GUIDEPOINT SECURITY

GRIT
Ransomware Report

JULY – SEPTEMBER 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 of their victims and almost all groups offer an option to withhold announcement if the victim pays a ransom within a specified timeframe and/or remove the victims once a ransom has been paid. Additionally, some groups include incomplete information about their victim or claim an attack despite successfully attacking only a small subset of their target. For these reasons, the data in this report is useful in aggregate, but should be evaluated as a report consisting of data sources that have variability. Despite the variability, this report is still an accurate representation of the total ransomware threat landscape.

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

Contents

QUARTERLY

Ransomware Summary

Q3 of 2023 continued an ongoing surge in ransomware activity, once again reaching the highest ransomware volume that we have observed since GRIT began tracking and reporting on ransomware statistics. The 14.9% increase since Q2 can be partly attributed to an increased number of groups operating in the ransomware space, as there is a direct correlation to the number of public victims of ransomware and the number of groups observed operating at any given time. GRIT began tracking 10 new Emerging groups in Q3, the largest amount of new groups observed in a single quarter across GRIT's data set. Other notable Q3 events including Clop's MOVEit campaign, LockBit's return to a high operational tempo, and Bianlian's sustained capabilities despite moving to an exfiltration only model—all of which have contributed to this quarter's rise in ransomware activity.

The large-scale ransomware attacks against MGM Resorts and Caesars Entertainment highlight possible seasonal targeting of the Entertainment, Hospitality, and Tourism (EHT) industry. Based on our research, the EHT industry was the fifth most impacted industry, it's highest position since GRIT began tracking ransomware activity. GRIT assesses that the increases in impacted organizations from this industry are a result of deliberate targeting, owing to increased seasonal holiday travel and the victims representing attractive financial targets. Other notable industry trends include continued attacks on the healthcare industry, as groups like Alphv continue to claim healthcare victims at a significant rate. In Q3, one out of every five victim posts to Alphv's leak site were healthcare organizations, suggesting that not all Ransomware as a Service (RaaS) groups are concerned with the potential law enforcement attention that healthcare victims could bring.

Established groups continue to maintain the highest market share and victim volume in the ransomware ecosystem, and long-time leader LockBit continues to operate without significant challengers, even amongst other Established groups. We note that some Emerging and Developing groups continue to claim high rates of victims that would rival the performance of Established groups such as Alphv and Bianlian.

The United States still accounts for 48% of publicly posted ransomware victims but saw a 3.3% reduction in total US victims from Q2 to Q3. Meanwhile, GRIT observed other consistently impacted countries have an increase in activity including the United Kingdom, which saw a 40% increase in their total number of public victims. Additionally, there was an almost 3% rise in "non-top ten" countries impacted by ransomware in Q3, highlighting a potential new trend in group's impacting historically less targeted countries.

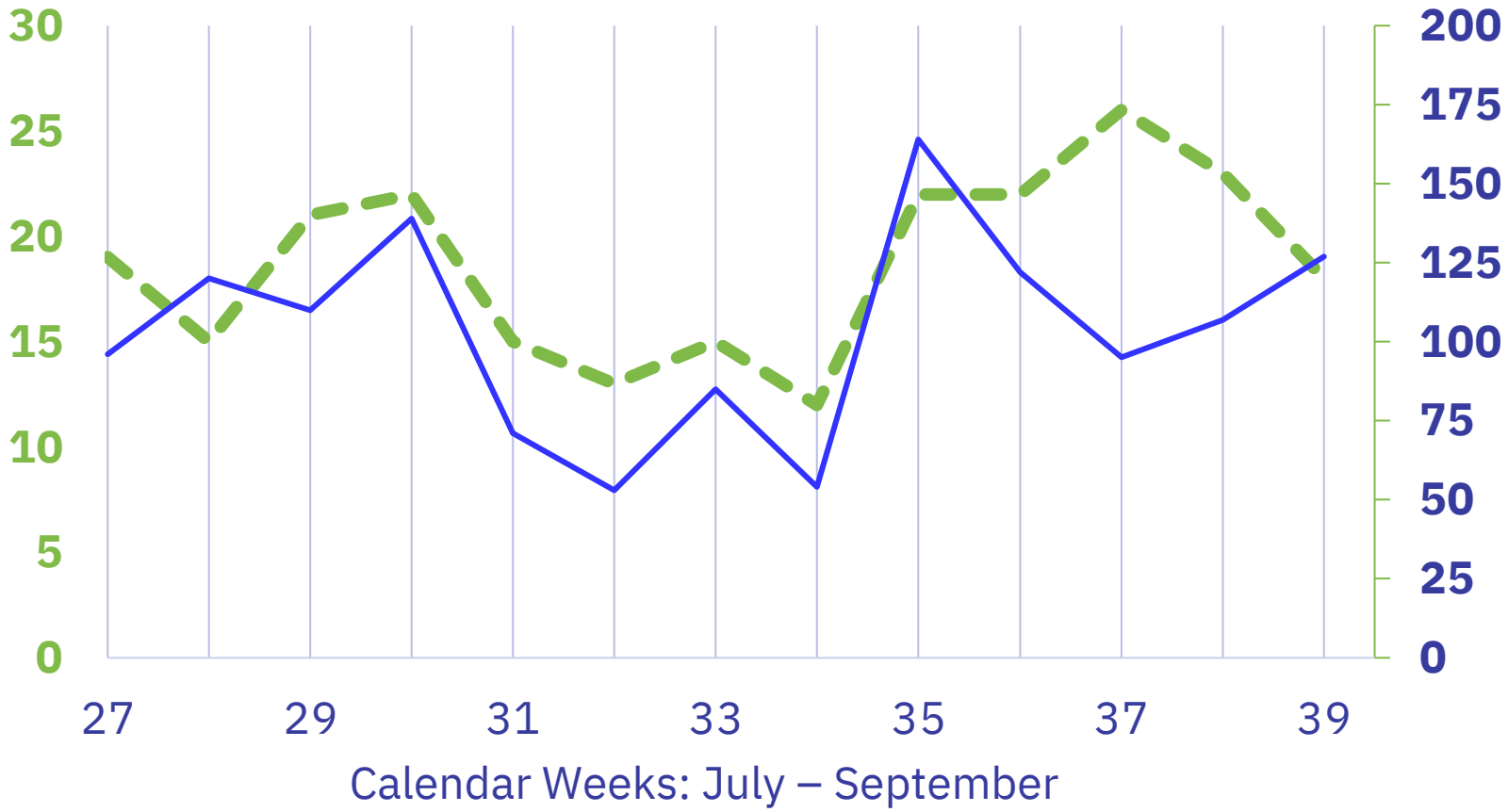
Total Publicly Posted Ransomware Victims	1353
Number of Tracked Ransomware Groups	46
Average Posting Rate (per day)	14.7

Rate of Publicly Posted Ransomware Victims (Q3 2023)

Q3 of 2023 marked the largest volume of public ransomware victims that GRIT has observed since we began tracking the ransomware ecosystem. Despite the high volume of activity this quarter, August saw a massive decrease in reported victims (368), with 25% fewer total posts than July (490) and September (495).

