GUIDEPOINT SECURITY

GRIT
Ransomware Report

2022 ANNUAL REPORT

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 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

ANNUAL

Ransomware Summary

2022 was yet another year with ransomware topping the charts as the most prolific and impactful threat to our networks, data, and operational capabilities. With 2,507 publicly posted victims across 40 industry verticals, ransomware groups were responsible for publicly posting 6.87 victims per day to their respective leak sites. GRIT tracked 54 groups utilizing a double-extortion methodology, many of which are utilizing a Ransomware as a Service (RaaS) model to increase productivity and maximize revenue.

The first quarter of 2022 started high with a posting rate that mirrored the value of Bitcoin, and as the price of Bitcoin became more volatile, so did the rates of victim postings, to a degree. Despite the volatility of cryptocurrency, ransomware victim postings remained frequent, as no quarter saw less than 569 total victims. Significant events, including the rebranding of Conti and the change in version from Lockbit2 to Lockbit3, also influenced the rates of ransomware victims and led to some volatility; however, yearly trends show that 2022 ended on a high note for ransomware groups.

Unsurprisingly, as 2022 progressed, the United States and other western countries were the main targets of ransomware groups. Western countries made up 77% of all publicly posted victims in 2022, with the United States accounting for 38.9% of total victims claimed by ransomware groups.

Similarly, the manufacturing and technology industries were consistently the most targeted industries, with construction and healthcare following close behind. Much of the top 10 most targeted industries remained consistent during 2022, although there was some movement within the top targeted industries from month to month.

As GRIT's methodology introduced the concept of ransomware group categories, we began to take a deeper and more granular look into how ransomware groups operate, how they target, and some of the characteristics that make them unique. To kick this annual report off, we will cover the ransomware group taxonomy we created over the course of the year, then we'll dive deep into 2022 to examine ransomware statistics and trends. If you just want a breakdown of the Q4 numbers, we'll separate those out after the annual review. Finally, we'll finish with a look at 2023 with some predictions of what we can expect, as ransomware will likely continue to be front and center as the most impactful cybersecurity threat we must defend against on a daily basis.

Total Publicly Posted Ransomware Victims	2,507
Number of Tracked Ransomware Groups	54
Average Posting Rate (per day)	6.87

Ransomware Taxonomy

As 2022 progressed, we realized that ransomware groups could be divided into subtypes based on their behaviors and operational maturity. By subdividing ransomware groups, we are able to obtain more detailed insights into how ransomware groups progress in their level of operational maturity and gained the ability to classify and identify potential rebranding activity.

Throughout this annual ransomware report, and during subsequent monthly and quarterly reports, we will distinguish ransomware groups by placing them into these four categories:

- Full-Time
- Rebrand
- Splinter
- Ephemeral

During our continuous monitoring, we now reclassify groups as they progress in their operational maturity. 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.

We are sharing our ransomware group taxonomy definitions as part of this annual report with the hope that they will be used and further developed by others in the community. By using this taxonomy, we believe the community will be able to more easily identify ransomware rebranding and group behaviors, which will lead to significant degradation in their capabilities to conduct operations.

Ransomware Taxonomy

FULL-TIME:

These groups have been active for nine or more months and often have months where they publicly claim 10 or more victims. Their standardized infrastructure and defined affiliate structure (if acting as a Ransomware as a Service) lead to consistent TTPs and behaviors with only slight variations based on ransomware operator.

Example: Lockbit

REBRAND:

These groups have typically been active for less than nine months, but their public posting rates regularly rival full-time groups. TTPs for this type of group are more varied than a full-time group, yet still project an organized and determined operational capability. If the rebrand wasn't announced publicly, these groups' TTPs will help identify their previous identity.

Example: Royal

SPLINTER:

These groups are established and have been active for 2-5 months with varied public posting rates. Their TTPs are varied, sometimes borrowed, and indicative of less experienced operators that are developing their brand and identity. If their split from another group wasn't public information, their TTP overlap with known groups can give them away.

Example: Onyx

EPHEMERAL:

These groups have been active for less than two months, with varied, but low, victim rates. Many times, these groups are a "flash in the pan" and do not progress to more developed and mature group types.

