States
2. United Kingdom
3. Germany
4. Italy
5. Canada

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

Ephemeral
1. United States
2. Italy
3. Canada
4. Argentina
5. Germany

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

Ransomware in Depth:

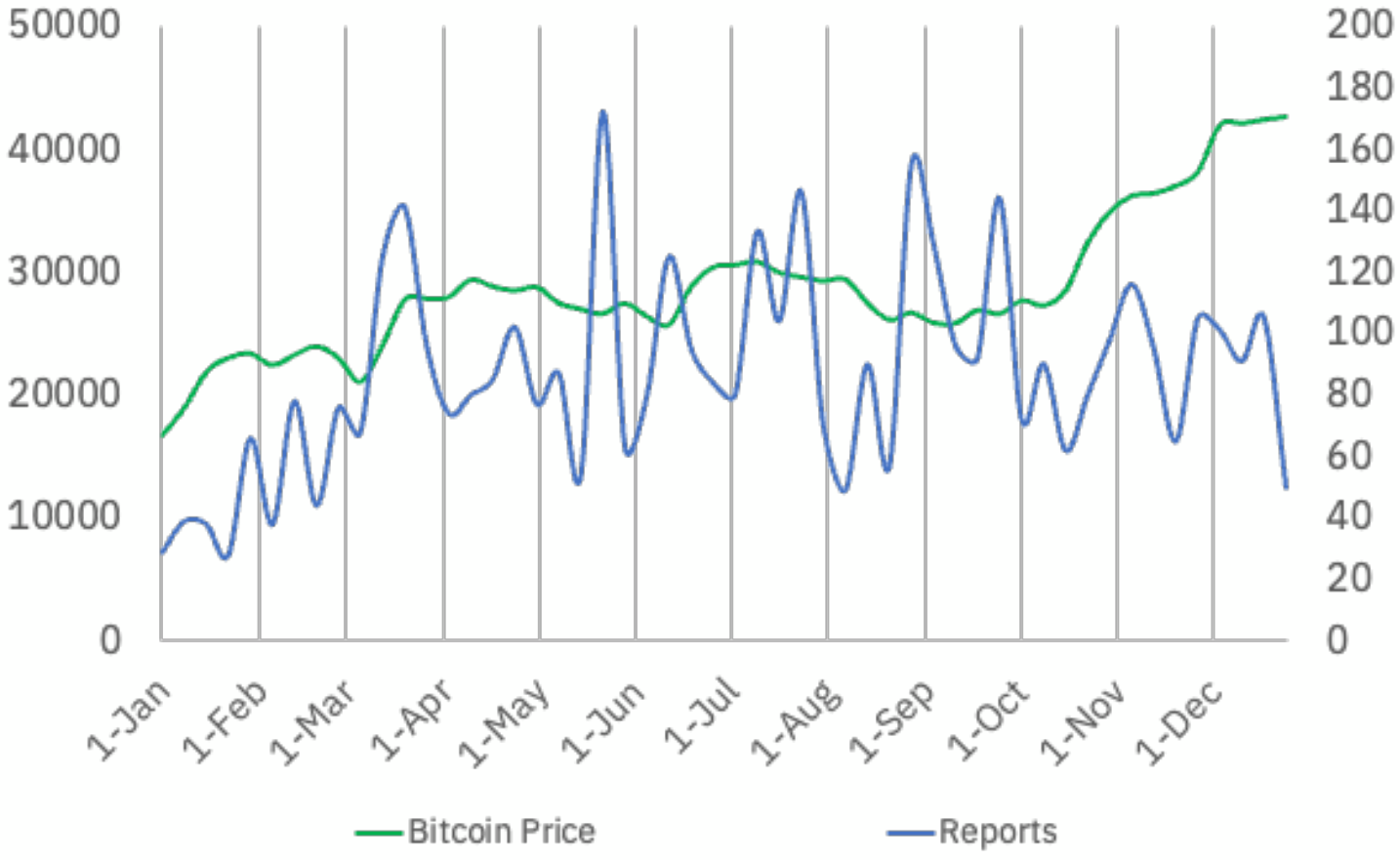
Major Events, Observations, and Trends in 2023

Throughout 2023, GRIT hypothesized that the price of Bitcoin may correlate with ransomware victim posting rates. As we closed out the year, we examined the year's complete data to validate or refute this hypothesis.

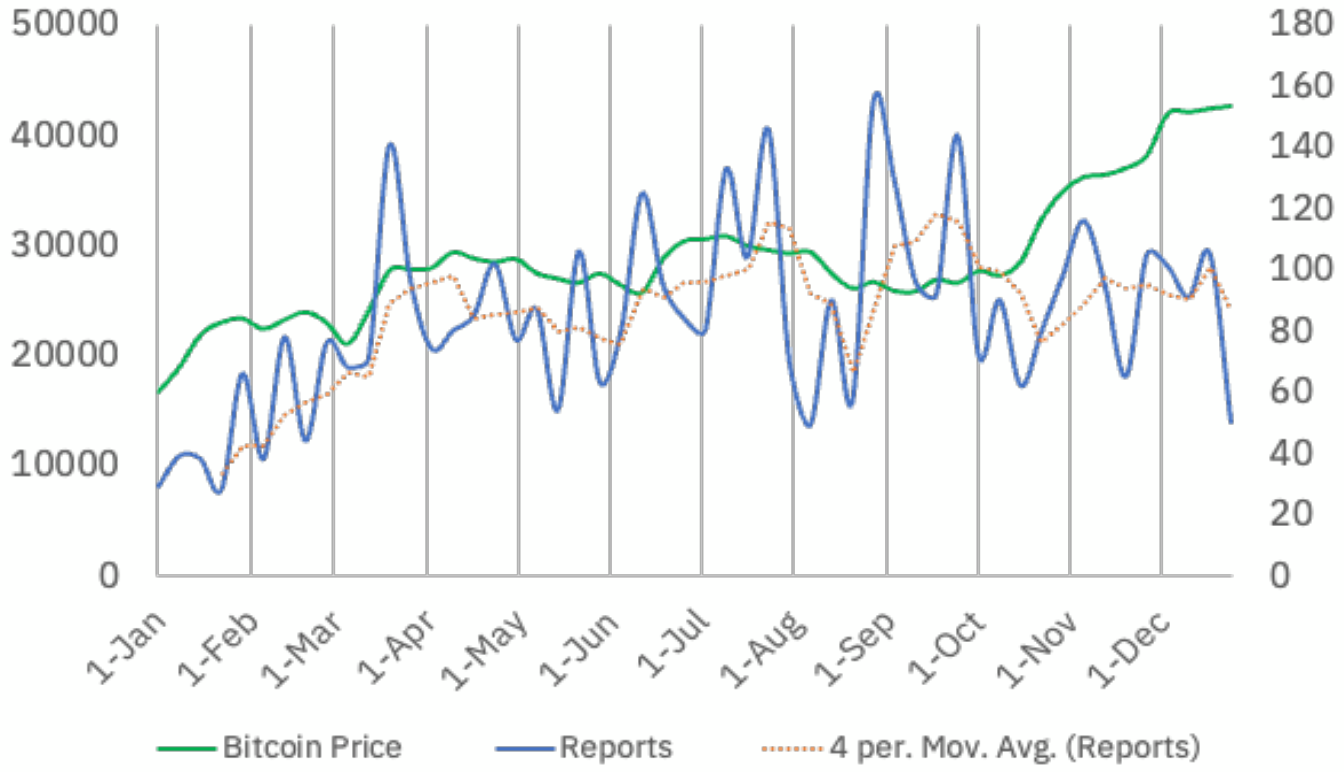
A cursory review of victim posts and Bitcoin prices across weekly intervals in 2023 reveals two possible focal points. The first is the general trend of an overall rise of Bitcoin value appearing to correlate with an increase in ransom victim posts during the first three months of the year, along with a steady increase in ransomware reports.

