GUIDEPOINT® SECURITY

GRIT
Ransomware Report

Q1, JANUARY – MARCH 2023

Methodology

Data collected for this report was obtained from publicly available resources, including threat groups themselves, and has not been validated by alleged victims. Thus, the number of publicly observed attacks and the actual number of attacks conducted may not be equal. Some groups do not publicize all victims, and almost all groups offer an option to avoid public announcements if their victims pay the ransom within a specified timeframe, or offer to remove public postings of the victim once a ransom has been paid. Additionally, some groups exaggerate their numbers by including incomplete information about their victim or claiming 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.

Contents

QUARTERLY

Ransomware Summary

Q1 of 2023 closed with an increase in publicly posted ransomware victims, continuing to impact worldwide organizations agnostic of industry. LockBit remains the most prolific ransomware threat group, and the rapid and widespread exploitation of a file-sharing application vulnerability brought cl0p into a leading position. Vice Society remains the most impactful group targeting the education sector, supporting the assertion that some groups maintain a consistent targeting profile.

GRIT continues to monitor evolving tactics, techniques, and procedures demonstrated by ransomware threat actors seeking to adapt to an increasingly crowded Ransomware-as-a-Service (RaaS) ecosystem. Increases in "Data Only" extortion efforts and increasingly coercive selective public leaks are examples of new methods employed by these threat actors to maintain profitability and market share.

Manufacturing, Technology, Education, Banking and Finance, and Healthcare organizations continue to represent the majority of publicly posted ransomware victims, probably reflecting the frequency with which threat actors target highly sensitive data and inadequately defended organizations.

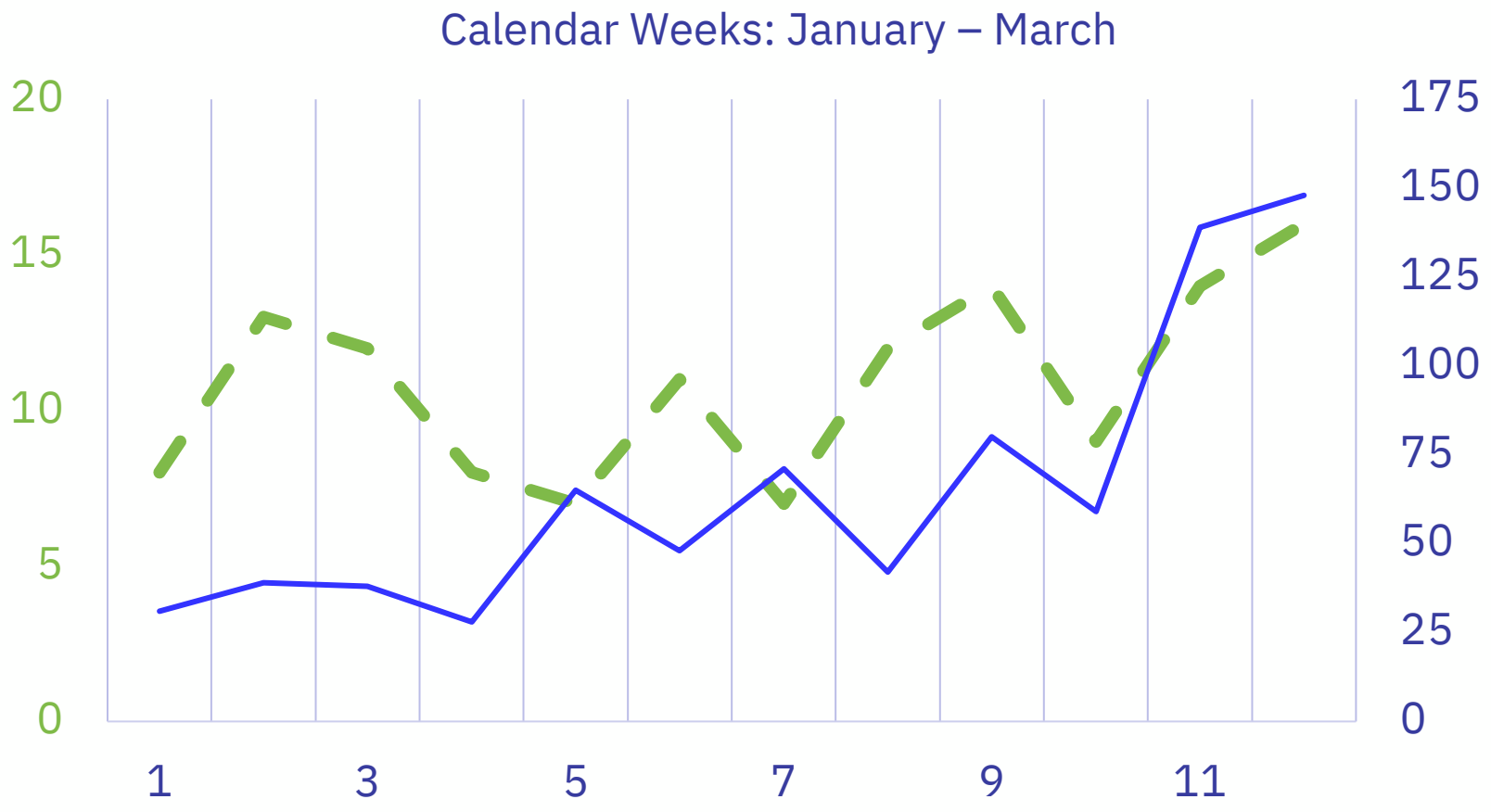
The United States continues to bear the brunt of global ransomware attacks, followed by the United Kingdom, Germany, Canada, France, and others. Though not approaching the volume seen in the western world, we continue to see notable numbers of attacks impacting other countries around the world – from Bangladesh to Barbados.