Example: Sparta

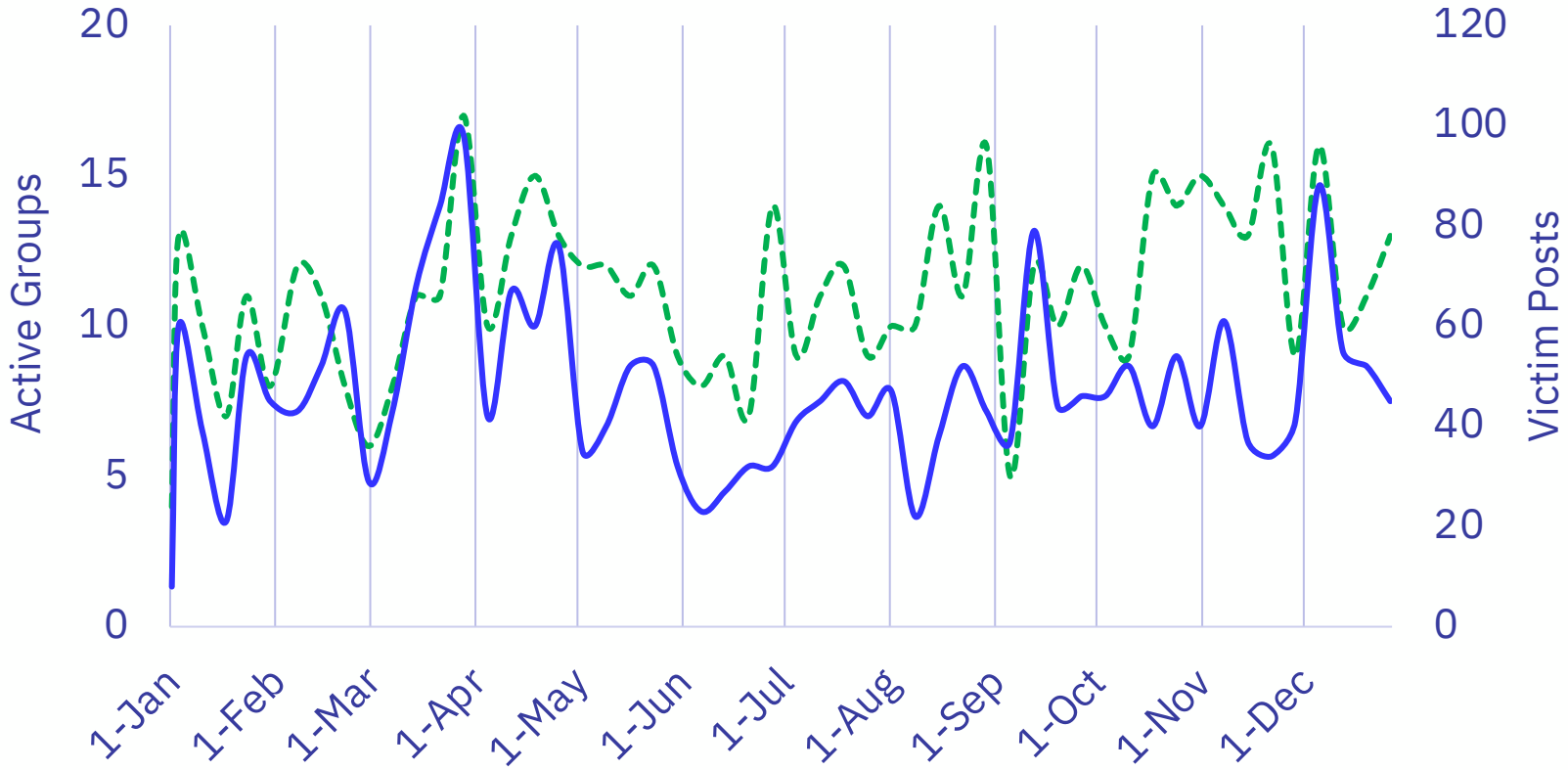
Annual Ransomware Trends

Rate of Publicly Posted Ransomware Victims (2022)

Throughout 2022, victim posting rates remained fairly consistent, with the biggest lull occurring in late June and early July. This lull can most likely be attributed to the shift from Lockbit 2 to Lockbit 3, although challenges in the crypto currency market may have also had an impact. (More on that in a minute)

On average, there were 11.2 groups operating during any week in 2022. Notably, every month in 2022 saw at least one new group emerge with double extortion capabilities.

March was the most active month of 2022 with 279 claimed victims, with April coming in at 278. Together March and April accounted for 22% of the total victims of 2022.



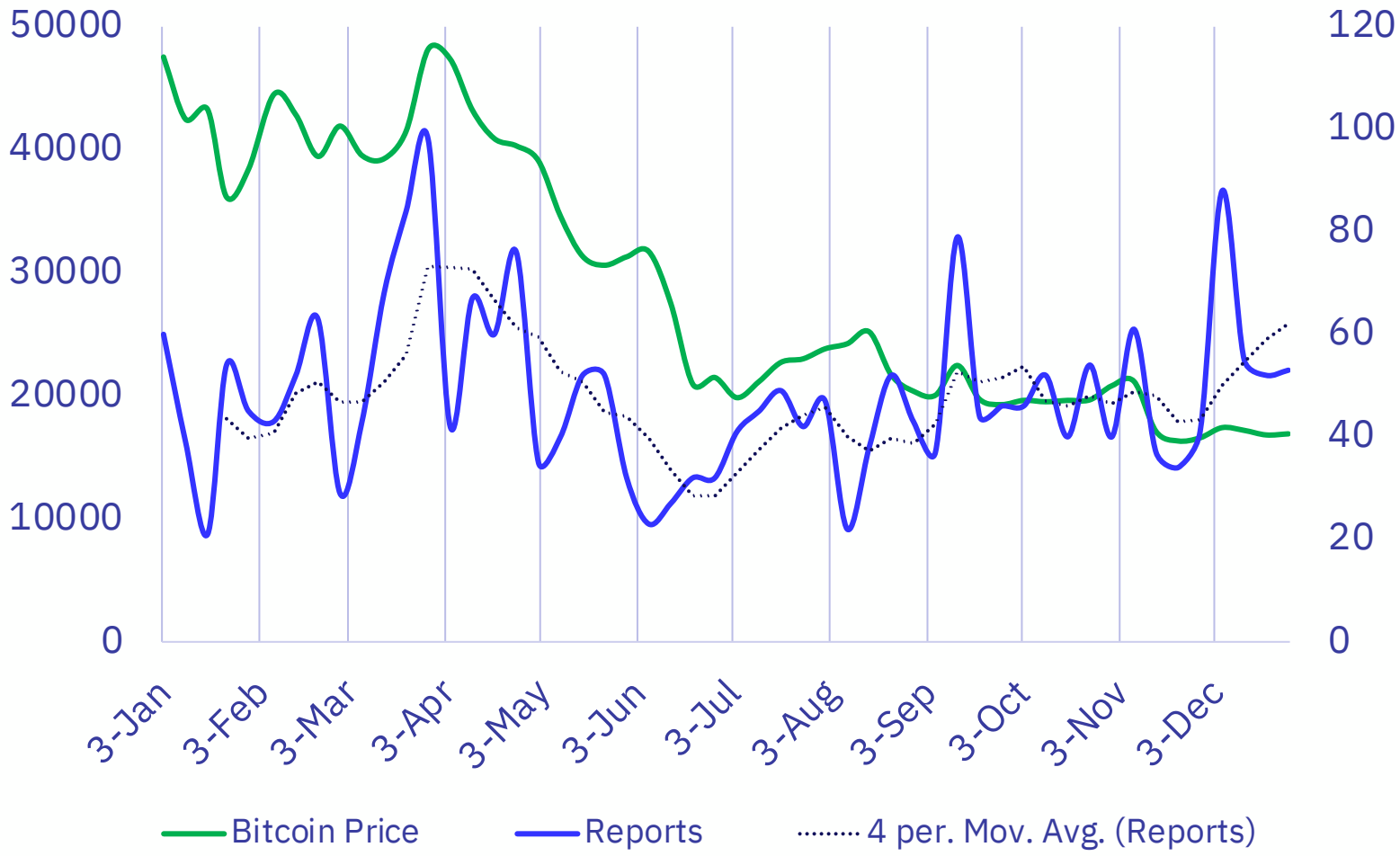
Total Groups	Total Posts	Average Posts per Week	Average Groups per Week
54	**2507**	**48.1**	**11.2**

One of the strongest correlations that we found when analyzing the data for all of 2022 was the link between victim posting rates and the price of Bitcoin.

Due to the way that groups tend to group their victim postings, the rate of posting doesn't seem to correlate to Bitcoin at first. But when we used a 4 period moving average to normalize the posting rates, the link became clear.