The second is an observable and dramatic shift between the rise of Bitcoin value in contrast with a decline in victim reports from October until the end of the year.

Rate of Posted Ransomware Victims vs Price of Bitcoin in USD (2023)



Rate of Posted Ransomware Victims vs Price of Bitcoin in USD, Outliers Removed (2023)



Methodically structuring our data painted a clearer picture and allowed us to better view trends with less noise. Firstly, Clop's mass exploitation campaigns resulted in the posting of 54 different victims at one time on March 18. This mass exploitation campaign is abnormal and skews the data that would otherwise be indicative of overall operational tempo. Similarly, the Developing group 8Base debuted their data leak site on May 23rd, with 66 victims posted simultaneously. Those victims were almost certainly acquired throughout the preceding months, likewise, skewing our data. These victims were removed from the associated graph to better demonstrate the overall trend in ransomware operational tempo during 2023.

We calculated a 4-day period simple moving average to better normalize victim post data and account for variances between dates of initial compromise and the date of a victim's post to a group's site.

Comparing this moving average with the price of Bitcoin, a much stronger correlation can be observed between posting rates and Bitcoin value. Supporting this observable correlation through data, we see a correlation coefficient of .565, demonstrating a moderate correlation. Limiting our focus to just the data from January through September before October's drop further yields a 0.747 correlation coefficient, reflecting a strong correlative relationship between victim post rates and Bitcoin value over time.

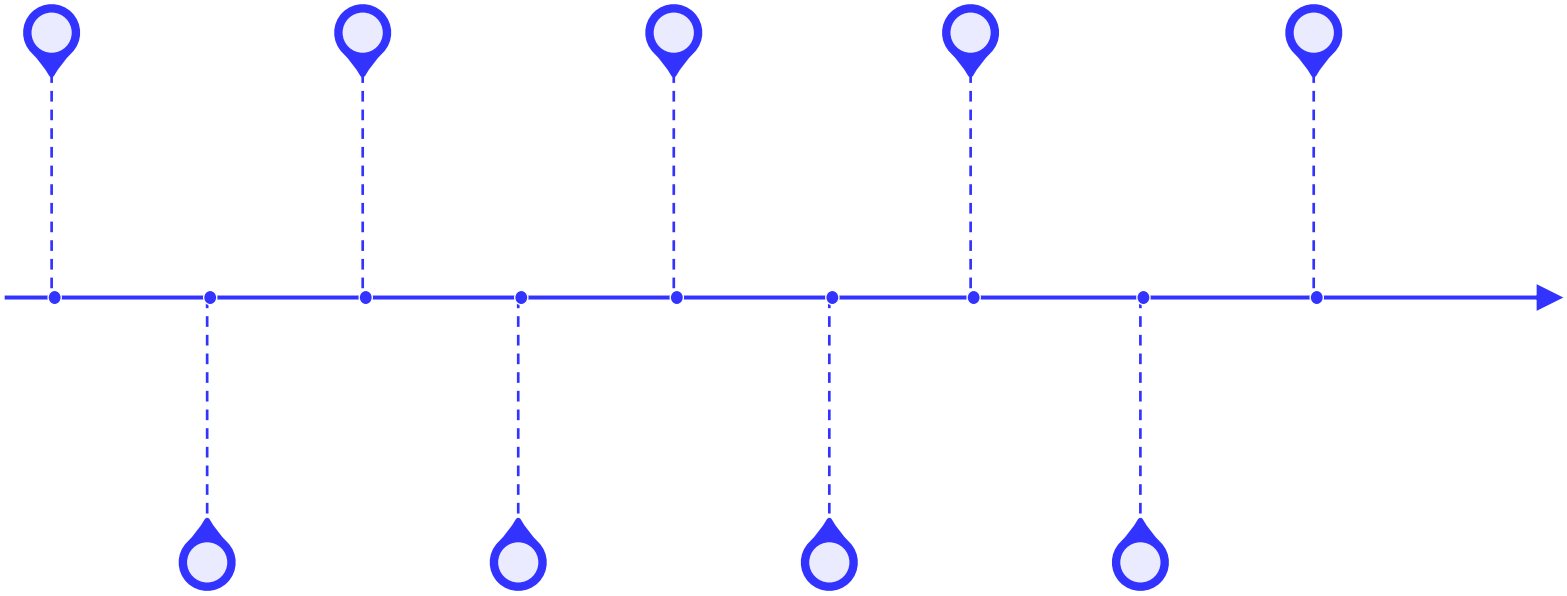
Rate of Posted Ransomware Victims vs Price of Bitcoin in USD, Outliers Removed (2023) (cont'd)

In reviewing the decreased correlation from October through the end of the year, we considered the root cause and the drivers of our hypothesis, searching for potential explanations. While we cannot conclusively rule out other drivers, we note that Bitcoin value surged during this time period, driven by announcements that the US Securities and Exchange Commission (SEC) may approve Bitcoin futures exchange-traded funds (ETF), which would provide a path for investors to purchase Bitcoin and Bitcoin derivatives through stock market exchange services.

Although we cannot affirm the motivations and drivers of individual ransomware actors, we note our findings as potentially suggestive of ransomware group activity increasing with interest in Bitcoin procurement over time, with increased activity correlating a moderate to high amount during periods of value growth in the cryptocurrency. We observed a similar correlation between the price of Bitcoin and the posting rates of ransomware groups during our 2022 ransomware report, which strengthens our assessment of a relationship between the two data sets, as this now appears to be a year-over-year trend. The dataset in 2022 did not experience the end-of-the-year separation between the trendlines as did 2023's data.

We note and acknowledge that we lack insight into the number of ransomware victims that pay ransoms across the year and that the addition of such data may substantially impact or change our findings.

Major Events in Ransomware:
2023 at a Glance



January 16
Bianlian Decryptor Released

February 8
Clop's GoAnywhere Campaign

March 29
3CX Supply Chain

June 1
Clop's MOVEit Campaign

August 29
Qakbot Disrupted

September 18
Scattered Spider Casino Attacks

October 7
Reignition of Israel - Palestine Conflict

December 15
New SEC 8-K Rules Take Effect

December 19
Alphv Disruption

Major Events in Ransomware:
Clop’s MOVEit Campaign

Clop's mass exploitation of Progress Software's MOVEit managed file transfer software impacted hundreds of victims across multiple industries in a lightning campaign, with impacts continuing throughout the Summer. The incident would go on to become one of the most reported cybersecurity stories of the year, with reporting providing information ranging from technical details of the exploit through to the ensuing fallout and data publication. Notably, the campaign mirrors earlier Clop mass exploitation campaigns, with the group executing an elaborate, coordinated plan to exploit previously unknown vulnerabilities, resulting in data theft and extortion for profit.