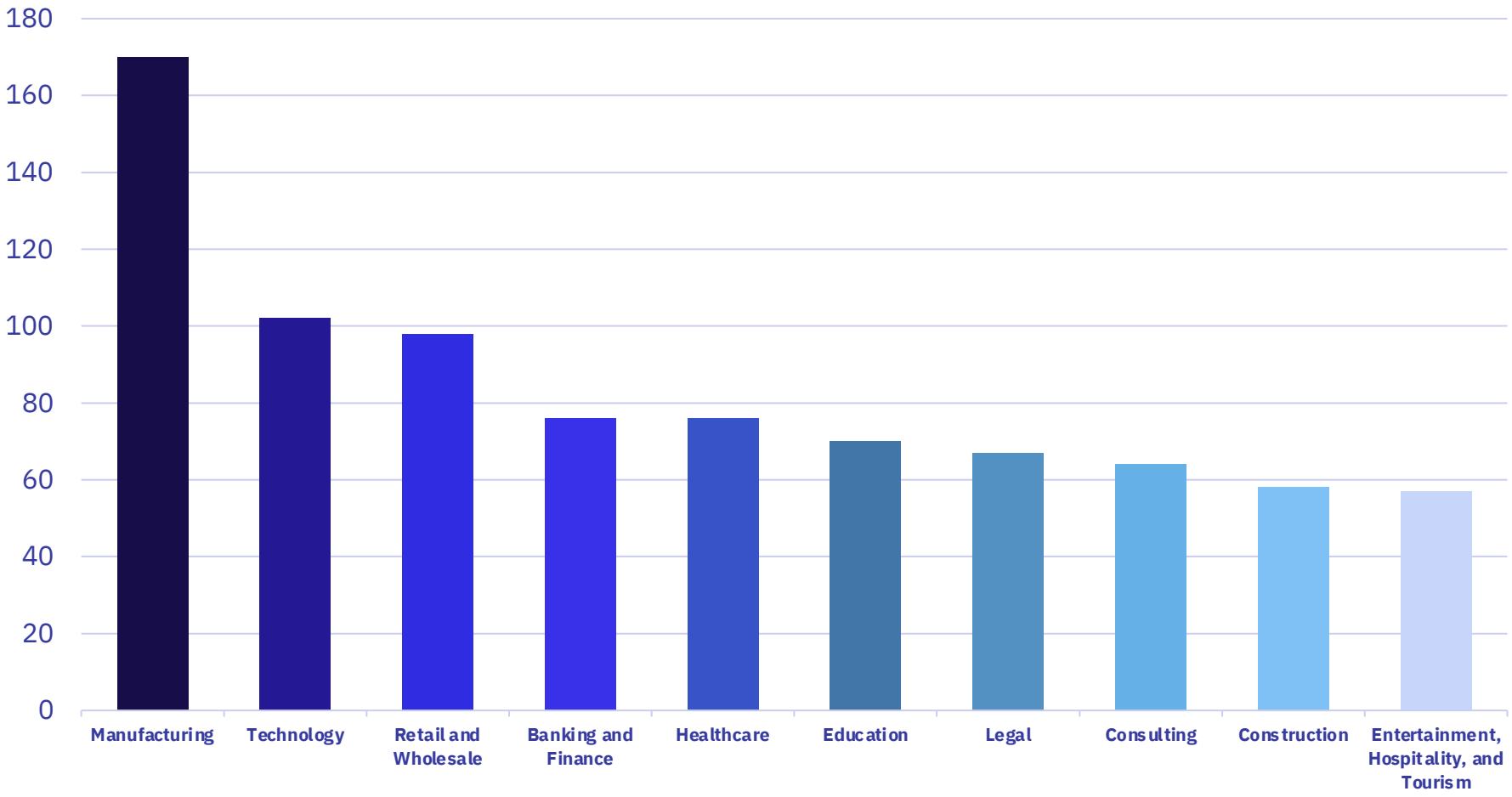
The same trend is visible among groups, with only 25 active groups in August, compared to 36 in both July and September.

Most notably, Clop fell from the top group in July and was not observed as part of the top 10 most active threat groups, which is tied to the end of their extortion efforts of their mass exploitation of MOVEit. Clop has not been observed posting to their leak site since July 31.



Total Posts	Total Groups	Average Posts per Week	Average Groups per Week
1353	**46**	**103**	**18.7**

Most Impacted Industries–Top 10–Q3 2023



- **Manufacturing**
  - Clop
  - LockBit
  - Alphv
- **Technology**
  - Clop
  - LockBit
  - Alphv
- **Retail & Wholesale**
  - LockBit
  - Ransomed
  - Clop
- **Banking & Finance**
  - Clop
  - Alphv
  - LockBit
- **Healthcare**
  - Alphv
  - 8Base
  - Bianlian

Retail & Wholesale has been experiencing a steady climb in observed victims throughout 2023. In Q1, Retail & Wholesale was the 9th most impacted industry with 38 victims, by Q2 they had climbed to the 6th most impacted industry with 71 victims, and in Q3 they are the 3rd most impacted industry with 98 victims.

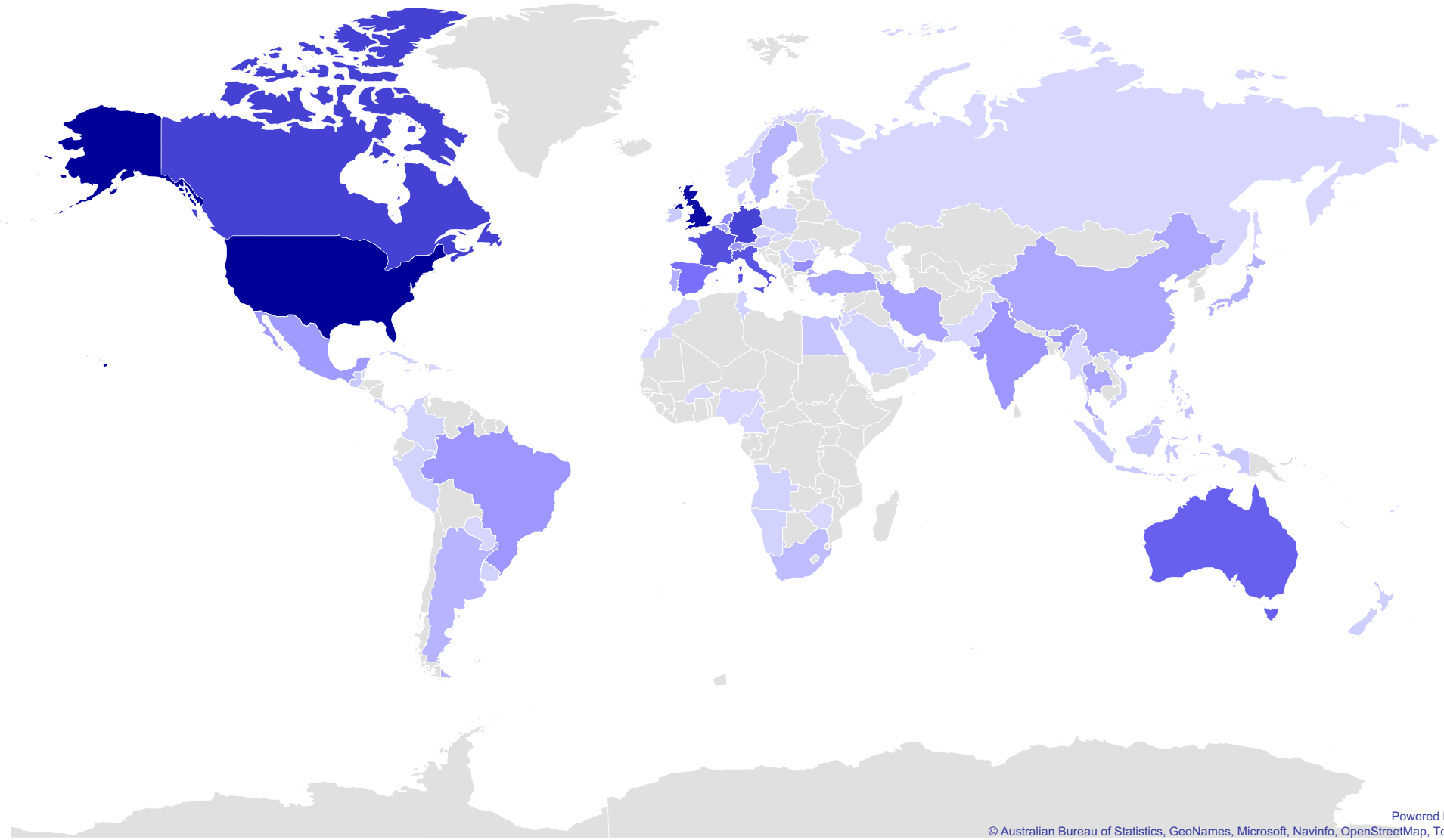
In contrast, the Insurance industry dropped well below their previous position from 9th to 21st most impacted industry, decreasing from 39 victims to 24 respectively. This may indicate that Q2 was an anomalous quarter for the industry, as Q3 appears to represent a return to form that closely mirrors Q1 numbers, when Insurance placed 21st with 15 victims.