This suggests that threat groups closely monitor Bitcoin prices and increase operations while Bitcoin prices are high to maximize profits. Likewise, it suggests that threat groups may slow down operations while Bitcoin prices are more volatile to reduce potential losses.

Rate of Publicly Posted Ransomware Victims vs Price of Bitcoin (2022)

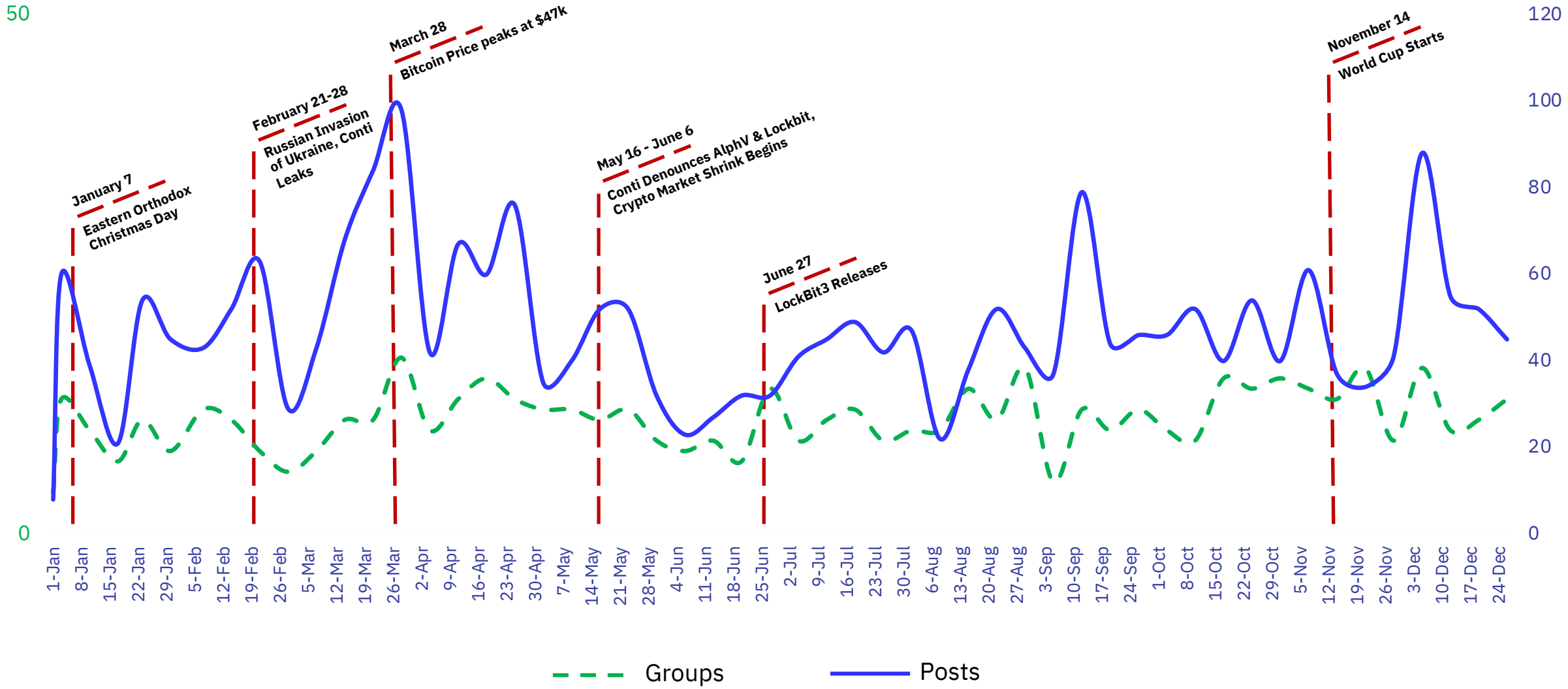


2022 Correlating Geo-Political and World Events

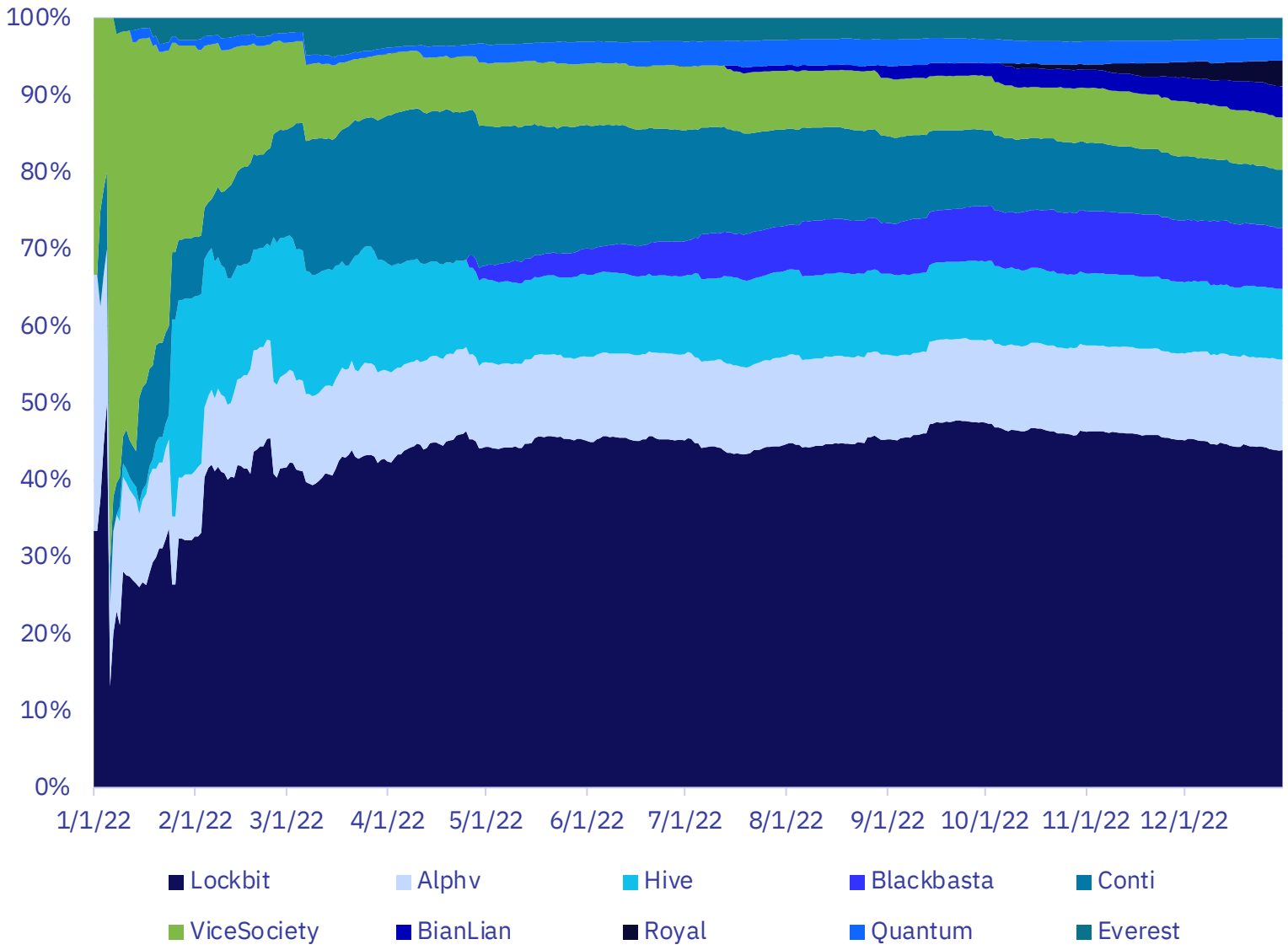
The following graph shows the daily rate of victim posting and active groups, overlaid with significant world events that may have influenced ransomware activity. Save for September 12, almost all the peaks and valleys for the year correlate to major world events.