The patience and planning demonstrated by the group in this case and other mass exploitation campaigns that rely on "zero-day" vulnerabilities are crucial to maximizing impact and revenue extraction before an associated vulnerability can be discovered and patched. To support Clop's "all at once" approach to exploitation, the group automated and tested a process that would extract all available data held by victim companies that ran the impacted application exposed to the internet. As the operation came to light in early June, Clop updated their data leak site with a generic message inviting anyone who believed that they might have been affected to reach out to them to prevent the publication of sensitive data collected in the campaign. This approach likely reduced the time burden of contacting individually impacted victims and initial communications unlikely to lead to settlement.

While the group worked through any ensuing negotiations with victims and began posting the data of non-compliant organizations to their data leak site, they very likely encountered issues with hosting the substantial amount of exfiltrated data on their existing infrastructure, facing limitations of the onion protocol, which hosted their site and the illegal nature of the data's possession. With necessity as the mother of invention, Clop would go on to experiment with alternative hosting strategies with varying levels of success. The group tried uploading data on a per-victim basis to clearnet sites hosted on domains directly naming the victim. This approach gained headlines, but the process was likely deemed too resource-intensive for Clop, who ultimately only used this approach on a handful of victims.

As an alternative strategy, the group also hosted victim data in a series of Torrent files. This strategy leveraged the inherently distributed nature of the Torrent protocol to make a more reliable, albeit significantly slower, solution to sharing stolen data. These actions by Clop demonstrate the difficulty of pulling off a true successful mass exploitation campaign, including managing "long tail" logistical considerations such as data storage. In spite of early issues, the incident would go on to be considered one of if not the largest single incident of data theft in history. Should mass exploitation campaigns spread as a tactic to other threat groups, Clop may prove to be a model for this style of attack and associated scale.

Major Events in Ransomware:
Scattered Spider attacks Major Casinos

In September 2023, two of the largest entertainment companies in the country, MGM Resorts International and Caesars Entertainment, confirmed downtime caused by ransomware attacks. As details emerged, the two attacks seemed to share a common thread, a connection with a threat group and new affiliate of Alphv, referred to as Scattered Spider by security researchers. Alphv called public attention to the attack by posting a diatribe to their data leak site in an attempt to place pressure on MGM after they refused payment. After weeks of downtime, MGM reported that their losses in this single attack would exceed $100 million USD. Unconfirmed details also emerged about the method of ingress for both the MGM and Caesars attacks; both were said to be a result of social engineering by Scattered Spider, which is known for its skill in English-language social engineering to circumvent Identity and Access Management.

A frequent tactic in this space, and one employed by Scattered Spider in the past, is breaching network accounts via calls to an organization's help desk. Threat actors, armed with information about an employee obtained from LinkedIn and a convincing story, aim to exploit established account recovery processes to gain access to privileged user accounts at a target organization. Social engineering tactics are as effective as they are hard to detect, and the strongest prevention for such attacks is policy and training – both human elements attempting to compensate for technological gaps. Of course, social engineering as a method of initial access is not new to ransomware actors. Phishing, which is also considered a form of social engineering, continues to pose a threat to every organization with an email presence. However, as email filtering technology improves and users become more knowledgeable, their impact is often limited. Ransomware groups seem to have adjusted to these headwinds, but actors like Scattered Spider show there is still a potential for large-scale compromises via exploitation of the human attack surface.

Major Events in Ransomware:
LockBit's new Affiliate Rules

In September, LockBit, the most prolific ransomware group of 2023, announced a new set of affiliate rules regarding the negotiation of ransoms with future victims. These new rules, which the group presented in a poll earlier in the year to collect affiliate feedback, implemented significant guardrails around how individual affiliates may price and negotiate ransoms. The new rules first define a sliding scale based on the victim's revenue to determine how high an affiliate must set their initial extortion demand. Furthermore, once the initial demand is calculated, the new rules forbid affiliates from negotiating discounts in excess of 50%. These actions are seemingly motivated by a reduction in ransom payments, a trend that could ultimately affect LockBit leadership's revenue. LockBit seems to have made these new rules effective starting October 1.

LockBit

Очень важный социальный опрос, просьба читать очень внимательно и проголосовать.

Так как ранг партнёров и ранг атакованых компаний очень различается, цены выкупа и размеры скидок никак не регламентируются, один партнёр может брать выкуп 10% от годового оборота компании, к примеру есть кейсы где сумма выплаты 2 миллиона долларов, а годовой оборот компании 10 миллионов долларов, и другие подобные кейсы с похожими цифрами, а другой менее опытный партнёр очень не грамотно ведет переговоры, очень сильно нуждается в деньгах и берет 0.00005% от годового оборота компании, например есть кейсы где у компании с годовым оборотом 2 миллиарда долларов, партнёр соглашается на выкуп 100 тысяч долларов, рекавери компании ведут статистику выплат и в соответствии с пред идущими результатами переговоров могут пытаться

повторить свой успех «талантливого» ведения переговоров, а по сути просто удачи и отсутствия дисциплины и регламента размера выплат в партнёрской программе, на мой взгляд это очень вредит в будущих переговорах всем партнёрам и тем у кого много денег и опыта, и тем кто недавно взял маленькую выплату, а теперь будет надеятся на крупную, когда появились деньги на еду.

Новички и те у кого на текущий момент мало денег, часто соглашаются делать скидки аж до 90% от изначально озвученной справедливой цены, из за подобных скидок страдают другие партнёры, которые имеют много денег и крепкие нервы, рекавери компании думая что любой партнёр может сделать скидку 90% пытаются продавить эту скидку в переговорах с опытными партнёрами где такой скидки никогда не будет, из за этого сделка либо срывается так как опытный партнёр публикует информацию после ничтожных предложений, либо переговоры затягиваются на длительное время в ожидании крупной скидки

Цель опроса разработать новые правила тактики ведения переговоров и политику ценообразования для размера выкупа и размеров допустимых скидок. Будет учтено мнение каждого партнёра. Новые правила, помогут улучшить ситуацию и стабилизировать размер выплат на высоком уровне.
Вы можете предлагать свои варианты, вы можете голосовать за несколько пунктов:
1. Ничего не менять и оставить всё как есть, каждый партнёр делает всё что хочет и не имеет никаких ограничений, как это было всегда.

2. Ограничение размера минимально допустимой запрашиваемой суммы в начале переговоров в зависимости от годового оборота компании, например 3% и запретить делать скидку более 50%, например если ревению компании 100 миллионов долларов, вы начинаете переговоры с 3 миллионов долларов и не имеете права брать выкуп менее 1.5 миллионов долларов.

3. Не вводить никаких ограничений на минимально допустимую запрашиваемую сумму, так как не всегда получается качественно нанести максимальный ущерб атакованной компании, но ограничить максимально возможную скидку от первоначально озвученного вами размера выкупа 50%, например если вы говорите компании что цена выкупа 1 миллион долларов, вы не имеете права брать менее 500 тысяч долларов.
4. Запретить брать сумму менее той цифры, которая указана в киберстраховке при условии, что вами была найдена киберстраховка.
5. Запретить брать сумму менее 50% от той цифры, которая указана в киберстраховке при условии, что вами была найдена киберстраховка.
6. Другой вариант, предложенный вами.

Мне очень важно услышать ваше мнение если я в чем-то ошибаюсь или что-то упустил или у вас есть своя гениальная идея как максимизировать наши доходы и стать богаче.