Aside from the Entertainment, Hospitality, and Tourism (EHT) industry replacing Insurance in the top 10, the remaining "top 9" are unchanged from preceding quarters.

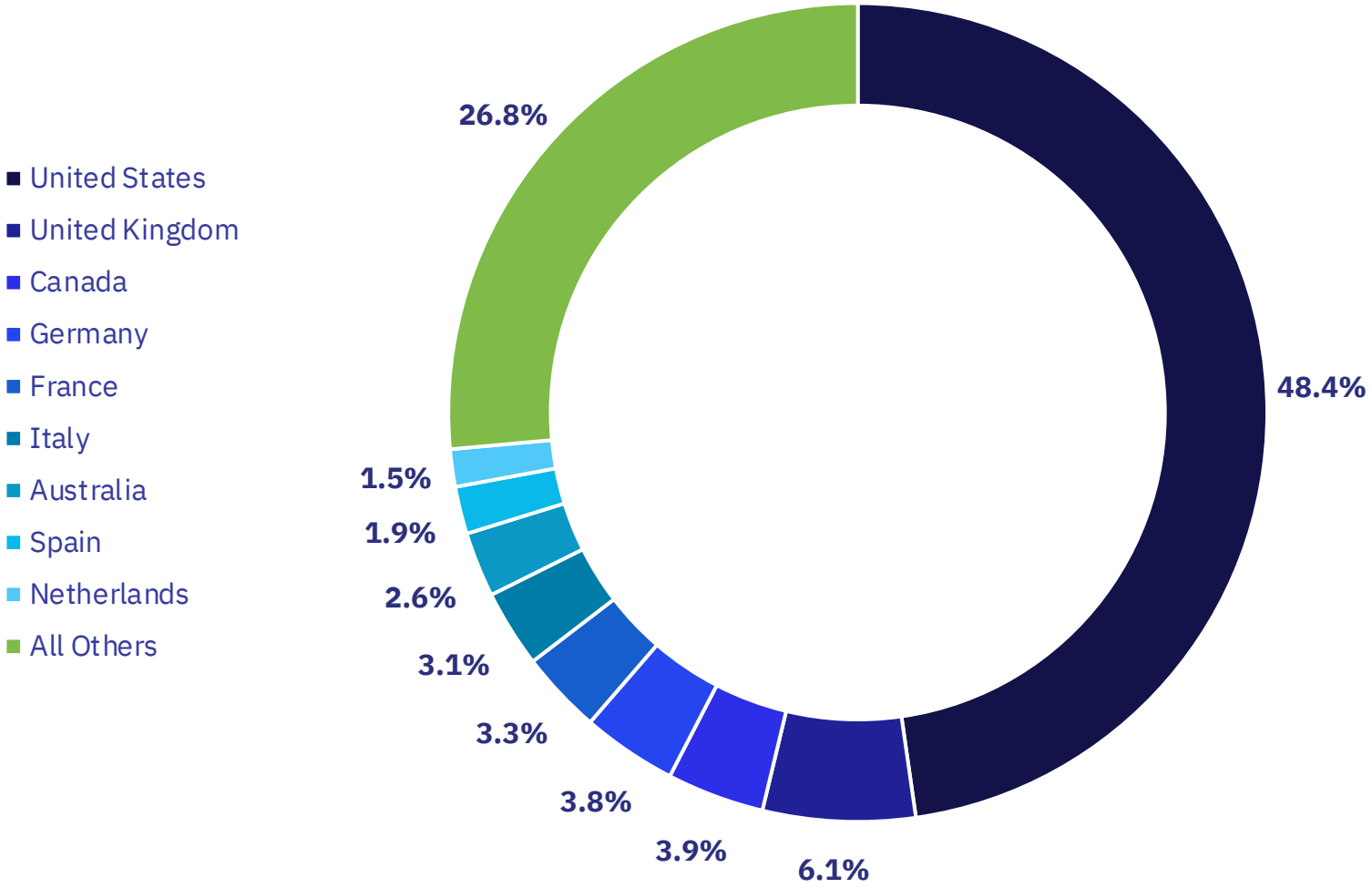
Geographic Breakdown of Ransomware Victims (Q3 2023)

Top 10:

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



Country Breakdown (All Threat Actors)