- **January 7, Eastern Orthodox Christmas Day: January 7, Eastern Orthodox Christmas Day**: We observed a two-week slowdown following Orthodox Christmas Day, a commonly observed holiday in Russia.
- **Feb 21-28, Russia Invasion of Ukraine and Conti Leaks**: There was a sharp–yet short-lived–decline in ransomware activity following the Russian invasion of Ukraine and the Conti leaks.
- **March 28, Bitcoin price peaks at $47k**: In the weeks leading up to March 28, we observed a rapid increase in ransomware activity that peaked as Bitcoin prices skyrocketed to $47k per bitcoin.
- **May 16 - June 6, Conti denounces AlphV and Lockbit, Crypto Market Shrinkage Begins**: Ransomware rates begin to fall as competition and animosity occurs between ransomware groups and cryptocurrency markets begin to plummet.
- **June 27, Lockbit3 Release**: Ransomware rates steadily increase following the official release of Lockbit3.
- **November 14, World Cup Starts**: Ransomware activity initially declines during the World Cup, but spikes as the World Cup progresses.

2022 Correlating Geo-Political and World Events



Cumulative Victims by Threat Group



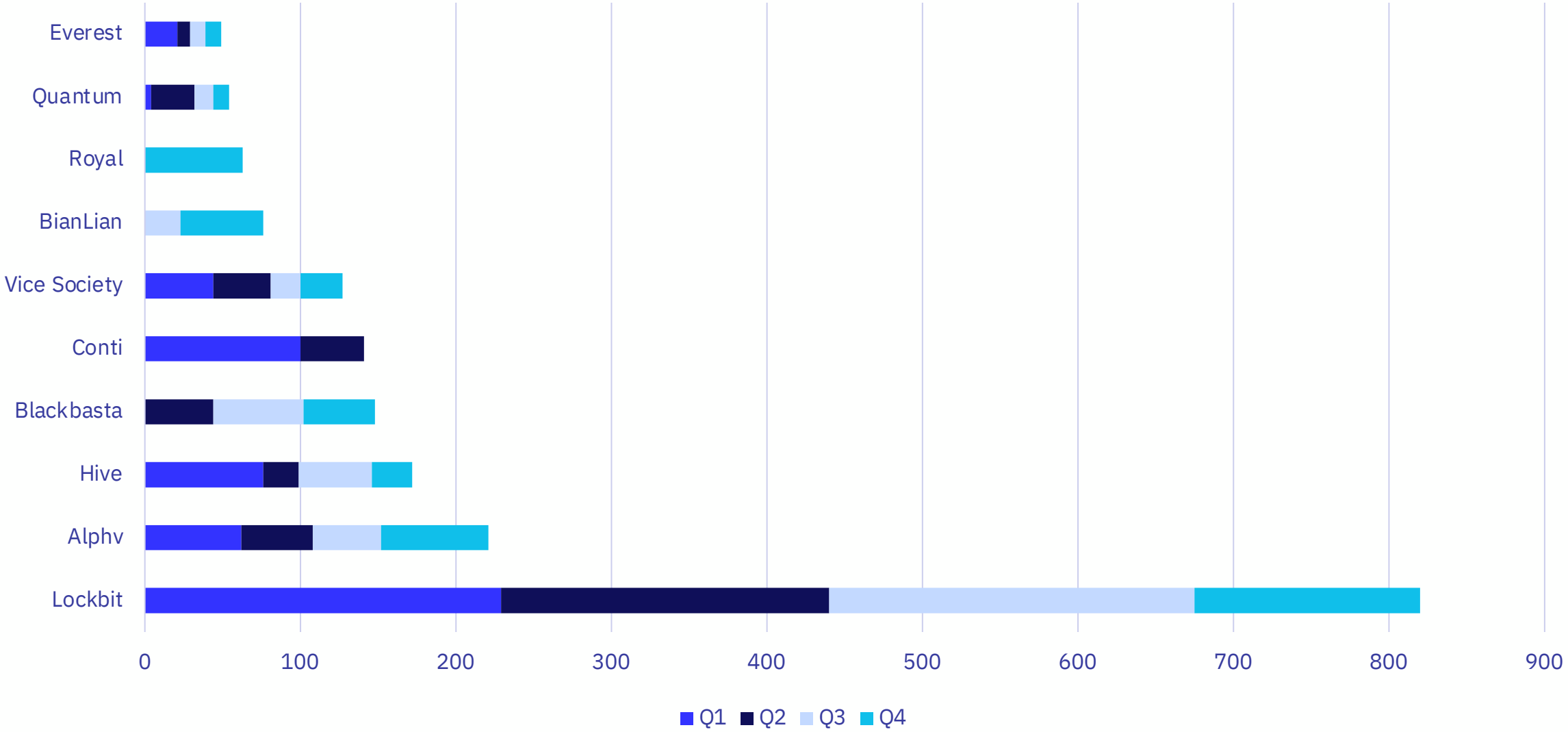
During 2022, Lockbit was responsible for the vast majority of ransomware victims, and at the end of the year accounted for 33% of all publicly posted ransomware victims.

Despite entering the double extortion game beginning in late April, Blackbasta still ended 2022 as the 4th most impactful ransomware group.