Major Events in Ransomware:
SEC Updates Guidance on incident notifications

On July 26th, 2023, the US Securities and Exchange Commission (SEC) announced new rules regarding the disclosure of “material” cybersecurity incidents experienced by public companies. The new rules, which were made effective December 18, 2023, provide guidance around how quickly a victimized organization must notify the public and shareholders of a cybersecurity incident. Specifically, public companies now must file an SEC Form 8-K with details of the incident’s nature, scope, and timing within four days of it becoming “material.” These new rules have already significantly influenced how organizations respond to ransomware and other forms of cybersecurity attacks.

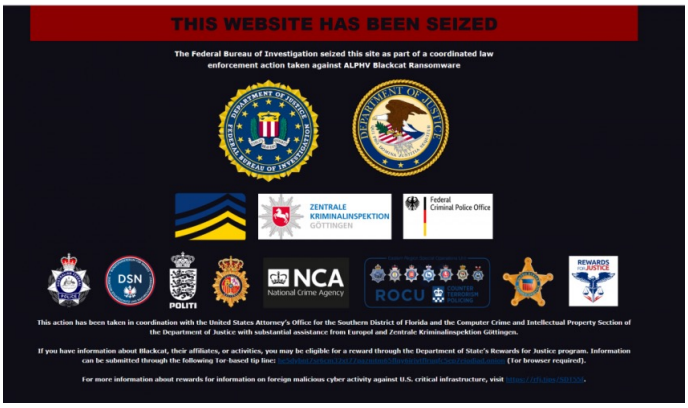
In the past, public companies have provided notice to shareholders about cyberattacks for the purpose of informing them about potential impacts to the organization’s “bottom line.” With the advent of the new SEC rule, companies are forced to provide notice on a shorter timeline and in greater detail. Ultimately, this puts added pressure on organizations affected by ransomware to identify materiality of a given breach; the new notification requirements provide protection for both shareholders and individuals who may have personal data compromised. By shedding light on incidents that might otherwise be concealed, the new SEC rule aims to bring more accountability to organizations victimized by ransomware.

Major Events in Ransomware:
Law Enforcement Disruption of Alphv

Starting as early as December 8th, 2023, and culminating in a seizure message posted to their data leak site on December 15th, several arms of United States and international law enforcement cooperated to disrupt the Alphv, also known as Black Cat, Ransomware-as-a-Service (RaaS) operation. The main impact to the group was the seizure of private keys for over 900 Tor sites operated by Alphv, leading to their eventual shutdown and takeover. In addition, law enforcement was able to capture decryption keys for around 500 recent victims of the RaaS group, meaning that any organizations affected by the group in a several-month timespan could potentially recover their encrypted data without cooperating with Alphv.

The disruption immediately sent shockwaves throughout the cybersecurity industry. While many celebrated the apparent takedown, Alphv quickly attempted to restore their operations. The law enforcement actions against the group have not yet resulted in arrests of Alphv affiliates or leadership, leaving Alphv operators to remain active. Several hours after the Alphv data leak site was changed to a law enforcement seizure notice, the site changed again, this time to a message from Alphv. This “unseizure,” appears to have occurred as a result of Alphv maintaining access to the keys needed to update the content served by the group’s Onion URL. The resulting message from Alphv, written fully in Russian, taunted law enforcement and advised their affiliates that they remained unscathed.

The group pointed visitors to a new Tor site, not under the control of law enforcement, and defined several new rules for operations going forward. Primarily, the group dramatically changed their payment structure for affiliates, who would now receive 90% of any ransom payments they generate. This change was likely motivated by the need to prevent a departure of affiliates who no longer trust the group following the law enforcement seizure. The 90% affiliate share offered by Alphv also contrasts with Lockbit’s stated shares of 60-80% - most likely an attempt to motivate affiliates to stay with the Alphv program instead of moving to their largest competitor. Alphv also announced that they would no longer be negotiating discounts with victims, and that they would be removing rules preventing the targeting of critical infrastructure. While law enforcement actions in this case had a noticeable impact on the ongoing operations of one of the most prolific ransomware groups, Alphv continues to maintain operations today.



Major Events in Ransomware:
Published Decryptors impact Ransomware Operations

Besides law enforcement arrests, one of the biggest disruptors to ransomware operations continues to be the threat of a public decryptor, either from reverse engineering, because of a cryptographic weakness, or intentional and unintentional leaks. The business model of ransomware groups depends on the group or affiliates being the only holders of decryptors, with the resulting victim need used as leverage to extort the victim for payment.

Early in January 2023, a team at Avast released a free decryptor for BianLian's ransomware. Their program leveraged a flaw in the group's encryption binary to ultimately guess and implement the key for decryption in a reasonable amount of time, given access to the encrypting binary. After seeing success, Avast released another decryptor in June, this time for the then-Emerging group Akira. Both events led to obvious and immediate changes in the threat actors' operations. BianLian and Akira have both since appeared to change course towards data exfiltration in their attacks, often avoiding encryption on victim networks altogether.

The threat of a public decryptor is existential to groups who build their own encryption software; this fact may even push some smaller groups towards joining RaaS outfits whose encryption technology has proven resilient to security researchers' reverse engineering efforts. Ultimately the efforts by Avast and other security researchers save victims significant time and money by avoiding ransom payment and reducing operational downtime. This, in turn, imposes costs on the ransomware operators, who must either develop a new encryptor or change their tactics entirely – outcomes beneficial to defenders across the board.

BianLian

Types of ransomware – single, double, triple extortion

At the outset of 2023, the preponderance of ransomware operations could be described as follows:

SINGLE EXTORTION – Attackers encrypt victim data and extort victims in exchange for a decryptor to recover files

DOUBLE EXTORTION – Attackers also exfiltrate data and use the threat of publishing sensitive information as a secondary form of leverage

TRIPLE EXTORTION – Attacker re-attacks the victim, usually through an availability attack such as Distributed Denial of Service (DDoS), as a way to add increased "pain points" and disruption in a retaliatory manner against non-compliant victims following encryption and/or data exfiltration.

Blurring of the Ransomware/Data-Theft Divide

The Rise of Data Extortion Operations

Over the course of 2023, we observed multiple groups, including RansomedVC and Ransomhouse, which focused on data extortion and data leaks absent the deployment of ransomware. In some cases, such as RansomedVC, the group encouraged the idea that they were capable of deploying ransomware, likely as a way of encouraging compliance, intimidating victims, or introducing uncertainty.

GRIT distinguishes this type of operation from "exfiltration-only" ransomware operations, in which attackers apply initial access and exploitation tactics similar to those used in ransomware operations but opt to focus on data exfiltration while eschewing encryption. These operations are often performed by groups that have historically conducted single or double extortion ransomware operations, likely to reduce the signature of their operations, continue operations following builder leaks or compromise, or reduce technical requirements of nascent or continuing operations.

Data Extortion Group Examples

The most recent example of data extortion group tactics can be seen in RansomedVC, a data extortion group that first emerged with a clearnet website and a wide range of claims in August 2023. The group would go on to claim high-profile victims, including Sony and Dragos, but further investigation by security researchers revealed that data posted by the group appeared to be recycled from previous breaches and repackaged to appear new or contained dated information, suggesting a distinct initial compromise point. Later statements from the group via Telegram laid bare the reasoning behind this: despite several claims of network intrusions and ransomware capabilities, the group had purchased data leaks and databases from brokers and other actors and attempted to re- extort victims or attract attention with the purchased data as deceptive evidence of breach. While we lack information indicating to what extent, if any, victims paid ransoms to the group, its perception and derision on dark web forums suggest that RansomedVC's deception did not remain a well-kept secret. Following a short-term hiatus for "security reasons" towards the end of 2023, the group's administrators have returned to Telegram, a dark web site, and a clearnet site while voicing their intent to resume selling compromised data.