Total Publicly Posted Ransomware Victims	849
Number of Tracked Ransomware Groups	29
Average Posting Rate (per day)	9.46

Rate of Publicly Posted Ransomware Victims (Q1 2023)

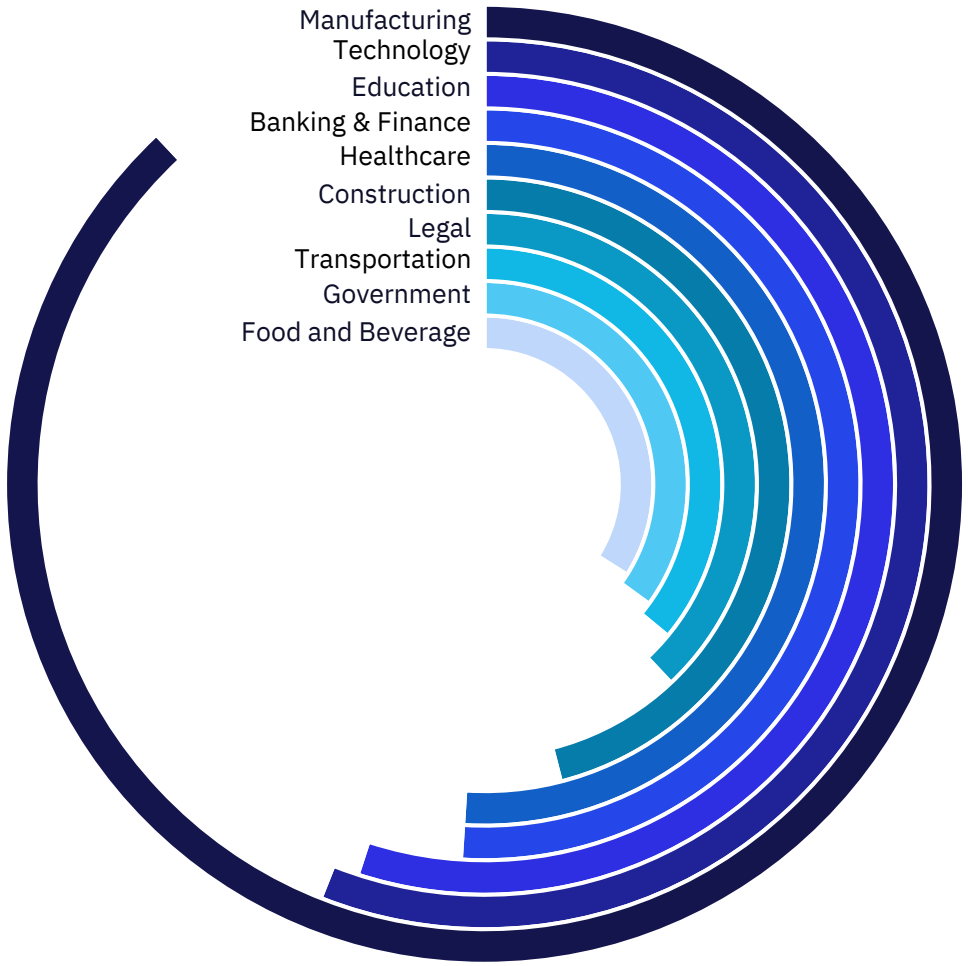
Repeating the patterns observed in 2022, postings at the beginning of Q1 2023 started at a slow but consistent pace that steadily rose throughout the quarter, with a surge at the end of the quarter brought on by cl0p's exploitation of a vulnerability in GoAnywhere Managed File Transfer software. However, GRIT observed a 27% increase in public ransomware victims compared to the same period last year, and a 25% increase from Q4 to Q1.

We observed a slight increase in Ransomware as a Service (RaaS) groups operating throughout the quarter, which can be attributed to the five new groups that began their operations this quarter.



Total Posts	Total Groups	Average Posts / Week	Average Groups / Week
849	**29**	**65**	**11**

Most Impacted Industries – Top 10 – Q1 2023



Manufacturing

- LockBit
- Royal
- AlphV

Education

- Vice Society
- LockBit
- Royal

Technology

- LockBit
- cl0p
- BianLian

Banking & Finance

- LockBit
- cl0p
- AlphV

Unsurprisingly, Manufacturing and Technology continued to be the most impacted sectors during Q1, a trend that persisted from our observations in 2022.