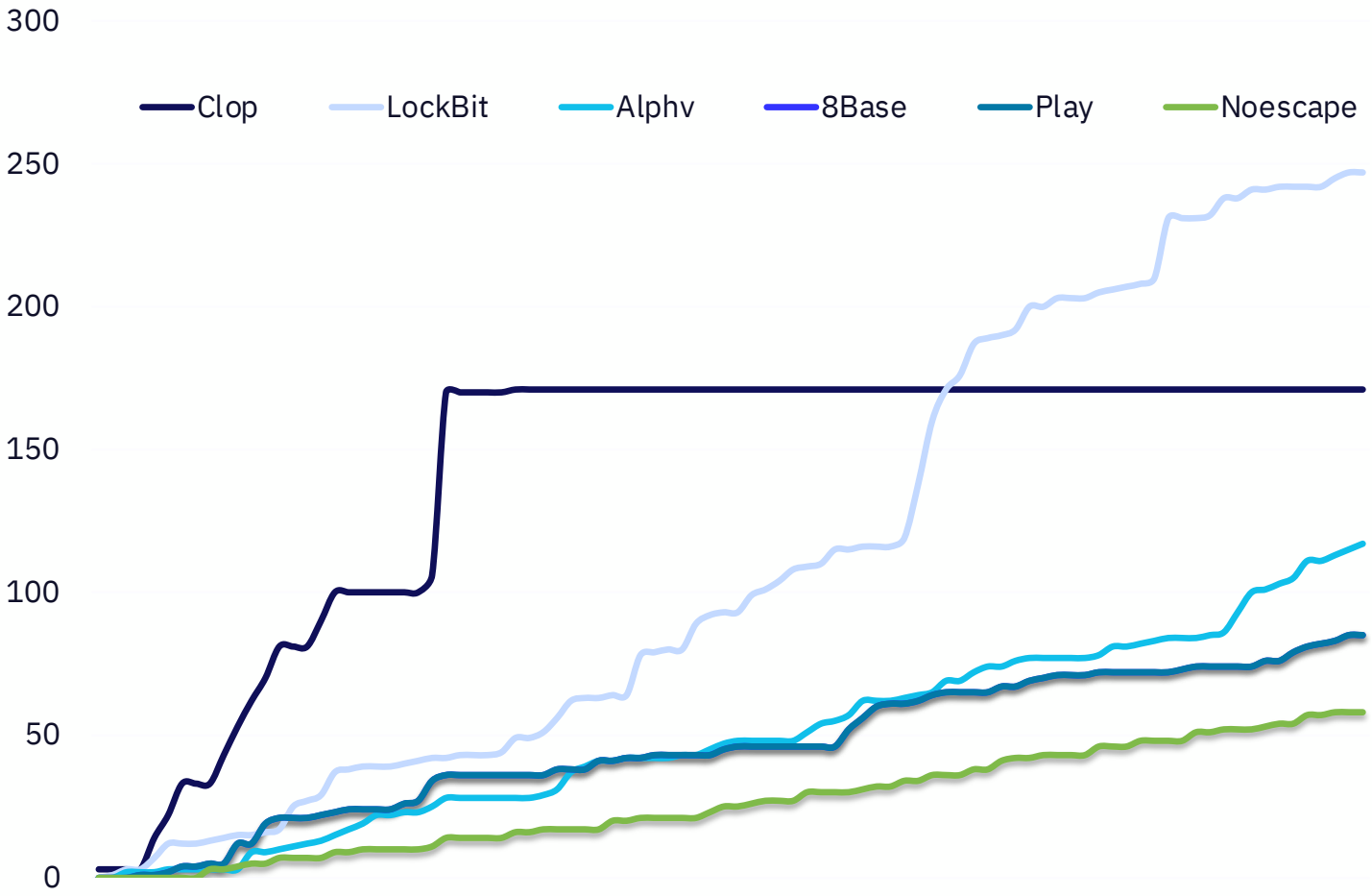
While US-based organizations saw an increase in total observed victim count in Q3 2023, the percentage of attacks directed against US-based organizations actually decreased by 3.3%, reflecting a marked increase in attacks impacting other nations.

In particular, United Kingdom-based organizations saw an increase from 59 victims in Q2 to 83 in Q3, an approximate 40.7% quarter-over-quarter increase.

Even though it isn't represented here, the victim count among non-"top 10" countries increased from 24.1% of the Q2 total to 26.8% in Q3, an increase of 79 victims. This represents a demonstrable broadening of ransomware's victim base outside of the most frequently impacted western countries.

Cumulative Victims by Threat Group

Ransomware Activity – Q3 2023



LockBit

LockBit remains the most prolific ransomware threat group, posting roughly the same number of victims in Q2 as Q3 despite a modest decline from 21% to 18% quarter over quarter in terms of total market share, continuing a trend first observed in its 32% reduction from Q1 to Q2.

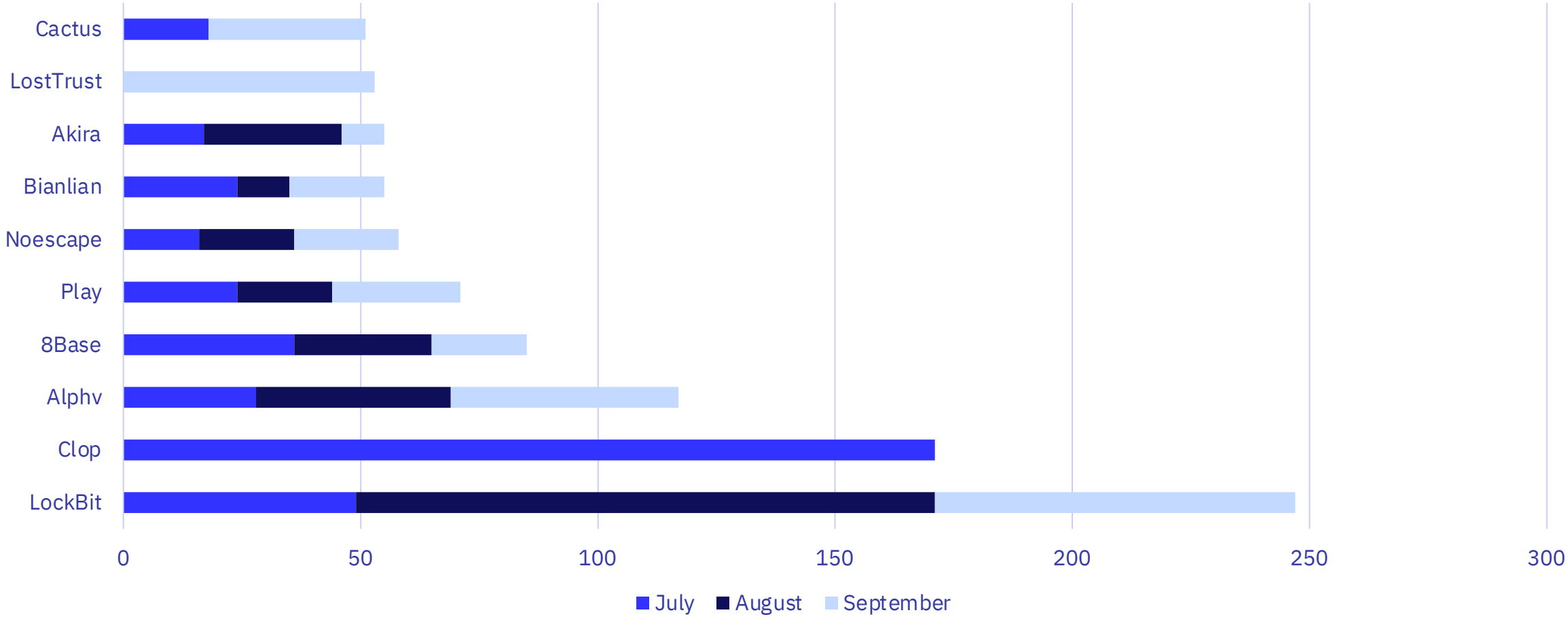
Clop

Clop (Stylized as cl0p) maintained a top spot in Q3 stemming almost entirely from its mass exploitation of a vulnerability in the MOVEit managed file transfer software. Clop's Q3 activity more than doubled its posted victims which resulted in a 5% total increase in victims from Q2 to Q3.

Alphv

Alphv (Stylized as AlphV) experienced a modest decrease in total victim volume and market share between Q2 and Q3 while retaining its position as one of the most impactful ransomware groups. Alphv continues to garner public attention through statements on high profile cases, as most recently demonstrated in its claiming of responsibility for the MGM resorts breach.