Ransomhouse, a similar data extortion group with no history or dependence on ransomware, could be considered an inspiration for RansomedVC, having begun its operations in 2022. Ransomhouse claims to exploit unspecified "vulnerabilities" in victim networks to steal data from victims, though we note that this could range from historical and unpatched vulnerabilities to basic misconfigurations and that the data theft observed to date reflects "smash and grab" tactics more than targeted or deliberate intrusions. Ransomhouse is suspected of purchasing data from ransomware groups in order to re-extort victims, but simultaneously attempts to paint their operations as the responsibility of "lazy" victims who had failed to properly secure their networks. Unlike RansomedVC, Ransomhouse has not been noted for attention-seeking behavior or the issuance of bombastic or self-promoting claims.

Lapsus, sometimes stylized as Lapsus$, was an extortion group that emerged in August 2021. Lapsus conducted a number of high-profile intrusions resulting in data theft/extortion and site defacements, impacting the Brazilian Ministry of Health, Rockstar Games, and Okta. Though Lapsus exhibited seemingly more advanced and direct tactics relative to RansomedVC and Ransomhouse, they similarly focused on data extortion. While commonly referenced as a ransomware group, there are contradictory claims regarding the use or dearth of ransomware encryptor use by Lapsus in open reporting. The group was known in part for its childish and juvenile communications on Telegram and taunting remarks made to victims; behavior made more understandable when London Police arrested seven teenage Lapsus members in early 2022. The group is believed to have disbanded in the wake of the arrests and is currently considered inactive, although intelligence reporting suggests that former members may have moved on to other groups.

Incentives for deceit/fabrication

Similar to ransomware groups, data extortion groups are motivated to extract the maximum possible ransom from their victims and often seek to do so by threatening consequences for non-compliance with demands. Unlike ransomware groups, data extortion groups do not hold file encryption as additional leverage and, in many instances, may never have directly accessed a victim's network. To compensate for this, we have observed posturing, exaggeration, and outright fabrication from some data extortion groups, likely to increase the probability of receiving payment. While ransomware groups are no strangers to embellishment and deceit, the root claim of network intrusion is generally verifiable forensically. Organizational teams facing data extortion groups are advised to practice due diligence in validating any claims made regarding the timing, scope, and impacts of an extortion group's alleged attack.

The use of exaggeration and embellishment by extortion groups, particularly RansomedVC, highlights the need for scrutiny and corroboration in modern cyber threat intelligence operations and security research. Early posts from RansomedVC were taken at face value by some security researchers, resulting in a litany of reporting of RansomedVC as a "Ransomware group" and giving credence to allegations of high-profile target impacts. This occurred despite a dearth of evidence supporting their claims, no observable ransomware encryptor or associated artifacts, and observed skepticism and hostility towards the group amongst personas on dark web hacker forums. Given RansomedVC's attention-seeking behavior, such reporting inadvertently rewarded relatively low-effort operations and, in doing so, could have encouraged victims to comply with ransom demands.

Hacktivism and data extortion

Distinct from data extortion and ransomware, hack and leak operations remain a frequent tactic of hacktivist groups and hacker collectives. Whereas hacktivist groups are ostensibly driven by ideological, religious, or political motivations, hacker collectives may conduct data theft ”for the lulz” and often appear to consist of younger or more immature operators.

We note that the distinction between these cybercrime groups, data extortion groups, and ransomware groups may be drawn in part by technical competency, with increasingly impactful intrusions and ransoms demanding increasing proficiency and experience. We assess that given reduced technical barriers to entry, such as leaked ransomware builders or proof-of-concept exploits, members of less experienced collectives or hacktivist groups may seek to progress to more advanced groups and explore more destructive operations.

Ephemeral and “No Name” Groups defined

In keeping with GRIT’s taxonomy for ransomware groups, we define Ephemeral ransomware groups as short-lived (“flash-in-the-pan”) operations that generally terminate within three months of the first victim being posted. Ephemeral groups often employ underdeveloped or rudimentary communication methods and infrastructure and may recycle commodity malware and/or leaked ransom builders in their operations. Ephemeral groups are unlikely to have operated under the RaaS model, as the time and development required to sustain such a model are incompatible with their short-lived operations.

Colloquially, the terms “no-name,” “immature,” “rudimentary,” and “commodity” have all been applied to similar groups and "non-branded" operations that do not appear to maintain long-term operations or develop their own TTPs and malware.

Use of Leaked Builders and Commodity Malware by Ephemeral Groups

Observed Behavior

In 2023, GRIT staff directly observed an increasing number of ephemeral or commodity ransomware groups during incident response and threat actor communications cases. While this is anecdotal evidence, security reporting and industry colleagues continue to report the prevalence of these groups, particularly against Small to Medium Sized Businesses (SMBs).

As ephemeral groups frequently rely on "second-hand" malware and ransomware, technical barriers to entry for members of the group are reduced. However, this dependence also frequently prevents in-depth understanding and the ability of group members to troubleshoot issues with malware or ransomware. This shallow understanding has led to unforeseen problems with encryption and/or decryption and group members who are unable or unwilling to correct issues. When such groups encounter problems after receiving payment, there is little incentive to expend resources toward resolution for the victim.

Ephemeral groups conducting negotiations often appear impatient, impulsive, and inconsistent throughout contact. We assess that this may stem from undefined or poorly defined processes for communications, a desire to quickly cycle through victims, or inexperienced operators.

Ephemeral groups do not benefit from maintaining a reputation or brand awareness, which reduces the risk of continued operations from deceiving victims or failing to follow through on agreements. As Ephemeral groups are likely driven to cycle through smaller victims and extract ransoms as quickly as possible and lack sufficient technical prowess to conduct effective operations, we have observed an increased willingness to attempt deception of victims and exaggerate the impact of intrusions. This most often applies to data exfiltration, with groups that have exfiltrated little or no data attempting to create the impression of widespread data theft.

Risks

GRIT advises enterprise teams and defenders to consider Ephemeral or unbranded ransomware groups as unique threat models distinct from ransomware-as-a-service and Established ransomware groups. We base this recommendation on the lower level of technical sophistication exhibited by such groups, the increased likelihood of deception in communications, and the reduced reliability and predictability of such groups in settlement and resolving decryption issues. While decisions to pay or not pay a ransom are those of individual victims, we advise that any organizations impacted by an Ephemeral group consider the increased risks of doing so, particularly in instances where recovery is feasible absent a decryptor.

Based on the observed behavior of Ephemeral groups, victims that opt to pursue a settlement with an Ephemeral group face an increased risk of technical issues in the decryption process and abandonment by the group in seeking troubleshooting or follow-on support to restore systems. Decryptors may be non-functioning or partially functioning and based on open-source encryption software or leaked builders from other ransomware groups. Partial but incomplete decryption and corrupted files are commonly observed during first attempts at resolution, though some groups have successfully resolved decryption issues.