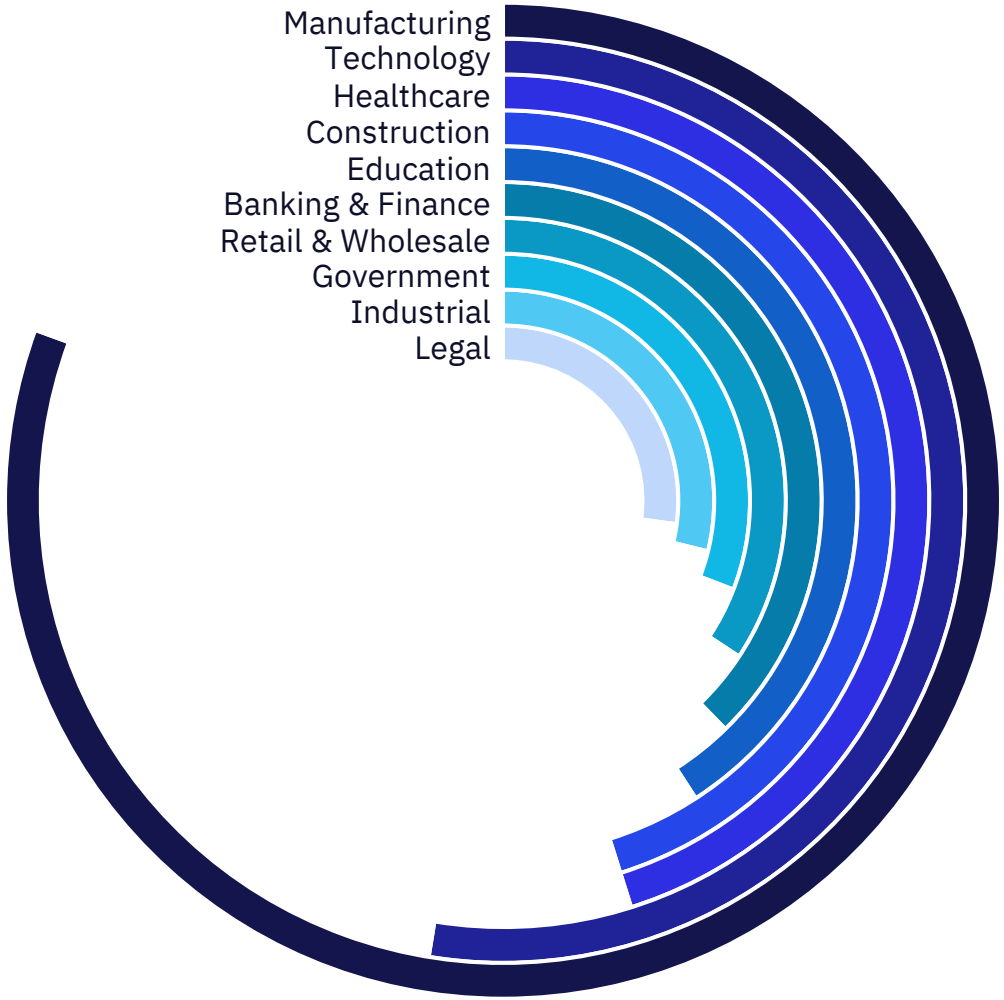
Vice Society began 2022 with a huge spike in publicly posted victims, posting 25 victims on January 6th. However, a sharp decrease and “low and slow” approach throughout the remainder of the year led them to 6th place overall among ransomware groups.

Despite both getting a late start in 2022, BianLian and Royal ended up as the 7th and 8th most impactful ransomware groups of 2022, respectively.

Top 10 Ransomware Threat Actors



Most Impacted Industries Top 10 – 2022



- **Manufacturing**
  - Lockbit
  - Blackbasta
  - Conti
- **Technology**
  - Lockbit
  - AlphV
  - Hive
- **Healthcare**
  - Lockbit
  - Hive
  - Vice Society
- **Construction**
  - Lockbit
  - Alphv
  - Blackbasta

In 2022, Full-Time groups accounted for the most activity in the most highly impacted industries.

Unsurprisingly, Lockbit was the most impactful Full-Time ransomware group in the top four impacted industries of 2022. Surprisingly, there more healthcare victims targeted by Lockbit were targeted after the release of Lockbit3 (51%), despite Lockbit explicitly calling out healthcare as a sensitive industry that should not be touched unless they are "for profit."

Reviewing Lockbit's late 2022 healthcare victims, some victims are for-profit organizations, but others are focused on patient health.

Despite receiving less focus by researchers, Hive was the third most active group in 2022, which is highlighted by their top 3 representation in the Technology and Healthcare industries.