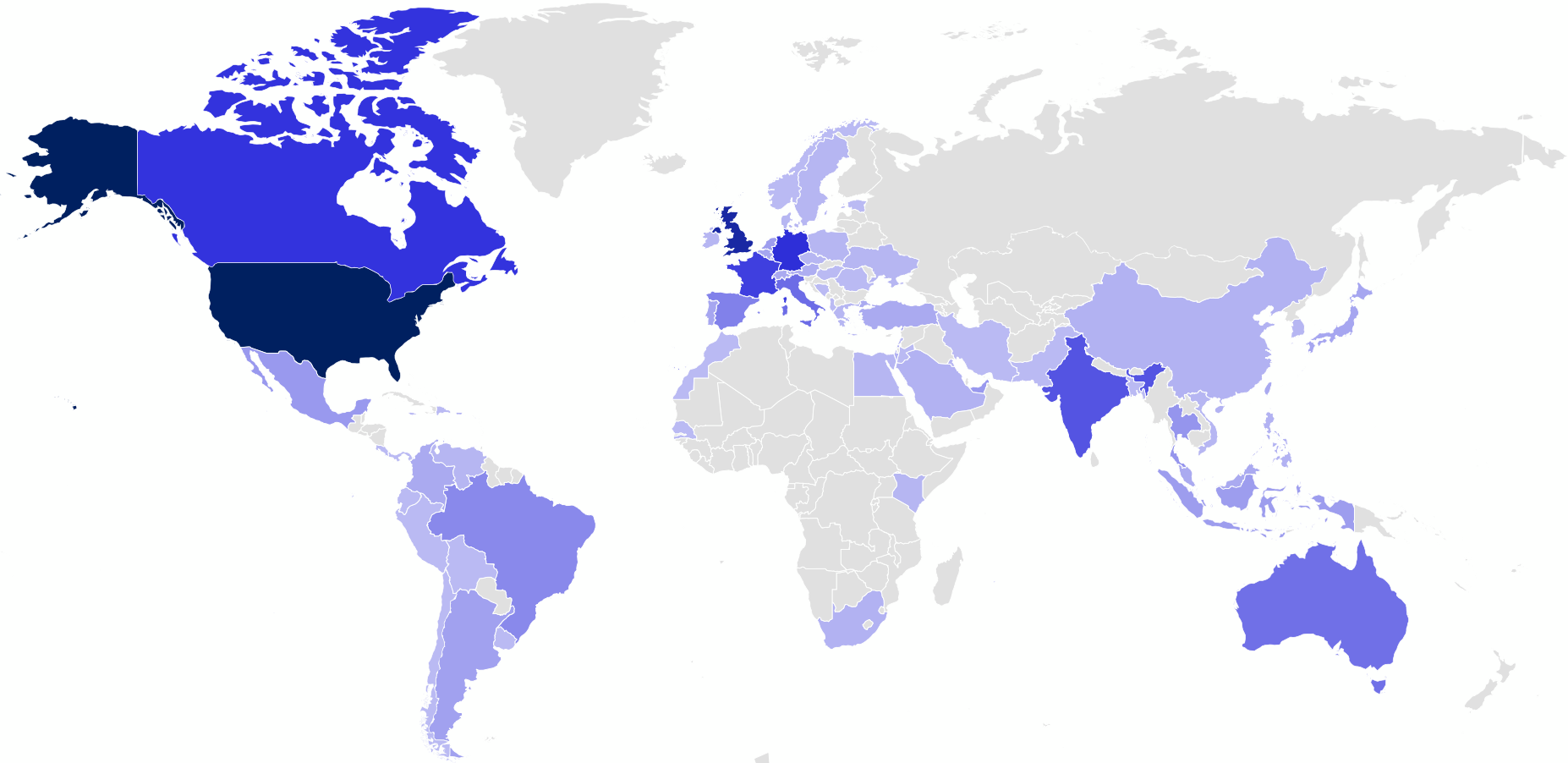
In notable moves, observed victims in the legal industry increased 65% from Q4 of last year to Q1 of this year. Of those victims, 70% were attributed to the most prolific “double extortion” model ransomware groups–LockBit, AlphV, Royal, and BlackBasta. As the “business” of ransomware continues to evolve, this increase could reflect the attractive draw of exfiltrating sensitive legal data that ransomware groups would likely view as more coercive leverage.

Finally, the Education industry saw a 17% increase in posted victims from Q4 to Q1, with Vice Society accounting for 27% of all education-based activity.

Geographic Breakdown of Ransomware Victims (Q1 2023)

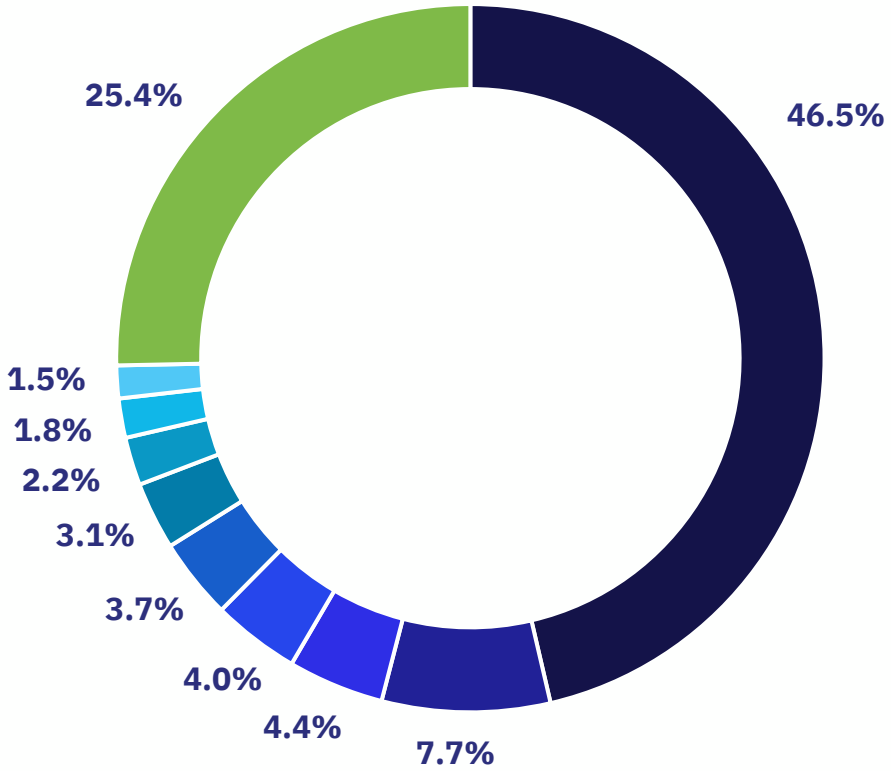
Top 10:

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

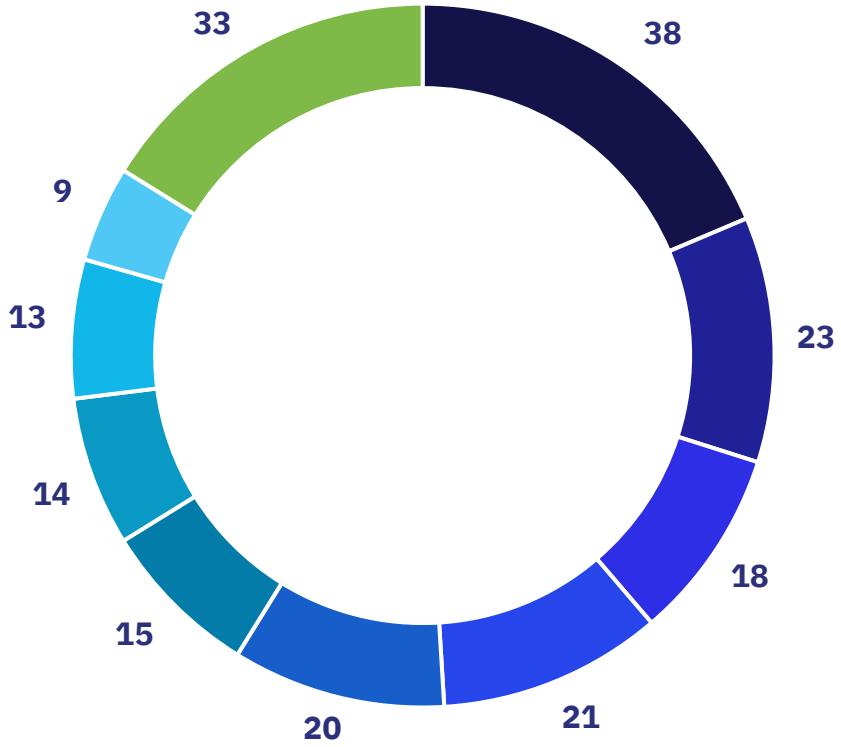


Country Breakdown (All Threat Actors)

Percent of Total Victims



Industries Targeted

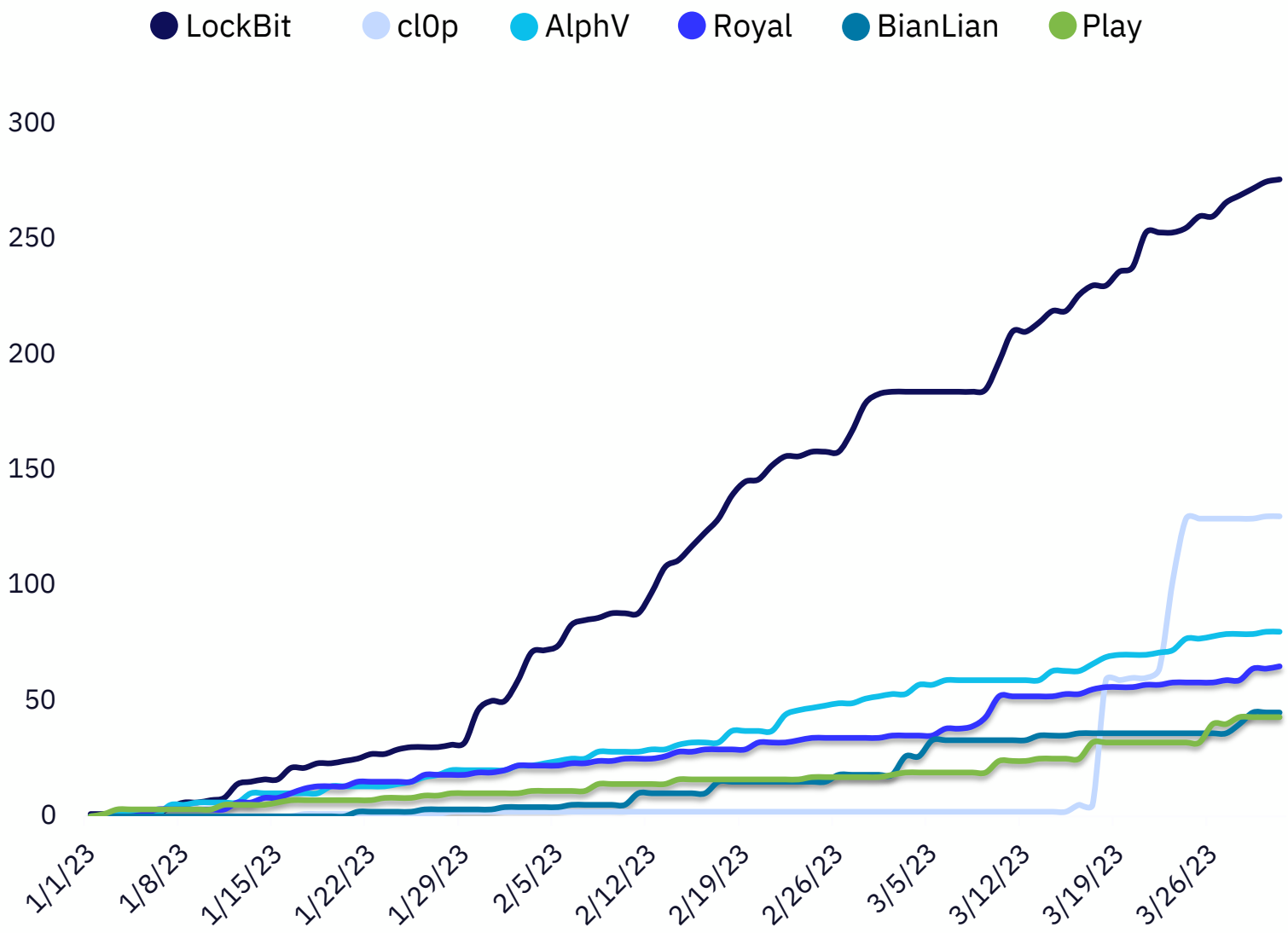


United States
Canada
Australia
All Others
United Kingdom
France
Spain
Germany
India
Brazil

US-based organizations remained the most heavily impacted by ransomware, making up 46% (395 of 851 total) observed victims in Q1. This is consistent with the ratio observed in Q4, where US victims accounted for 45% of victims (301 out of 676). The current ratio appears to be holding steady since first increasing from approximately 40% in Q2-Q3 2022.

Outside the US, observed attacks against organizations based in India appear to be accelerating. This increase is driven mainly by LockBit, which accounts for 35% of the attacks over the past two quarters. Between Q2 and Q3 of 2022, there were only 14 observed attacks, and in Q4 of 2022 and Q1 of 2023 that number has ballooned to 40.