While rare in most modern ransomware operations, we have observed Ephemeral groups attempt to renege on agreements or extort victims for additional ransom payments, particularly in instances that require multiple decryptors or prolonged support. We do not know whether this is driven by a short-term myopic approach to operations or as an excuse to break off communications in situations where the group cannot provide a working decryptor. We assess, based on this behavior, that the likelihood of re-extortion and sale of victim data may be higher amongst Ephemeral groups, even in cases where a ransom is paid.

Novel Coercive Techniques in 2023

Intent and effectiveness

We have primarily observed novel coercive techniques deployed against larger targets likely to have been extorted for substantial ransoms as part of a so-called “big game hunting” approach. While this may be due in part to the outsized media coverage that attacks against large organizations attracts, we assess that this trend likely also represents increased resource allocation by ransomware groups to extract disproportionately high ransoms from victims deemed able to pay.

In addition to attempting to coerce non-compliant victims, novel coercive techniques also likely serve a dual purpose of discouraging non-compliance from future victims. In the same way that fear of sensitive data being posted may have historically encouraged compliance from victims, fear of reputational damage and negative press coverage presents an additional problem that may justify compliance on the client's part.

As Ransomware-as-a-Service groups compete for limited affiliates, highly publicized coercive tactics may also serve to burnish the brands of participating groups, creating an air of ruthlessness and effectiveness that affiliates may find desirable. The media coverage of these tactics almost certainly increases the name recognition of associated groups and may support recruitment in the future.

Assessed future use

We have observed the increased use of novel coercive techniques by an increasing range of ransomware groups throughout 2023; although Alphv remains the most prolific in deploying these tactics, LockBit, Medusa, BlogXX, and Hunters International have done so as well. We assess that the use of novel coercive techniques by ransomware groups will increase and continue to evolve in 2024.

While we lack insight into the success of novel coercive techniques to date, we consider it unlikely that novel coercive techniques will decrease the rates of payment from future victims, based on the observed continuing operational pace of the associated groups, continued use of these tactics, and our discussions with colleagues across the industry.

While we continue to assess that the use of these techniques by ransomware groups will attract considerable law enforcement attention, December’s takedown of Alphv’s dark web blog and subsequent resurgence highlighted the resilience of established ransomware groups. Absent particularly successful and aggressive law enforcement efforts, we consider it unlikely that the risks of law enforcement disruption will outweigh the perceived benefits of novel coercive techniques in the form of ransom payments, increased compliance, or recruitment of affiliates over time.

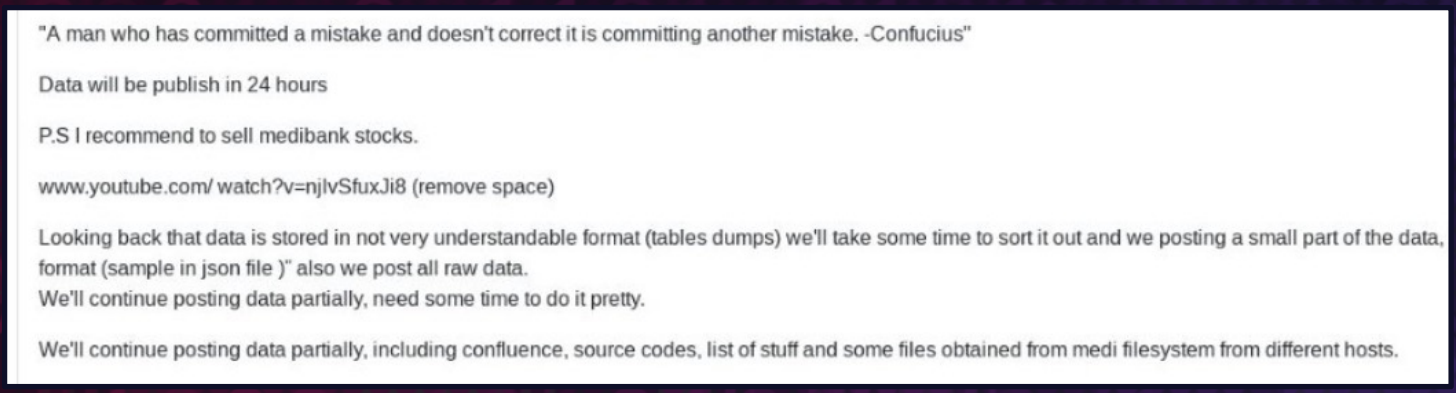
Novel Coercive Techniques Defined

GRIT first explored the topic of novel coercive techniques, and specifically selective public leaks, in Q1 of 2023. Today, we define novel coercive techniques as those exhortative actions taken by cybercrime groups outside of single, double, or triple extortion operations, designed to employ unique approaches to increase the perceived cost of non-compliance by victims. Over the course of 2023, this has included selective public data leaks or direct extortion of and threats to a victim's customers, patients, or clients. Given the resources and time associated with these efforts, novel coercive techniques have been most frequently associated with larger, Established ransomware groups, which almost certainly benefit from substantial resource pools.

Examples of Novel Coercive Techniques in 2023

BlogXX releases patient information

In a late 2022 attack against an Australian Health Insurer, potential REvil affiliated group BlogXX leaked alleged lists of patients who had received abortions and mental health treatment after the victim refused to pay a $10 million dollar ransom demand. The lists were posted with accusations that the victim's CEO "refuses to pay for yours [sic] data more, like 1 USD per person. So, probably customers data and extra efforts don't cost that."



"A man who has committed a mistake and doesn't correct it is committing another mistake. -Confucius"

Data will be publish in 24 hours

P.S I recommend to sell medibank stocks.

www.youtube.com/ watch?v=njlvSfuxJi8 (remove space)

Looking back that data is stored in not very understandable format (tables dumps) we'll take some time to sort it out and we posting a small part of the data, format (sample in json file)" also we post all raw data.
We'll continue posting data partially, need some time to do it pretty.

We'll continue posting data partially, including confluence, source codes, list of stuff and some files obtained from medi filesystem from different hosts.

LockBit releases failed negotiation chats

In early 2023, the LockBit ransomware group published "failed" negotiation chat logs with a ransomware victim, adding a comment that the victim "should have chosen better negotiators." Although this is not an inherently new extortion technique, this approach is likely intended to discourage aggressive negotiation approaches and increase the impact of "shaming" efforts by the threat group. Posts of ransomware negotiation chats appear to have become more common in 2023, particularly in response to failed negotiations or instances where the TA believes they were "strung along."

Alphv releases cancer patient photos

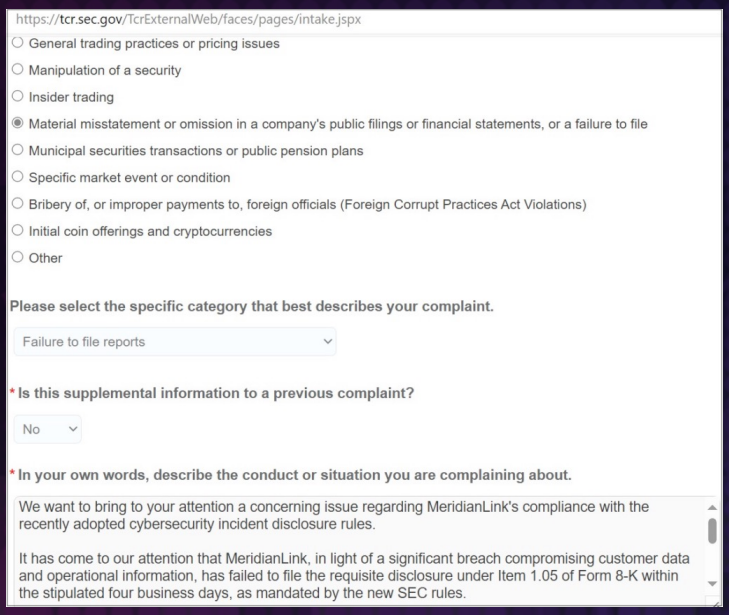
In an early 2023 ransomware attack against a U.S. healthcare network, Alphv leaked sensitive clinical photos of cancer patients after the network refused to pay a ransom. Alphv celebrated the leak, stating "Our blog is followed by a lot of world media, the case will be widely publicized and will cause significant damage to your business".