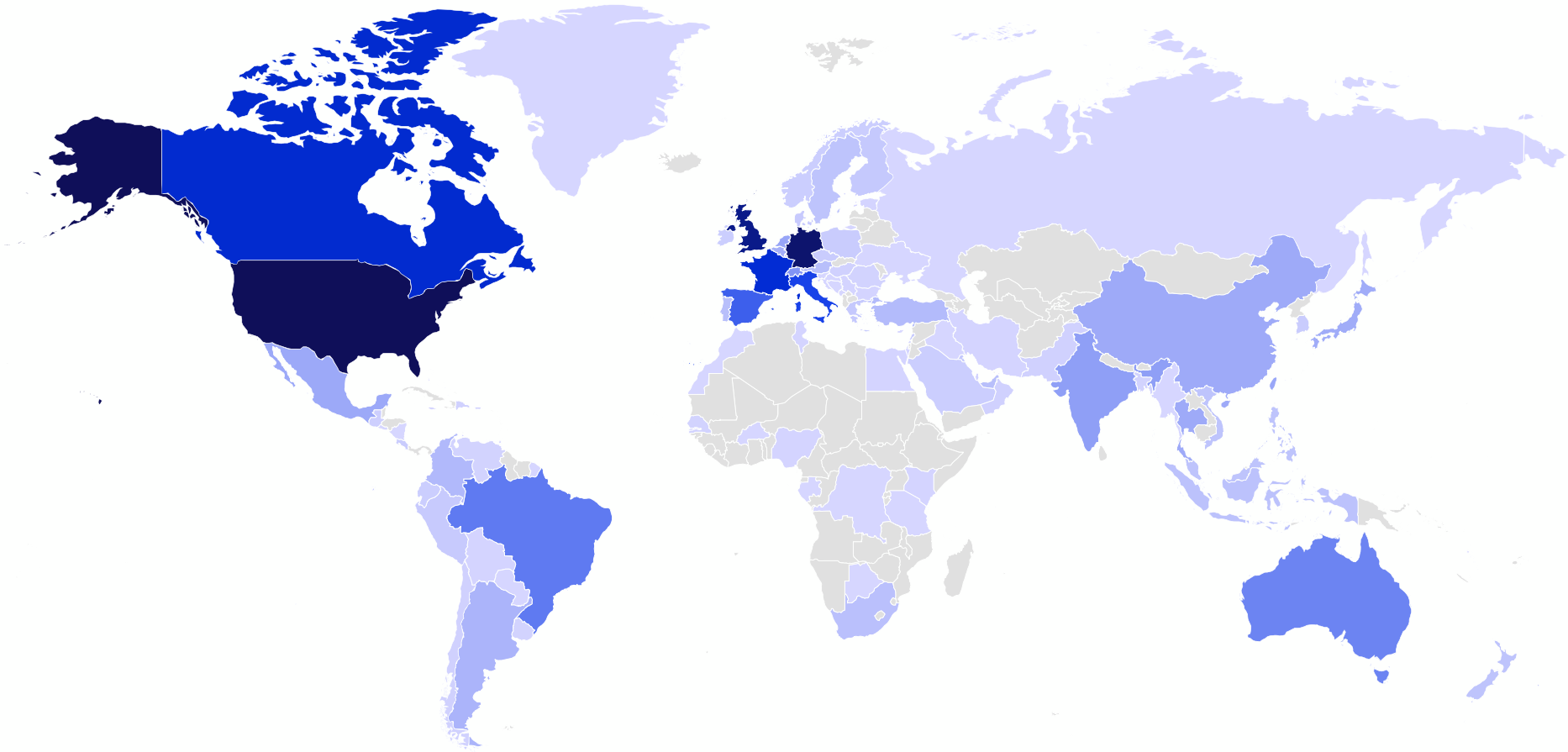
Blackbasta is the only non-Full-Time group represented in the top-impact groups. However, there is strong correlation between BlackBasta's TTPs and the now-defunct Conti, so their presence as a Rebrand is less surprising in this ranking.

Alongside Vice Society's strong presence in Healthcare targeting, they also accounted for more than 1/3rd of all Education victims (48 out of 143) for the year. Their track record across the year has consistently shown their willingness to target sensitive industries.

Geographic Breakdown of Ransomware Victims (2022)

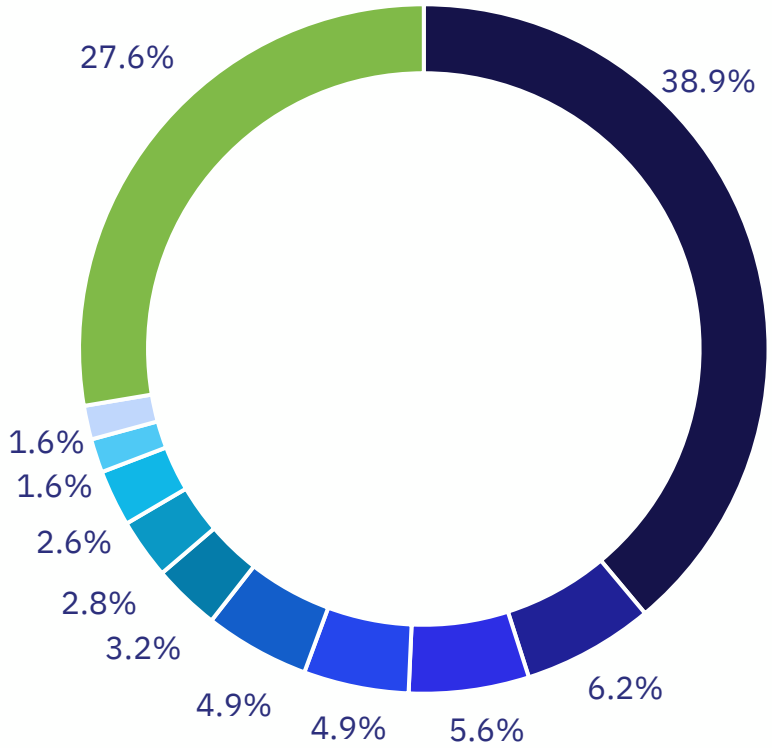
Top 10:

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



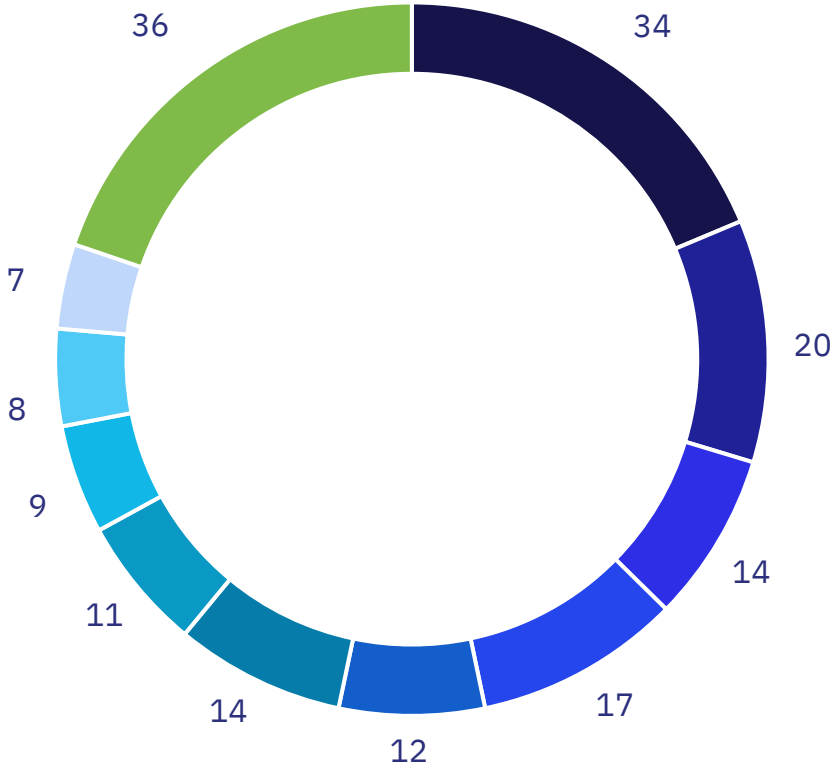
Country Breakdown (All Threat Actors)