Cumulative Victims by Threat Group

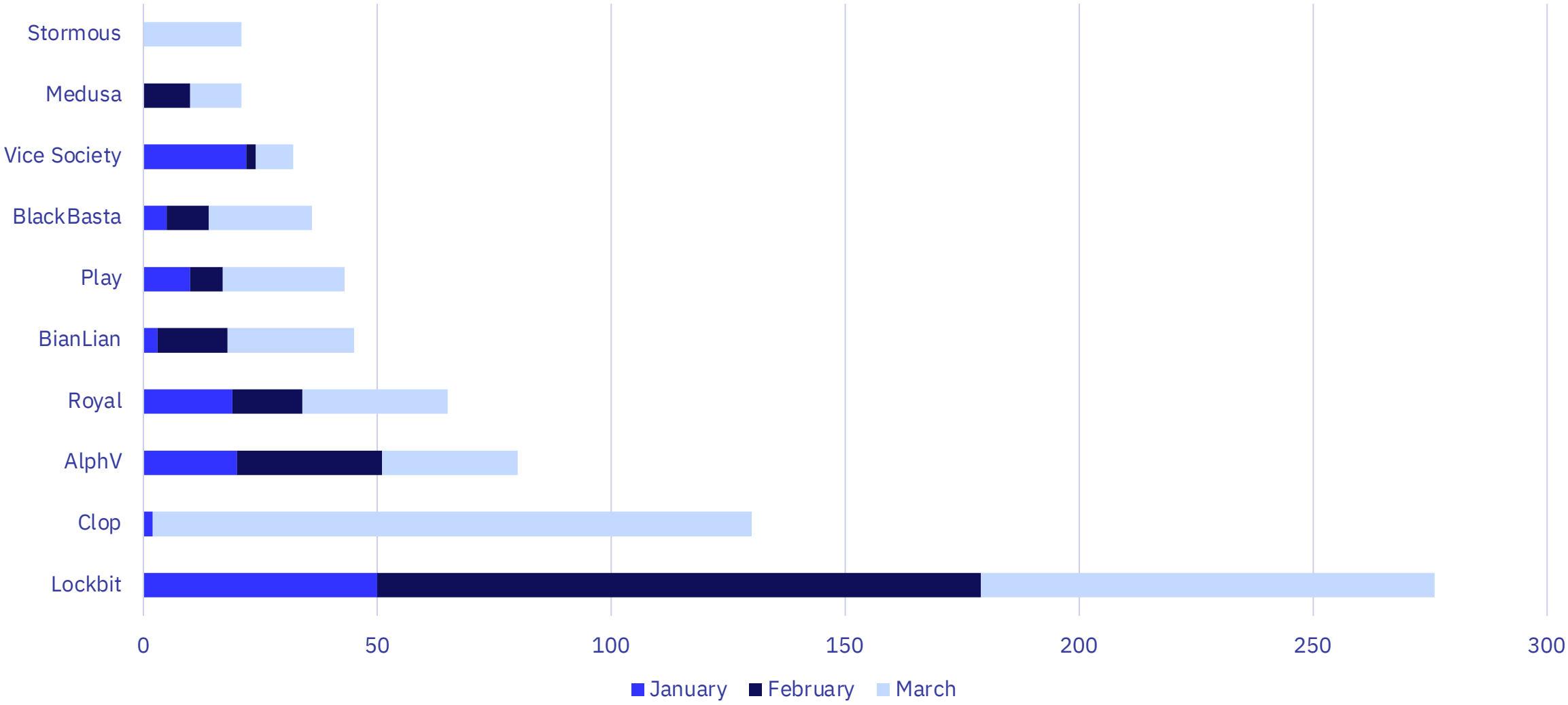


LockBit remains the most prolific ransomware threat group, and GRIT has observed an increase in both the number of posted victims and their share of reported attacks. LockBit's reported victims decreased 31% from Q3-Q4 2022 before this quarter's increase of 15% (276 victims, up from 240 in Q4). LockBit's share of affected victims also increased in Q1 from 21% (145 of 676) to 32% (276 of 851).

A widespread exploitation of vulnerable GoAnywhere instances led to cl0p claiming a significant share of victims in Q1. cl0p only had two public victims across January and February, before claiming 128 victims in March.

AlphV primarily impacted legal or banking and finance industry victims in Q1, increasing the number of publicly posted victims 16% from 69 in Q4 2022 to 80 in Q1 2023.