Medusa publishes student data

In a February 2023 attack against an urban school district, the Emerging ransomware group Medusa published screenshots of notes describing sexual assault allegations after the district refused to pay the group's ransom demands. The group also posted a video of their reviewing the exfiltrated data and provided an option on their data leak site for anyone to pay the ransom, a previously unobserved tactic.

Additional Alphv publicity seeking behavior

In November 2023, following an attack on a software company, Established ransomware group Alphv released a post and screenshots as proof that they had filed a complaint to the Securities and Exchange Commission (SEC) regarding the victim's alleged "material misstatement or omission." Specifically, Alphv sought to highlight the victim's failure to report the breach within four business days in accordance with new SEC rules. The incident attracted demonstrable media attention, specifically within the security space.


https://tcr.sec.gov/TcrExternalWeb/faces/pages/intake.jspx

- General trading practices or pricing issues
- Manipulation of a security
- Insider trading
- (•) Material misstatement or omission in a company's public filings or financial statements, or a failure to file
- Municipal securities transactions or public pension plans
- Specific market event or condition
- Bribery of, or improper payments to, foreign officials (Foreign Corrupt Practices Act Violations)
- Initial coin offerings and cryptocurrencies
- Other

Please select the specific category that best describes your complaint.

Failure to file reports

*** Is this supplemental information to a previous complaint?**

No

*** In your own words, describe the conduct or situation you are complaining about.**

We want to bring to your attention a concerning issue regarding MeridianLink's compliance with the recently adopted cybersecurity incident disclosure rules.

It has come to our attention that MeridianLink, in light of a significant breach compromising customer data and operational information, has failed to file the requisite disclosure under Item 1.05 of Form 8-K within the stipulated four business days, as mandated by the new SEC rules.

In September, Alphv claimed responsibility for a highly publicized attack against MGM Resorts. Following widespread media coverage detailing outages at MGM properties, Alphv released a statement detailing how the group's affiliate had allegedly gained access, while attempting to highlight repeated alleged failures to evict the group from MGM's networks. The group closed the statement by claiming continued access and threatening to carry out additional attacks if not contacted.

LockBit's use of social media bot accounts in October

From October to November 2023, Established ransomware group LockBit attempted to extort a relocation services company. When negotiations broke down, LockBit amplified claims of the attack and tagged multiple corporate partners on the social media site X, formerly known as Twitter. The group used what appeared to be a series of bot accounts to repost, like, and otherwise share the posts, and later released copies of the negotiation messages.

Hunters International Extorts Healthcare Client

In December 2023, Emerging ransomware group Hunters International claimed responsibility for an attack against a cancer medical center. Likely following non-payment of the group's ransom demands, the group contacted an unknown number of the center's patients, threatening the release of private information and offering removal of individual data for $50. A few weeks later, clients of a non-profit health network received similar messages and offers to remove their data for $50. While the secondary attack has not been attributed to Hunters International at the time of this report, we note the similarities in behaviors as a probable indicator of tactic reuse by Hunters International, or adaptation by another group.

Signposts of Ransomware Activity and 2024 Outlook

Signpost analysis defined

In reviewing 2023's ransomware trends, GRIT analyzed and considered potential signposts or indicators contributing to increases or decreases in ransomware operations or ransom payment rates. These indicators are anecdotal in nature but were reviewed critically for feasibility of impact and consistent observations over the preceding two years. In addition to evaluating the assessed positive or negative impact on ransomware operations writ large, GRIT staff also assessed the direction (likelihood increasing or decreasing) of each indicator moving into 2024. The end result, presented here, is a consolidated signpost analysis of contributing factors and their assessed direction in 2024.

Impact on Ransomware	Discourages Ransom Payments or Reduces Ransomware Operations	Has no Impact on Ransom Payments or Ransomware Operations	Encourages Ransom Payments or Increases Ransomware Operations
			
Assessed Direction of Trend	Likely to Decrease in Frequency	Unlikely to Increase or Decrease in Frequency	Likely to Increase in Frequency
			

Trend	Impact on Ransomware	Direction in 2024
Posted ransomware victims continue to increase in volume Increases in ransomware victim volume are expected to continue until the point of saturation, with additional actors seeking entry while prospects of revenue generation remain.		
Instances of novel coercive techniques increase in frequency and sophistication Effective and novel coercive techniques are expected to continue, with fear of reputational impacts, news coverage, and client/customer extortion impacting willingness of some victims to pay.		
Additional ransomware builders of Established ransomware groups, and/or commodity malware are released or leaked Sporadic leaks of ransomware builders and commodity malware are expected, presenting new opportunities and reducing technical barriers to entry for new entrants.		
Law Enforcement operations to disrupt, arrest, and try ransomware operators increase LE disruption of ransomware operations is expected to remain steady, with particularly impactful disruption likely to deter new entrants and discourage current ransomware operators.		
Inflation increases or currency value decreases in Russia and Central Asian states Economic impacts of Russia's war on Ukraine are expected to continue, driving economic hardship that may encourage new entrants.		
US, UK, or EU governments adopt additional reporting requirements for ransomware victims Increased reporting requirements are expected in the short-to-medium term, increasing awareness of Ransomware's pervasiveness and discouraging payment by victims.		
US, UK, or EU governments adopt bans on ransom payments Outright bans on ransom payments are not anticipated in the near term, though their implementation would almost certainly reduce ransomware operations and payments.		

Trend	Impact on Ransomware	Direction in 2024
"Zero-Day" vulnerabilities in enterprise software increase Ransomware operators are likely to continue seeking zero-day vulnerabilities and developing or purchasing accompanying exploits as a means to gain initial access and overcome increasing security capabilities. Some vulnerabilities may become part of mass-exploitation campaigns, generating substantial victim volume.		
Publication or leaks of free ransomware decryptors increases Publication or leaks of ransomware decryptors, from security organizations or law enforcement, is expected to continue, and serve as at least a temporary setback to double-extortion operations.		
Cybersecurity liability insurance rates increase substantially, coverage options decrease, or ransom reimbursements decrease Costs are expected to increase in the short-to-mid-term, reducing ransom coverage and thereby the ability of victims to pay ransoms at current rates.		
Additional international sanctions are placed on named ransomware groups, restricting ransom payments to known established groups Additional group-specific sanctions are not anticipated, though implementation would deer and effectively criminalize many ransom payments.		
Substantial leak or compromise of internal group communications for prolific Established ransomware group (à la Conti Leaks) Embarrassing revelations and leaks of prominent ransomware groups are not anticipated, but would likely lead to dissolution, splintering, or rebranding of impacted groups.		
Ransomware groups increasingly implement negotiation restrictions, such as minimum ransom amounts or "discount" percentages Increased implementation of negotiation restrictions may occur in the short-mid-term following LockBit's model, though such restrictions could eliminate the ability of many victims to pay, reducing total revenue for affiliates.		
High-impact, high-visibility ransomware event resulting in physical damage or casualties Severe, catastrophic physical impacts of ransomware may or may not occur but would more likely result from an accident than deliberate intent. Negative press and law enforcement attention from such an incident would likely lead some groups, affiliates, or individual operators to "go to ground" to avoid detention.		