Percent of Total Victims



- United States
- France
- United Kingdom
- Spain
- Germany
- Canada
- Australia
- Italy
- Netherlands
- Japan
- All Others

Industries Targeted



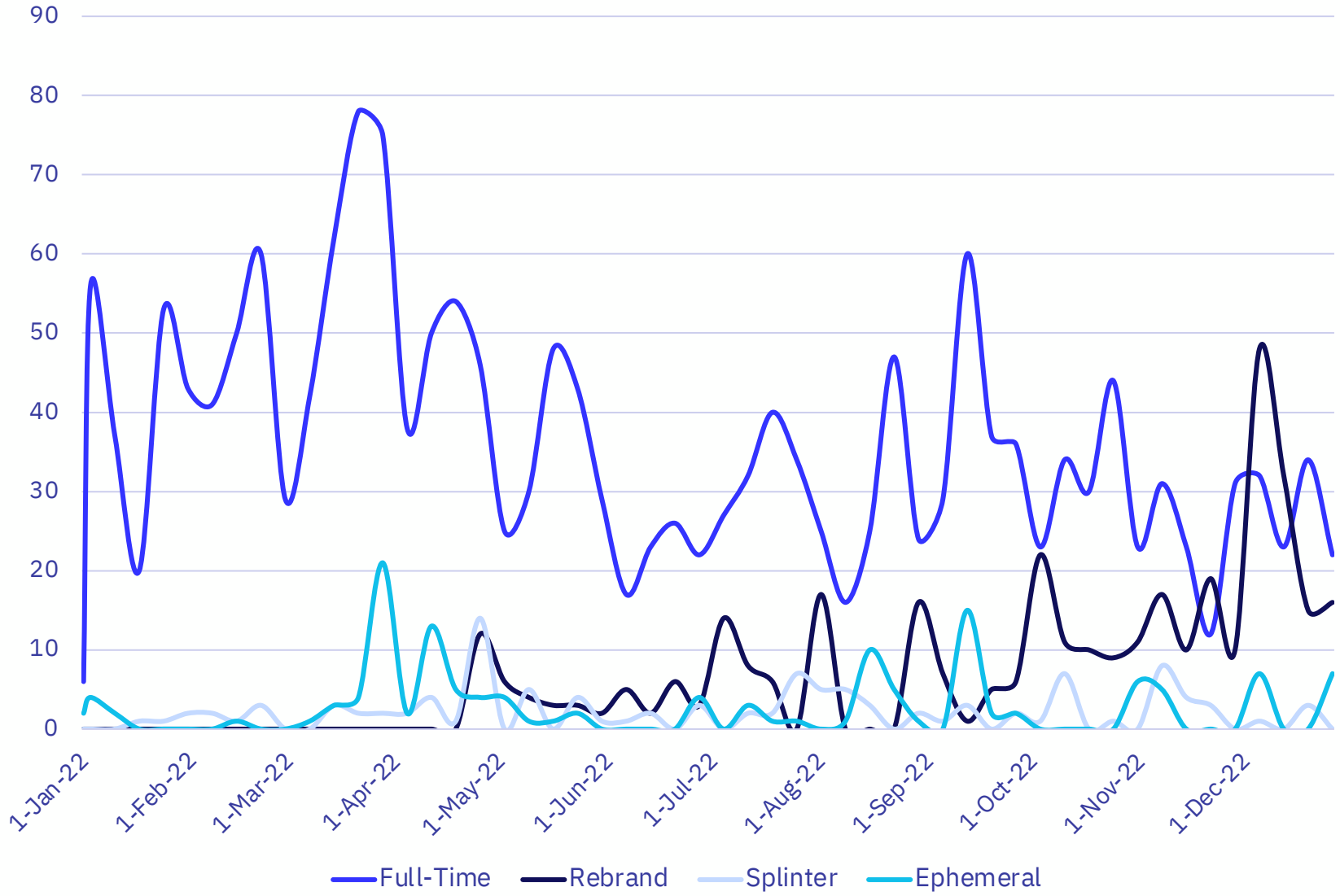
As observed through all of 2022, the United States is by far the most targeted country across all ransomware groups, and Western countries made up for the vast majority (77%) of all ransomware attacks.

There seems to be no direct correlation between industries targeted based on country.

Threat Actor Activity Breakdown

2022 Recap

Rate of Publicly Posted Ransomware Victims (2022)



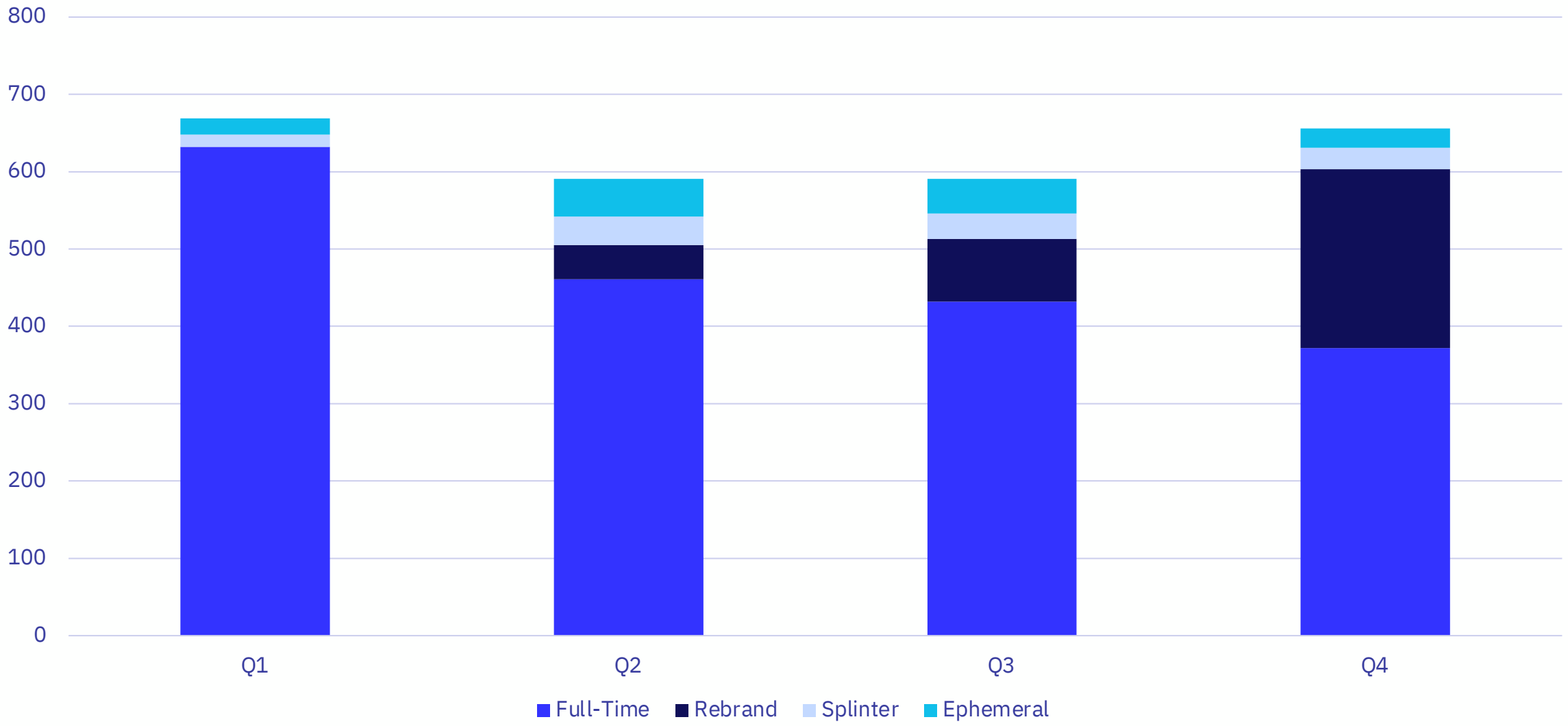
Q1 and Q4 were the most active quarters of the year, while Q2 and Q3 showed less activity.