Top 10 Ransomware Threat Actors



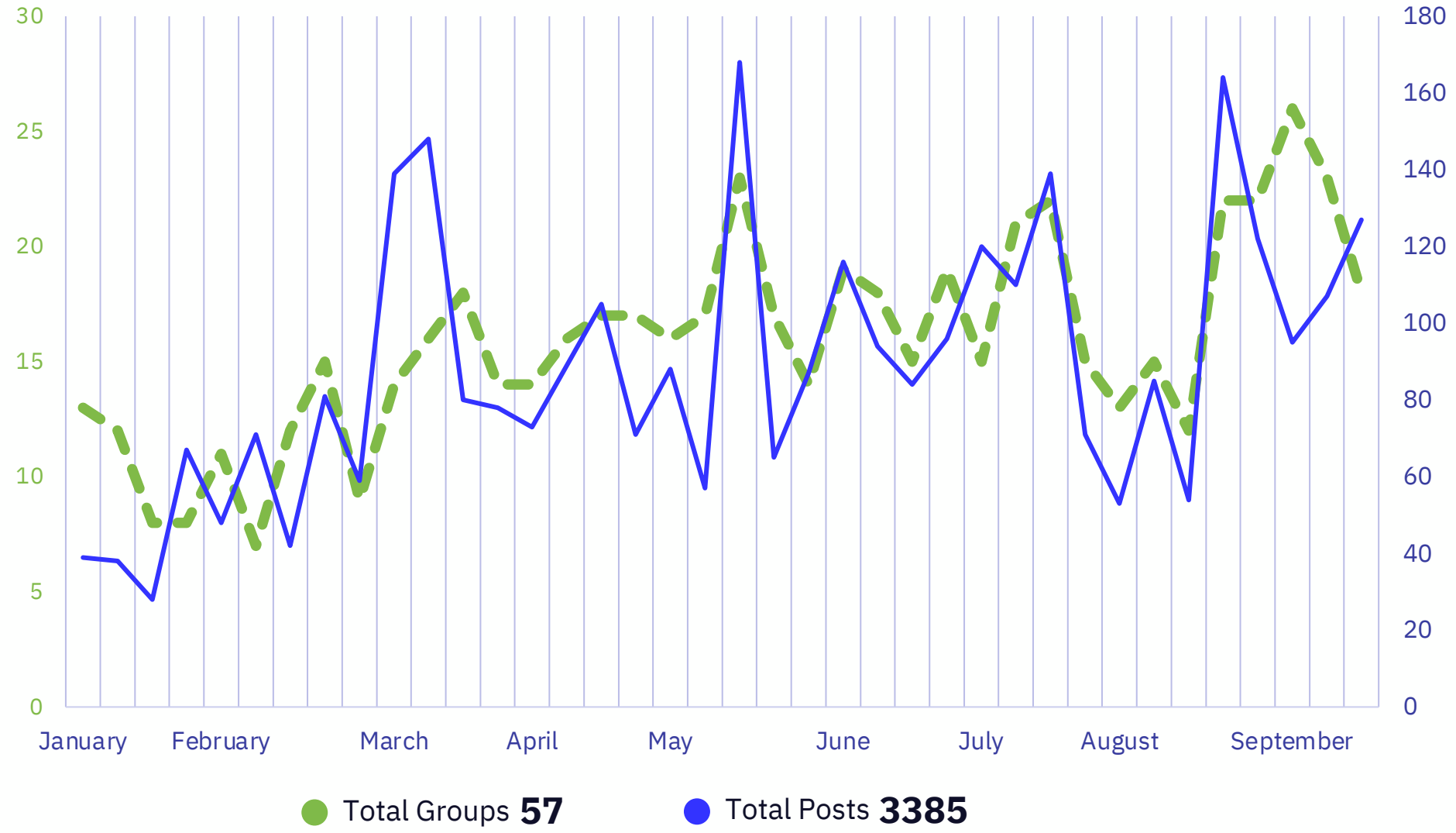
Year to Date Ransomware Trends

Through Q3 2023, there have been 3,385 total victims posted by 57 unique groups. By comparison, 44 unique groups claimed 1,846 victims during the same time period in 2022, representing an 83% increase. The ransomware ecosystem as a whole is on pace to nearly double its number of publicly posted victims year over year despite a much less significant increase in the number of actors, suggesting increased victim volume attributed to the most Established and operationally mature groups.

The increase in reported victims can be partially attributed to the large scale of Clop's mass exploitation campaigns, but the data also echoes sentiments from around the industry that fewer companies are willing to pay a ransom, potentially contributing to increased victim posts on ransomware group blogs.

Another recurring trend is the positive correlation between the number of active groups and the number of victims posted at any given time. While seemingly obvious, this indicates that newer Emerging groups are able to find their own victims without reducing the victim volume of Established groups.

Rate of Publicly Posted Ransomware Victims (Year to Date)