2023 Final Remarks and Summary

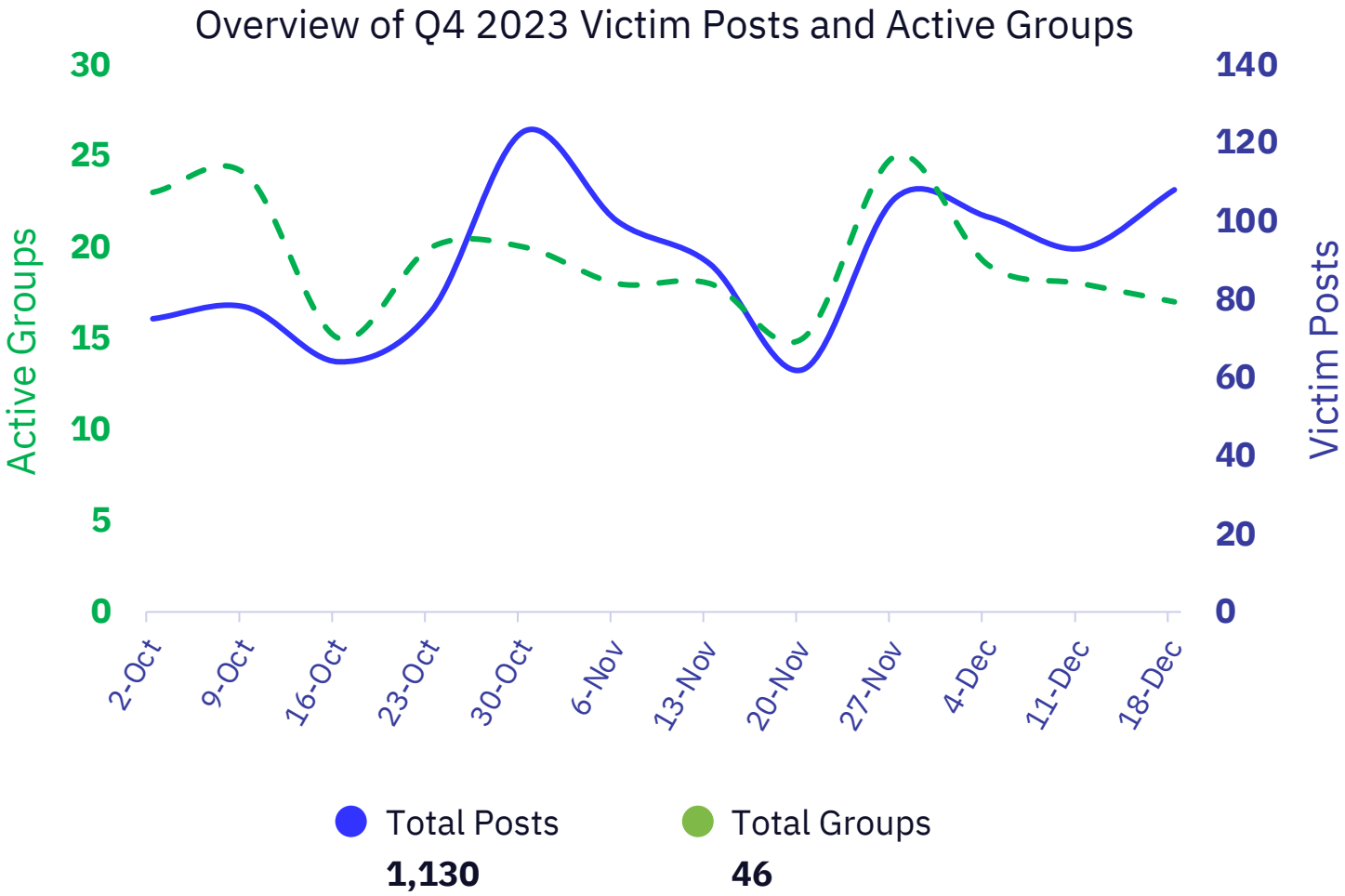
In 2023, ransomware continued to increase in terms of impact, sophistication, and the number of participating actors, an indication that the ransomware ecosystem has not yet reached a point of market saturation. As with any economic microcosm, this point will eventually be reached through continued increases or outside impacts on the market that drive the saturation point lower. Put another way, we can expect ransomware impacts to continue an upward trajectory into 2024 and beyond until such a point that ransomware groups' financial interests conflict with one another or until law enforcement and regulatory pressures reduce the perceived attractiveness of the space and the risk calculus of its participants.

In the same vein, the success of ransomware groups amidst other cybercriminals will continue to encourage impostors, shysters, and frauds eager to exploit society's fear of ransomware to generate a profit by other means. Scrutiny of threat actor claims, both public and private, will become an increasing imperative for defenders in order to defend and deter against data re-extortion and identify exaggerated claims. As is often said and often overlooked in our community of practice: ransomware operators, extortion groups, and hacker collectives are criminals, and we trust or believe them at our own peril.

Ransomware’s “heaviest hitters,” as reflected in long-term, Established and prolific groups such as LockBit, Alphv, and Clop, continue to account for not just the lion’s share of victims but also much of the innovation and tactical changes across the ransomware ecosystem. TTPs and behaviors exhibited by these groups inevitably trickle down to less mature ransomware groups seeking to increase effectiveness and revenue generation. This hierarchy reflects the importance of law enforcement disruption and security research exposing the operations of these groups, with operational disruption against them likely to generate the greatest impacts on the ransomware economy.

As 2024 unfolds, Defenders and the security community are increasingly aware of and prepared for the threat of ransomware. Our future success will depend on our ability to adapt to and match the paces of a committed, resilient, and increasingly professionalized adversary. To this end, industry best practices in threat intelligence, information sharing, and public-private partnerships remain our most viable and effective options to force adversaries to cede ground.

Appendix: Q4 2023 Ransomware Observations



Overall, Q4 2023 was slower than preceding quarters, with the lowest volume of observed victims (1130) since Q1 (859). Additionally, October and December had the lowest volume of posted single-month victims at 336 and 361, respectively, since February, which only saw 242 victims.

In terms of group activity, the soft-spoken Established group, Play, was an outlier, jumping from fifth place with 71 victim posts in Q3 to second place with 113 victim posts in Q4, continuing an upward trend. This jump was the largest increase in victim volume among any Ransomware group in Q4.

Conversely, GRIT observed the greatest drop in activity from Clop, which decreased from 171 posted victims in Q3 to only 4 in Q4, despite maintaining an active leak site and an additional site dedicated to the sharing of torrents containing leaked victim data. We assess that this drop corresponds with Clop's shift from "traditional" ransomware operations and towards a focus on mass-exploitation of vulnerabilities and a campaign-style approach to operations.

Appendix: GRIT Ransomware Taxonomy

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

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

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

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

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

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

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

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

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