Top 10 Ransomware Threat Actors



Industry Spotlight

Education

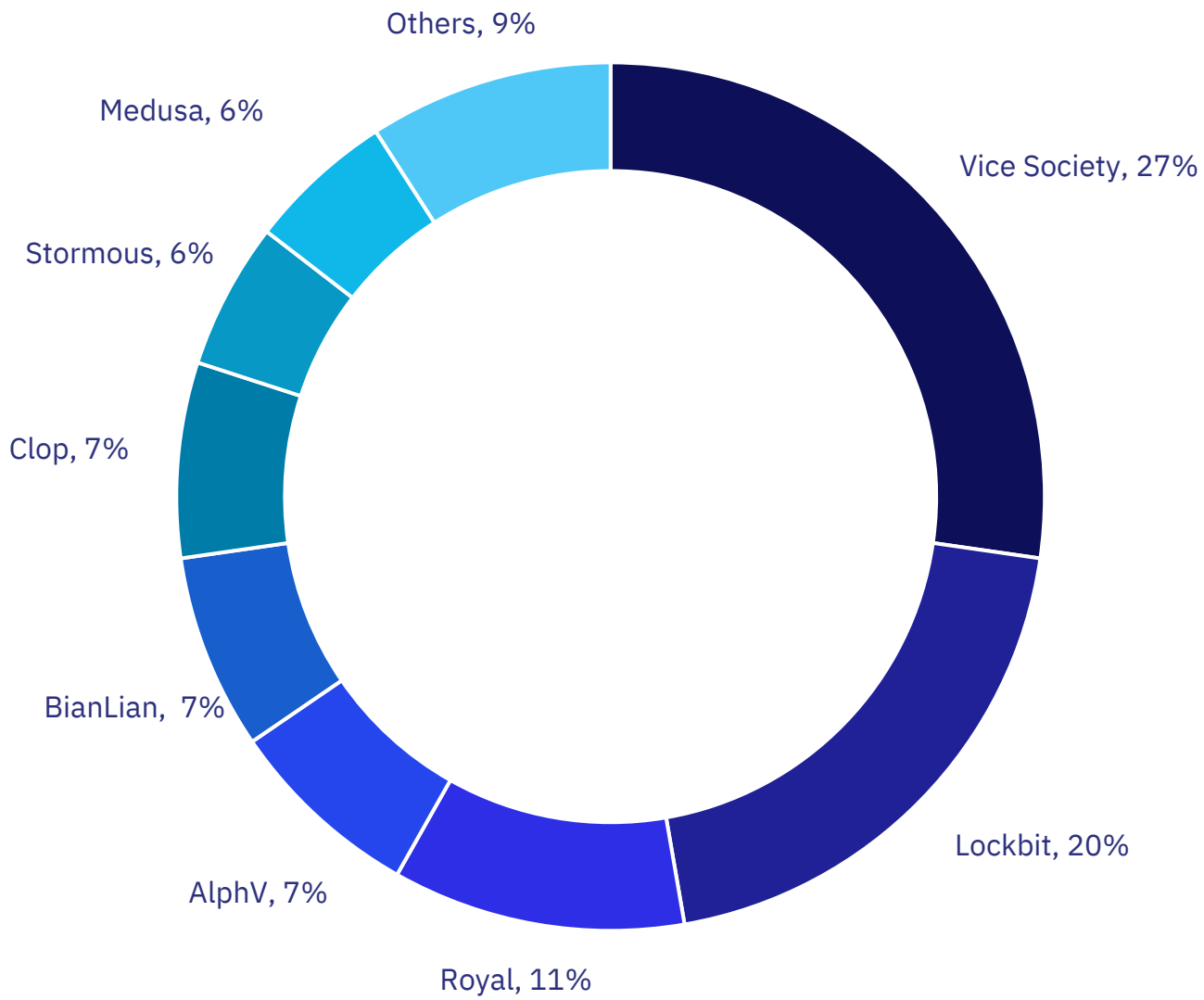
Ransomware Threat Groups Targeting Education

Vice Society remains the most dominant threat actor impacting the education sector. Although Vice Society represents 27% of publicly claimed education victims (down 1% from Q4 2022), they have increased their overall quarterly victim count by two.

LockBit has increased their share of public education victims by 9% in Q1 2023 compared to Q4 2022, accounting for 20% of all publicly posted education victims. Among LockBit's more prominent education victims in Q1 was Western Michigan University.

Although long-time, "fly-under-the-radar" groups like Medusa and ambitious groups like Royal make up a small percentage of total education victims, they are both associated with high-impact attacks against large K-12 public school districts, including the Minneapolis School District and Dallas Public Schools.

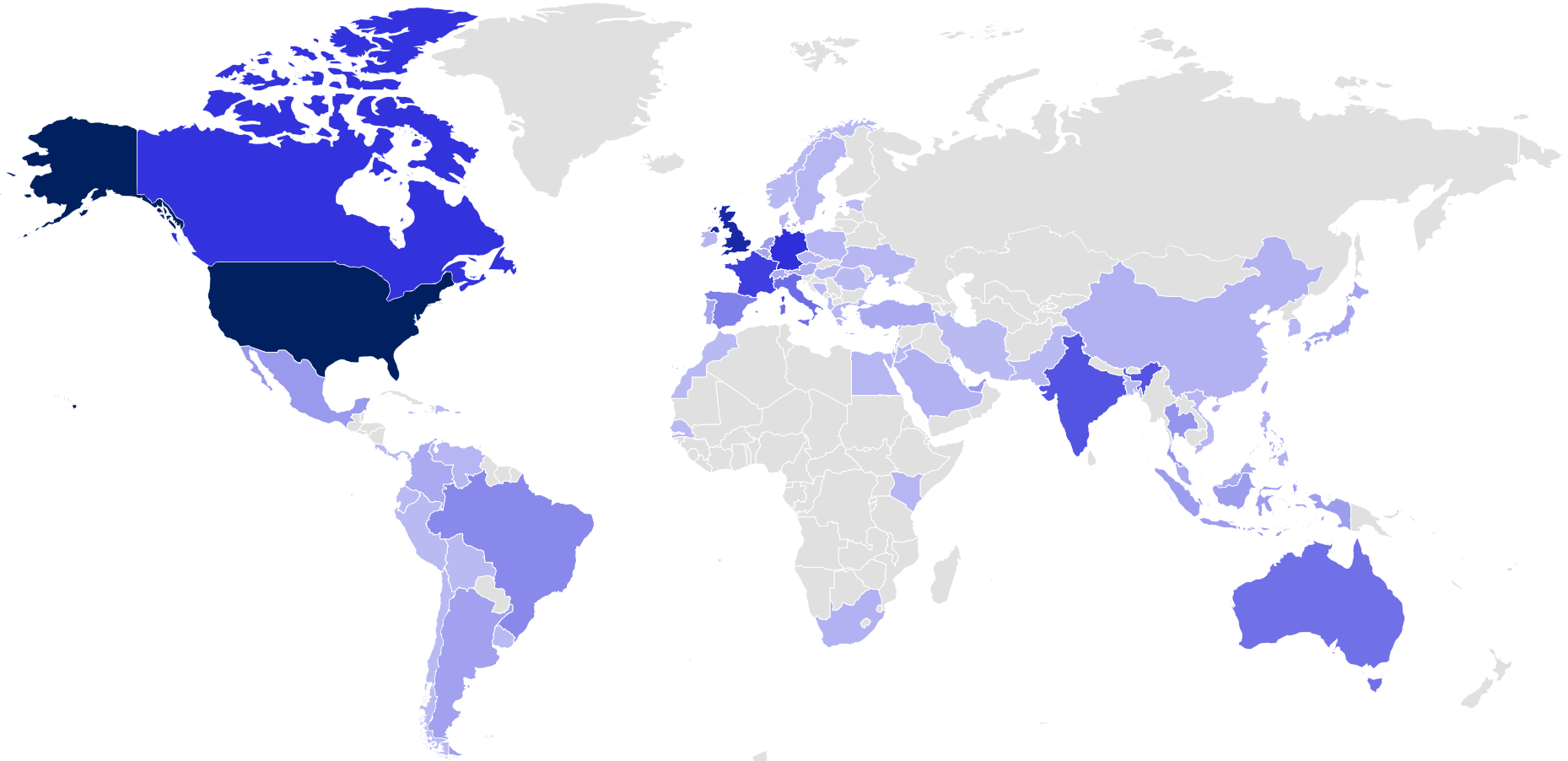
GRIT's review of education trends from 2022-2023 shows a consistent victimization of the education sector regardless of quarter. Because of this year-round victimization, we assess that the actions of students are not consistently the "weak link" in ransomware intrusions against educational institutions.