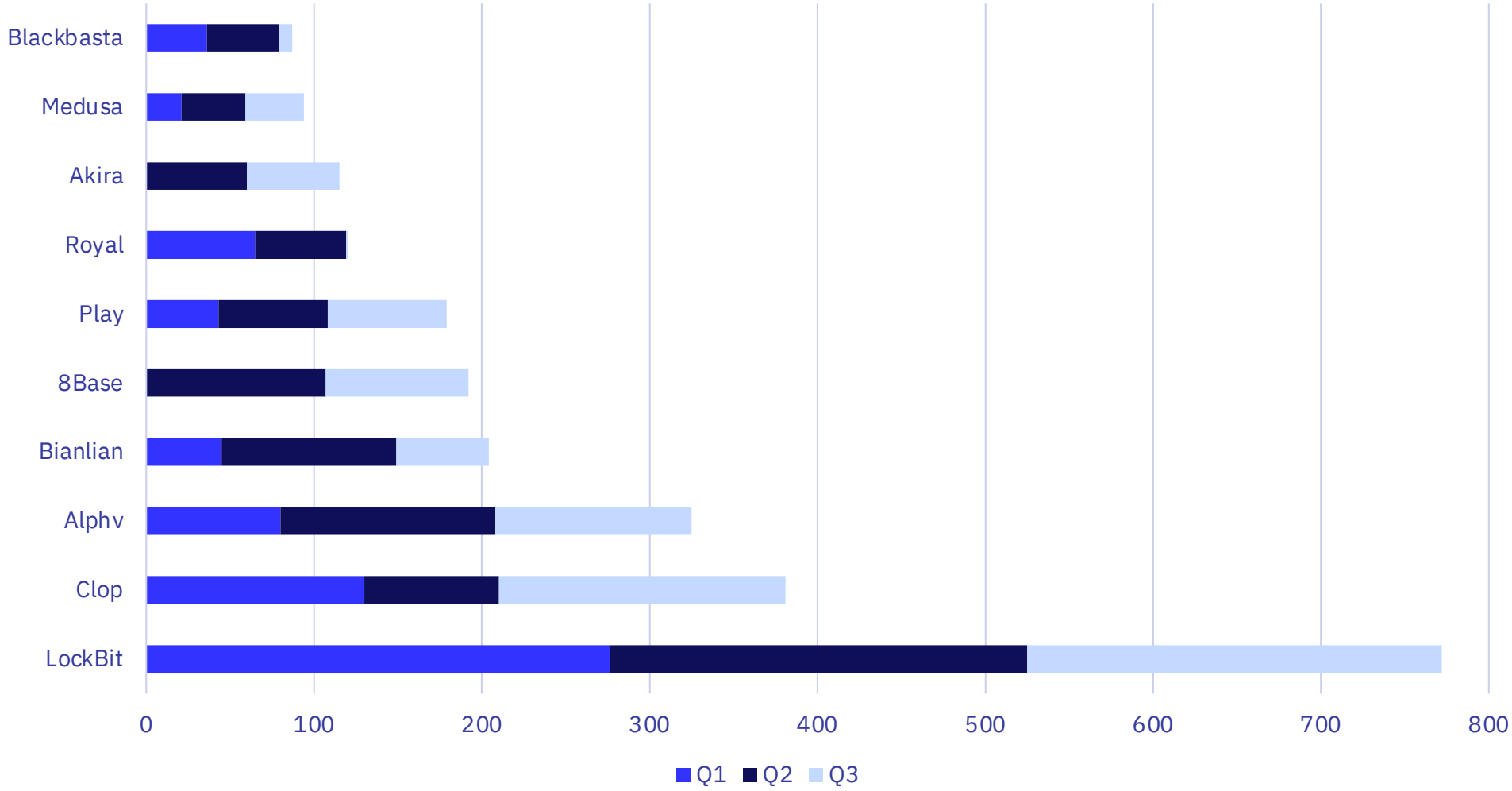


LockBit maintains their hold on the number one spot, posting 770 victims this year to date. Comparatively, LockBit was responsible for 670 victims in the first three quarters of 2022, showing that the largest Ransomware-as-a-Service operation continues to increase its victim volume.

Through its successful mass exploitation attacks, Clop has surged to the number two spot. At this point in 2022, the group had only 38 posted victims, highlighting the significance of Clop's shift to mass exploitation tactics.

Despite not operating publicly until Q2, new groups Akira and 8Base rose to long-term spots on the top 10 list with operations that have rapidly scaled. Royal remains on the top 10 list despite having not posted since July 19th, a testament to its impact in the first half of the year. All indications suggest that the once Established group is no longer operational, possibly as the result of splintering or intentional rebranding.

Top 10 Ransomware Threat Actors (Year to Date)



Threat Actor Spotlight

Ransomed

Ransomed

Ransomed, also reported as Ransomed[.]vc or RansomedVC, is an Emerging data extortion group and aspiring Ransomware-as-a-Service group first observed in August 2023. The group first gained attention for its Twitter account and Clearnet web page advertising for prospective affiliates, both of which have been taken offline at the time of this report.

Ransomed has posted several high-profile "victims" with publicly posted extortion demands ranging from $8,000 to $1.015MM. Details appended to each victim range from descriptions of site defacement, to database exfiltration, to "access to everything on [the victim] servers." In some instances, the alleged data compromised lacks detail or may be public information, suggesting that Ransomed and its affiliates are likely pursuing opportunistic or "smash and grab" data theft and extortion rather than double-extortion ransomware operations.

Ransomed claims to have cooperated with the ransomware groups Stormous and Everest in posts to its dark web blog, though it has not provided details. GRIT is not aware of a distinct Ransomed ransomware at the time of this report, and limited intelligence reporting indicates that the group is still in the process of developing an encryptor. Ransomed's cooperation with these ransomware groups likely represents an additional means of data extortion by these "partner" groups rather than a joint ransomware operation.

Ransomed's posted victims included a disproportionately high 15 Bulgarian domains in September, in each case claiming successful data exfiltration. This disproportionate impact could signify active targeting of Bulgaria or affiliates with specific knowledge of Bulgarian language.

We also note Ransomed's posting a Russian organization, an extremely anomalous move in the ransomware and extortion ecosystem, in which cybercrime groups typically avoid targeting victims in the Commonwealth of Independent States (CIS). Ransomware groups, in particular, generally eschew Russian victims in order to avoid attracting the attention of the Russian Federation's police or intelligence services.

Major Casinos Attacked by Alphv Affiliate

In September 2023, security reporting from multiple sources began covering an outage affecting systems at properties owned by MGM Resorts International in Las Vegas, before eventually confirming an ongoing cyberattack. In the days following, industry peer Caesars Entertainment reported a past breach under similar circumstances. Both attacks were later attributed to the Established group Alphv, including through a public statement pertaining to the MGM breach on their data leak site. Both the MGM and Caesars breaches were reportedly conducted by the same affiliate of Alphv, a sophisticated cybercrime group previously dubbed Scattered Spider by security researchers. Scattered Spider is known for gaining access to victim networks by leveraging sophisticated social engineering tactics and for targeting identity and authentication applications, especially single sign on platforms.

Casinos, even with mature security programs, have proven to be an attractive target for opportunistic financially motivated cybercrime. Similar to Manufacturing and Transportation companies, most casinos operate 24/7 and stand to lose significant revenue for any operational downtime caused by a ransomware attack, both from gaming operations losses and losses of associated businesses such as hotels and restaurants. Casinos also typically have large amounts of cash on hand, probably encouraging threat actors to demand even larger payments. From a data desirability perspective, Casinos are required to gather and hold personally identifiable information on their players for tax and compliance purposes.

These attacks serve as a reminder that tactics, techniques, and procedures are often more valuable methods of attributing ransomware affiliates rather than the primary groups themselves. Ransomware as a Service operations such as those of Alphv and LockBit consist of a rotating cast of operators who perform the "hands on keyboard" portion of a group's attacks, and who may support multiple groups at any time. Two attacks attributed to the same primary group may have been performed completely differently by entirely distinct affiliates.

FBI Warns of Duplicate Ransomware Attacks

On September 27th, 2023, the Federal Bureau of Investigation (FBI) released a Private Industry Notification warning of instances in which two or more ransomware groups impacted the same victim in close proximity. The FBI observed deployment of combinations from the following ransomware groups, presumably from Ransomware-as-a-Service affiliates of multiple operations: AvosLocker, Diamond, Hive, Karakurt, LockBit, Quantum, and Royal.

The same Private Industry Notification warns of custom data theft and wiper tools observed in 2022, in which data wipers remained dormant until a set time, at which point they corrupted data in alternating intervals.

Some security researchers have pushed back on the novelty of the former claims, with Emsisoft citing instances of duplicate ransomware deployment dating back to at least 2021, probably in an attempt to complicate recovery or ensure successful encryption.

GRIT has observed multiple instances of victims impacted by multiple ransomware variants or extortion groups in 2023:

- A manufacturing company was impacted by both LockBit and Bianlian within eight days in August 2023
- An organization was impacted by both LockBit and Royal within the span of a week in March 2023.
- A government organization was posted by Quantum in May and August 2022 before being posted by the extortion group Snatch in September 2023, indicating a possible attempt to re-extort the organization with data initially exfiltrated earlier.
- We note at least four instances in which Cactus, LockBit, NoEscape, and Royal impacted organizations between March and September 2023, before later being posted by LostTrust in September 2023. LostTrust is assessed to be a rebrand of Metaencryptor, an Emerging ransomware group first observed in August 2023. This degree of overlap is anomalous and could represent purposeful targeting of previous ransomware victims by the group.

Despite Shift to Exfiltration-only Operations, Bianlian Operations Continue Apace

Bianlian, a non-RaaS ransomware group observed operating since at least July 2022, has continued claiming victims at a consistent pace following its transition to exfiltration-only operations in early 2023.

A publicly available decryptor for Bianlian was published by cybersecurity software company, Avast, in January 2023, likely leading the group to abandon double-extortion operations in favor of data theft and extortion.

Bianlian's posted victims increased 200% in July and 567% in September year-over-year, and remained consistent in August, indicating that the change in tactics has not substantially disrupted the group's operational capabilities. We note that the increased number of posted victims could represent either an increase in total victims impacted by the group, or an increased percentage of victims opting not to pay the demanded ransom, both of which are equally plausible.

In a similar instance, the Ransomware-as-a-Service group Akira had a publicly available decryptor posted by Avast in late June 2023 and has been observed conducting at least some exfiltration-only attacks since. In the three months following publication of the decryptor, Akira's posted victims have remained relatively stable, decreasing only 8% from the preceding three months.

Despite Akira's continued operations, recent security reporting has covered the development of a new "Megazord" encryptor attributed to the group, suggesting a probable attempt to resume double-extortion operations in the near-term. We assess that the key differentiator between the actions of Bianlian and Akira in this instance is Akira's operating model as a RaaS group, which depends on the core group adding value to continue attracting affiliates and receiving portions of ransom payments.

Alphv Conducts String of Attacks Against Healthcare

In September, Alphv claimed over ten victims from the healthcare industry, accounting for one out of every five of its leak site posts. Prior to September, healthcare victims typically comprised 10% or less of Alphv's victims. GRIT is continuing to monitor the group to determine if this streak carries over into October, and the remainder of 2023, to determine if this a purposeful long-term shift towards the healthcare industry.

As discussed in previous ransomware reports, ransomware attacks against healthcare organizations often attract unwanted law enforcement and negative public attention, a risk that we assess drives affiliate rules explicitly ruling out this target set for some groups.

Healthcare victims remain amongst the most susceptible to data extortion and double-extortion ransomware, stemming from the operational impacts and service disruption of encryption, and the sensitivity of patient health data.

Alphv's September victims included one large healthcare organization which was prefaced with a "warning" post seemingly designed to further coerce the victim and attract publicity to the attack. This publicity-seeking behavior combined with highly-publicized communications in the wake of the MGM attack suggest that the group is probably less concerned with attracting law enforcement pressure relative to its peers, including LockBit. Alphv's behavior could represent an internal sense of security, an attempt to burnish its brand as particularly aggressive, or a gradual testing of norms in pursuit of additional victims and revenue.

Industry Spotlight

Entertainment, Hospitality, Tourism

Industry Spotlight

Entertainment, Hospitality, Tourism

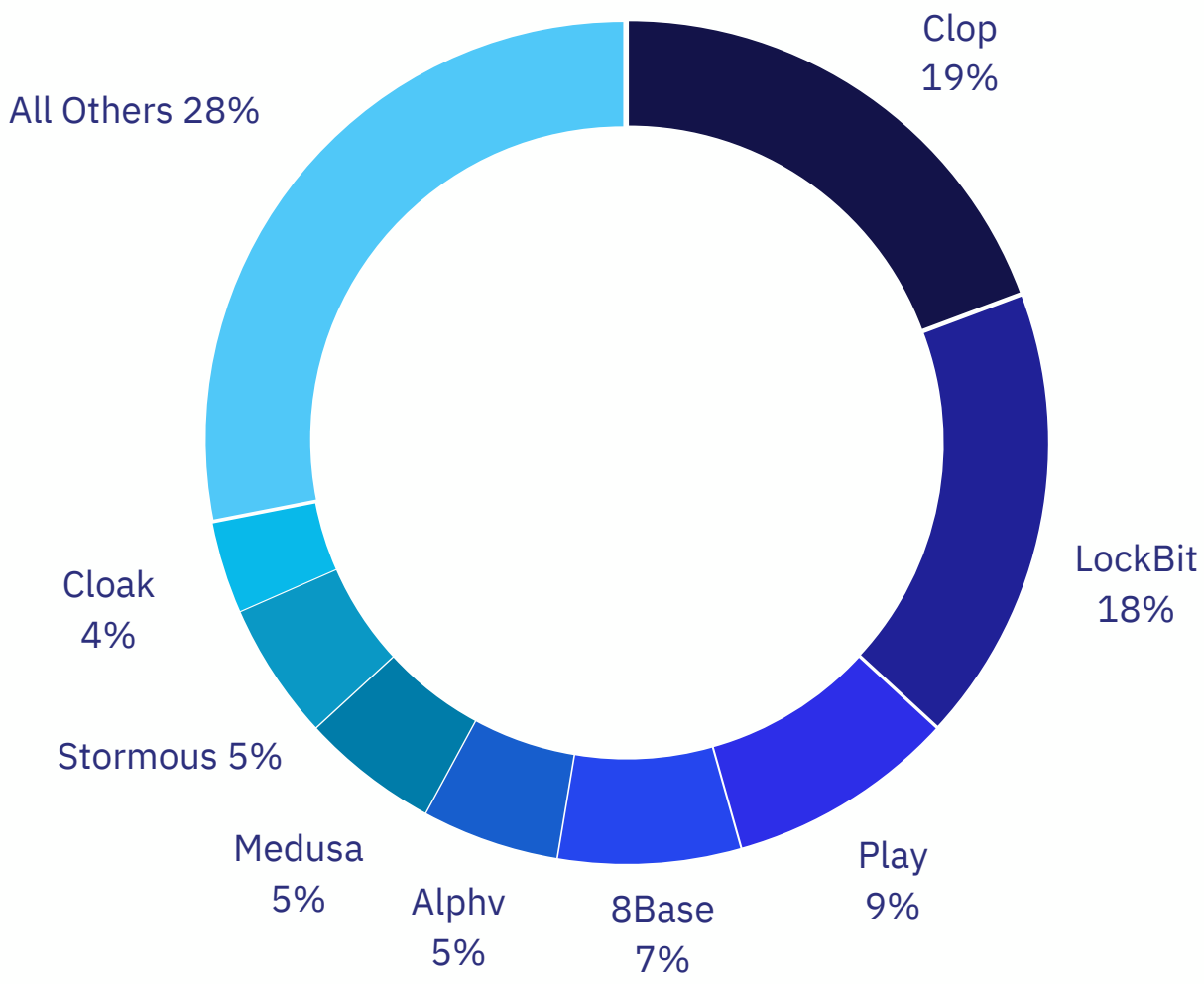
The major ransomware attacks reported publicly as impacting Caesars and MGM Resorts in Q3 mirror a greater trend observed by GRIT around the Entertainment, Hospitality, and Tourism (EHT) industry. GRIT's review of historical data reveals that ransomware attacks against the EHT industry appear to increase during Q3. In Q3 2023, GRIT observed an increase of 24 victims in the industry relative to the preceding quarter. When analyzed through the perspective of trimesters vs. Quarters, the trend becomes more stark – February through May 2023 saw just 35 victims in the EHT industry while June through September saw 75, a 114% increase in victim volume. GRIT observed a similar trend in these time periods in 2022, with threat actor's posts increasing 68% in the summer months of 2022.

The seasonality of this trend may be a result of deliberate targeting. The United States is far and away the most disproportionately targeted by ransomware attacks, and the June through September timeframe often includes a summer vacation for many Americans.

Times of increased vacationing correspond with increased travel and spending at hotels, on entertainment, and at tourist destinations. Threat actors may perceive this as the opportune time to target the industry to maximize victim revenue and therefore, ransom demands. Operational downtime caused by a ransomware attack can devastate revenues for businesses in the EHT industry, potentially granting threat actors increased leverage during double extortion attacks.