Geographic Breakdown of Ransomware Victims (Education Industry – Q1 2023)

Countries Targeted

1. United States
2. United Kingdom
3. Australia
4. Germany
5. France/Brazil



Other Industry Trends

In Q1, GRIT observed a noticeable increase in reported victims associated with the Legal and Engineering industries.

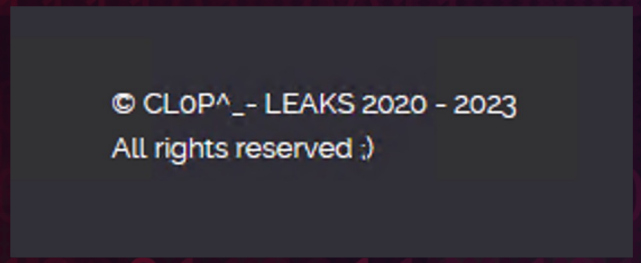
GRIT assesses with moderate confidence that the Legal and Engineering industries continue to be heavily impacted based on the probable perception by threat actors that they often maintain sensitive personal data or intellectual property which they are contractually obligated to protect. This may make organizations in these industries more attractive to attackers pursuing data extortion attacks, either alone or in conjunction with data encryption attacks.

The Legal and Engineering industries, combined, accounted for 31 posted victims in March, a rate of 1 post per day. This represents an over 250% increase from an average of .377 posts per day during 2022.

AlphV and LockBit each claimed 24% of observed legal industry victims during Q1, while LockBit claimed responsibility for 52% of all observed Engineering victims.

Threat Actor Spotlight

Cl0p Ransomware Group



cl0p

Threat Actor Statistics

Clop (often stylized as cl0p) has been observed conducting ransomware attacks leveraging single and double extortion techniques against victims across multiple industries since February of 2019. While cl0p has primarily impacted North American organizations, it has also been observed impacting organizations in the United Kingdom, Germany, Australia, and others.

cl0p tends to cluster its activity, often ending large periods of seeming inactivity by extorting several victims at a time. This tactic was recently demonstrated by a series of attacks carried out this quarter against users of the GoAnywhere MFT secure file-sharing solution. GoAnywhere MFT is widely used by US and Western organizations, which allowed cl0p to leverage a vulnerability (CVE-2023-0669) to exfiltrate sensitive data from a wide range of customers who had not yet patched the vulnerability. In March 2023 alone, cl0p claimed 128 victims on its leak site, most of which appear to have been related to the exploitation of the GoAnywhere vulnerability.

This is not the first time that cl0p has employed this tactic. GRIT observed another cluster of activity in January of 2021, where cl0p leveraged a vulnerability in Accellion FTA, an enterprise file transfer application with similar functions to GoAnywhere MFT. Given the ubiquity of corporate storage and transfer solutions and cl0p's TTPs to date, GRIT assesses that cl0p will almost certainly continue to attempt exploitation of similar solutions in the near future.

Escalating Coercive Tactics in Ransomware

GRIT has observed an increase in the use of novel coercive tactics by numerous prolific ransomware groups that follow the "double extortion" model of operations. In double extortion, the ransomware operators not only encrypt files on corrupted networks and hosts, but also exfiltrate data. The ransomware groups then leverage the threat of leaking data to the public to coerce compliance with ransom demands.

- 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 actor.

The use of additional coercive tactics when the threat of broad data leaks has failed to induce compliance has been referred to as "triple extortion" in some security reporting. Additional coercive measures have included Distributed Denial of Service (DDoS) attacks and selective public leaks designed to generate media attention and cause reputational damage to organizations.

- The use of Distributed Denial of Service (DDoS) attacks as an additional tool to coerce compliance by ransomware actors rose to prominence in 2020, and has since been incorporated by a diverse range of actors, including AlphV and LockBit. Ransomware groups may initiate DDoS attacks when victims fail to reply or engage with them as indicated in ransom notes, or upon failure to reach a negotiated settlement.

Escalating Coercive Tactics in Ransomware

The use of selective public leaks is likely more common with larger-sized organization victims, and when exfiltrated data is particularly sensitive, such as with healthcare organizations. The ransomware groups responsible frequently post threatening or braggadocious messaging likely designed to encourage customer outrage and cause reputational damage.

- In a late 2022 attack against Australian Health Insurer Medibank, the group BlogXX, affiliated with REvil, leaked alleged lists of patients who had received abortions and mental health treatment after Medibank refused to pay the $10 million USD ransom demand, according to The Guardian. The lists were posted with accusations that the Medibank 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".
- In an early 2023 ransomware attack against a U.S. healthcare network, AlphV–aka BlackCat–leaked sensitive clinical photos of cancer patients after the network refused to pay the ransom, according to Recorded Future. 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".
- In a February 2023 attack against Minneapolis Public Schools, the emerging ransomware group Medusa published screenshots of notes describing sexual assault allegations after the district refused to pay the group's ransom demands, according to Wired and Ars Technica. The group also posted a video reviewing the exfiltrated data and provided an option on their data leak site for anyone to pay the ransom, a previously unobserved tactic.