The EHT industry does not often rank highly in victimization when compared to other more commonly targeted verticals but was the 5th most targeted industry in June 2023. GRIT assesses that while some threat actors may jump at any opportunity to compromise an EHT company, more sophisticated actors may target the timing of their extortion operations more deliberately in in the hopes of improving their chance at payment.

Ransomware Threat Groups Targeting Entertainment, Hospitality, and Tourism Industry



The 57 victims in the Entertainment, Hospitality, and Tourism (EHT) industry this quarter were claimed by 23 different threat groups, including many of the Emerging groups first observed this quarter. 90% of the Emerging groups first observed in Q3 had at least one victim in the EHT industry.

23 threat groups, or 50% of the active threat groups observed this quarter, had at least one victim in the Entertainment, Hospitality, and Tourism industry.

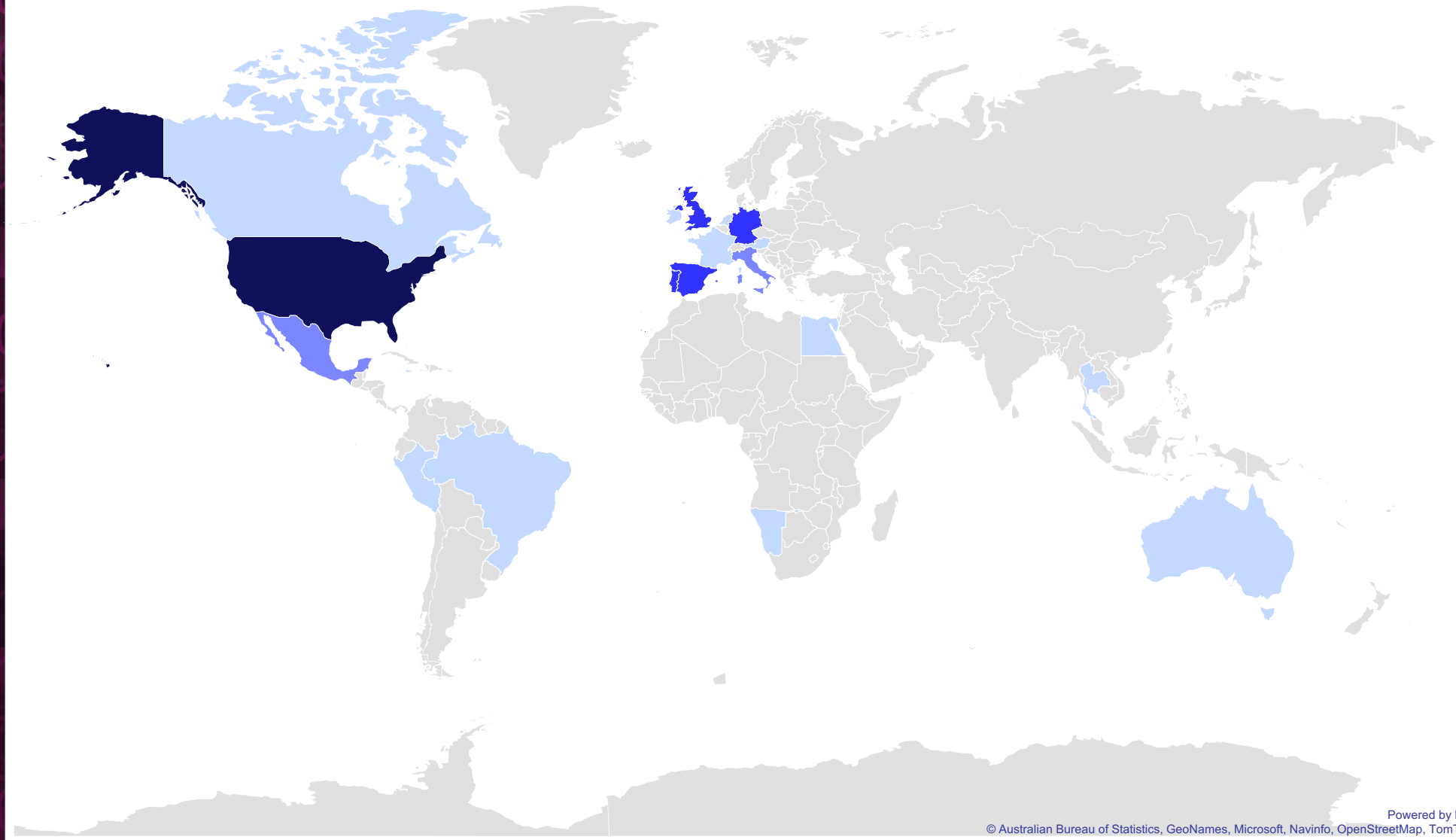
Unsurprisingly, Clop accounts for the largest share of these victims with 11, followed closely by LockBit with 10.

Geographic Breakdown of Ransomware Victims

(Entertainment, Hospitality, and Tourism Industry – Q3 2023)

Countries Targeted

1. United States
2. United Kingdom
3. Germany
4. Portugal
5. Spain



Quarterly Wrap Up

Q3 2023's figures highlight the continuing breadth and depth of ransomware's impact, as threat groups continue to victimize across all industry verticals and extend their reach worldwide. As more Emerging ransomware groups join the ransomware ecosystem to seize on new opportunities, we continue to see surges in publicly posted victims - contributing to consistent growth from quarter to quarter.

Mass exploitation events still remain as a significant contributing source to overall ransomware activity, although leading Established groups such as LockBit and Alphv continue to be the primary drivers of ransomware activity. In the case of LockBit, a short-lived lull in operational activity was immediately recognizable over the summer but did not prevent the group from retaining its place as the most impactful ransomware group in Q3. Alphv claimed responsibility for a number of High-profile attacks which overshadowed their victimization of multiple healthcare organizations, seemingly flouting behavior that would typically be downplayed to avoid attracting law enforcement attention. The lack of mid-to-long-term slowdowns and increasingly brazen behavior by leaders in the ransomware space indicate that attempts to stem the tide of modern ransomware have not yet been successful.

Looking forward to Q4, GRIT assesses that there will be continued upward trends in data-only exfiltration by groups that have been impacted by the release of public decryptors, or groups without the resources to develop and maintain their own encryption capabilities. Standalone ransomware groups, including Bianlian, may choose to continue this trend as part of their long-term operations, while Ransomware-as-a-Service groups such as Akira may pursue data-only exfiltration as a stop gap while developing new encryptors or pursuing Rebrands.

As current Emerging and Developing groups continue to hone their skills and refine their processes, GRIT assesses that the number of publicly posted ransomware victims is likely to increase through Q4, resulting in significant annual growth in ransomware victims from 2022 to 2023 and setting up 2023 to be Ransomware's most impactful year to date.

Ransomware groups continue to find methods of adapting to a changing ecosystem, whether through Emerging and Developing groups adapting unique niches in the ransomware community, as observed with Ransomed; or through Established groups, including Alphv, consistently impacting sensitive industries and newsworthy victims. GRIT stands firm in our belief that community and law enforcement intelligence sharing remain key to identifying and limiting the effectiveness of ransomware groups. As 2023 begins to come to a close, GRIT is continuing to monitor the ransomware landscape and sharing relevant trends, TTPs, and IOCs to identify and slow ransomware activity.