Escalating Coercive Tactics in Ransomware

GRIT assesses with moderate confidence that the increased use of "triple extortion" tactics, including selective public leaks, is an attempt by ransomware groups to increase the likelihood of victim compliance with ransom demands, particularly in the face of declining revenues. GRIT makes this assessment based on available reliable security reporting, as well as past background and analysis of the offending ransomware groups.

In early 2023, Blockchain analysis vendor Chainalysis published findings indicating that ransomware revenue had decreased 40% in 2022, a decrease from $765.6 million to $456.8 million. While Chainalysis notes that the true revenue totals are much higher, they retain the assessment that the drop is indicative of an increasing refusal of victims to pay ransoms. This decrease in payments occurred simultaneously with an increase in actual ransomware attacks.

- Given the increasingly crowded Ransomware-as-a-Service ecosystem, the use of selective public leaks could serve a secondary function of brand burnishing, with the goal of not only coercing compliance from ongoing victims, but highlighting the credibility of the offending group and discouraging future victims from rebuffing ransom demands.

GRIT assesses with moderate confidence that more advanced ransomware threat actors–those with strong infrastructure and the capability to successfully exfiltrate and review compromised data–will increasingly deploy novel coercive techniques, particularly as the fallout of existing instances generates media coverage and civil lawsuits against affected organizations. GRIT makes this assessment based on the increased prevalence of these techniques in open-source reporting, as well as our professional understanding of business risk calculus as it pertains to ransomware events.

Rise in Exfiltration-Only Attacks

In Q1 2023, GRIT has observed an uptick in "exfiltration-only" ransomware attacks. In situations where a known Ransomware threat actor has been unable to encrypt a victim's network, either because of defenses or lack of access, they have continued with the extortion process, relying solely on the leverage of data they have successfully exfiltrated. In particular, we observed the ransomware group BianLian moving towards this model of data-centric extortion, probably following the publishing of a universal decryptor for their specific encryption.

When leveraging recent compromises of the GoAnywhere platform, cl0p chose to simply exfiltrate all data that they were able to access, and extort companies solely to prevent its public release. We've also observed multiple ephemeral groups favoring this approach, likely due to the simplicity of execution and reduced need for encryption and additional tools; this further deprives incident responders of evidence that could be used for attribution.

The motivation behind threat actors eschewing encryption in their attempts to monetize their victims is likely as varied as it is unclear. While in theory this type of extortion demands a smaller price tag due to the reduced impact on the victim, GRIT has observed multiple threat actors mining exfiltrated data for specific sensitive information to use in making pointed threats and increased ransom demands during negotiations.

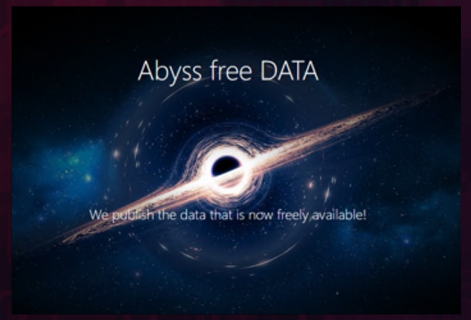
Different industries may very well be affected differently by this trend. For industries such as Manufacturing and Technology, encryption, with or without data exfiltration, is still devastating as it leads to downtime and lost production. The improvement and mass adoption of backup solutions has made recovering from an encryption event possible for most organizations, but restoring operations takes time which may be unacceptable to certain businesses. Companies in the Legal and Healthcare field are unfortunately the most vulnerable to data theft attacks, as they typically control large amounts of sensitive and personally identifiable information.

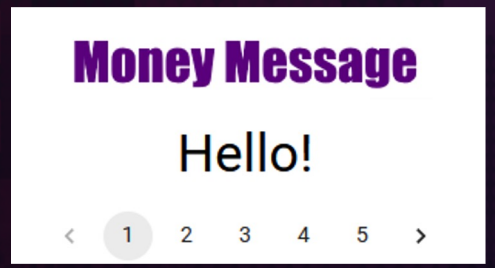
Additional Threat Actor Trends

Q1 saw several interesting trends related to threat actors previously and consistently observed during 2022. Specifically, GRIT observed the following threat actor trends throughout the quarter:

There were five ransomware groups that GRIT began tracking during Q1:

- MoneyMessage
- Abyss
- Vendetta
- FreeCivilian
- Nokoyawa





GRIT is monitoring the emergence of an unbranded and particularly fast ransomware dubbed "Rorschach" or "Bablock" in open-source security reporting. This threat actor allegedly encrypts at nearly twice the speed of LockBit–considered the fastest encryptor–through intermittent encrypting. We lack reporting tying this emerging threat actor to historical Ransomware groups.

GRIT is tracking a possible uptick in ransomware events where initial contact by the threat actor is established via e-mail (often using proton mail, onion mail, or similar privacy-focused services) as opposed to independent infrastructure (i.e. dark web chat sites). This may be a result of increasing activity by "ephemeral" groups that lack supporting infrastructure, or could represent an operational security shift by established actors.

Quarterly Wrap Up

The increase in reported ransomware victims across Q1 2023 reflects the continued prevalence of ransomware as a worldwide, industry-agnostic threat.

Open-source reporting indicating a decrease in the amount of paying victims, while significant, does not appear to have detracted newcomers and ongoing operations in the Ransomware-as-a-Service (RaaS) ecosystem. Barring substantial disruption by international law enforcement or continuous declines in revenue, GRIT's assessment is that ransomware threat activity is unlikely to decline in the near term.

GRIT will continue to monitor for evolving tactics, techniques, and procedures demonstrated by adaptive ransomware threat actors, and we anticipate downstream mimicry by other organizations when demonstrably successful techniques emerge. Unfortunately, the likely result of these evolutions is increasingly socially abhorrent behavior, as ransomware groups target the most vulnerable or exploitable victims. Community and law enforcement information sharing will be vital in stymying the effectiveness of new techniques. GRIT remains dedicated to the mission of increasing threat intelligence sharing through partnerships, both public and private.