Full-Time group activity steadily declined as 2022 progressed, which may show the potential impacts of Conti's mid-year rebrand effort and the proliferation of new Rebrand groups entering the scene.

Mirroring the decline in Full-Time group activity, Rebrand group activity grew steadily as 2022 progressed, culminating in a large surge in Q4.

Splinter and Ephemeral group activity remained consistent throughout 2022.

Post Rates per Quarter

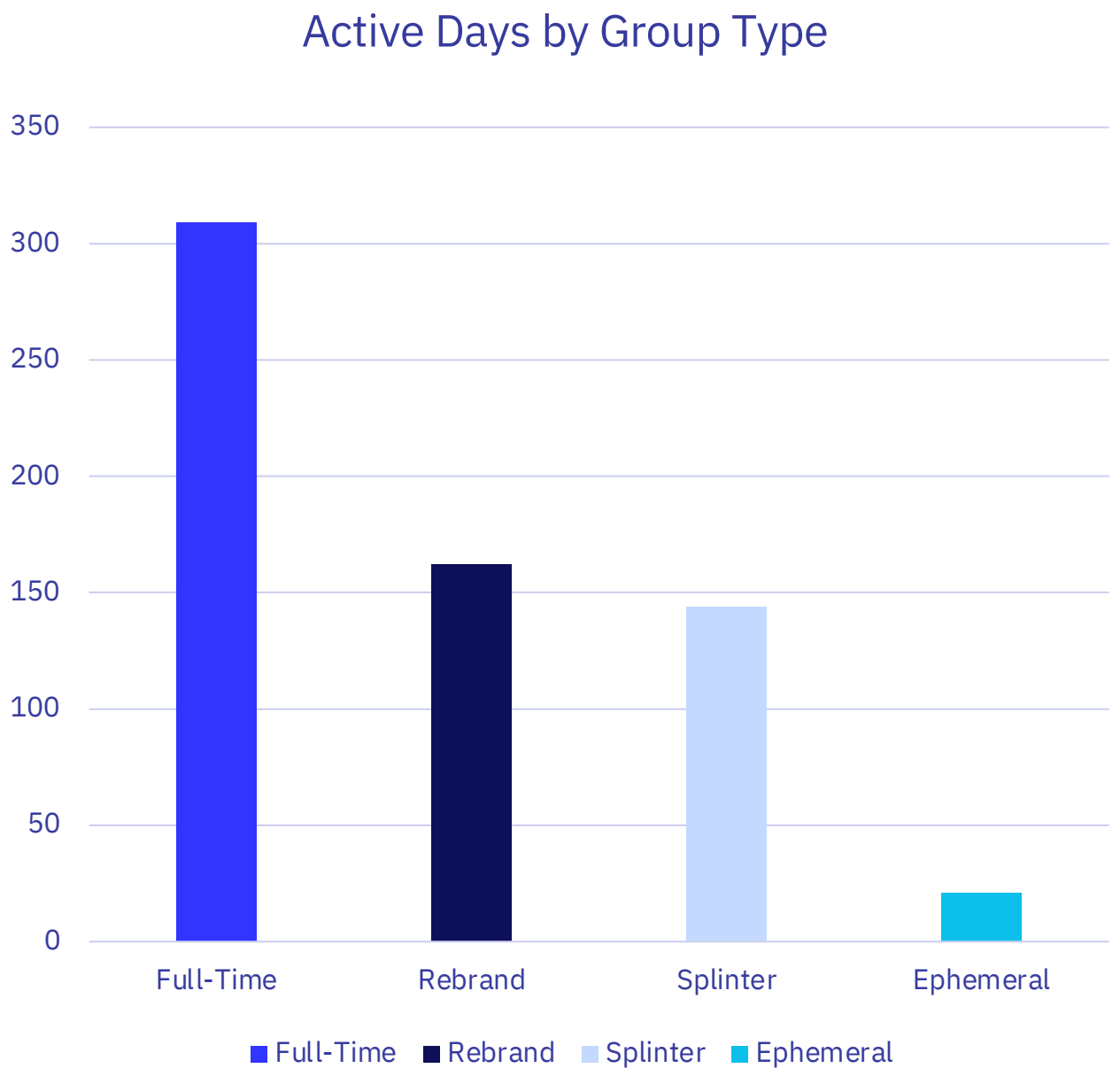


2022 Average Operating Duration by Group Type

The average days active in 2022 for each group type represents a clear illustration of the taxonomies defined by GRIT.

The average operating duration of Splinter groups rivaled the average duration of rebrand groups. This illustrates the maturation process pursued by many groups as they progress from Splinter, to rebrand, and potentially full-time. If an Ephemeral group matures into a successful splinter group, it is likely that they will mature into higher and more consistent group types.

On average, ephemeral groups only operated for 21 days–showing their "flash in the pan" nature–and contribute to the volatility associated with the number of groups operating during any given week.



Industry Targeting by Group Type

Full-Time

Victim Industry	Number of Public Victims
Manufacturing	320
Technology	234
Construction	233
Retail and Wholesale	210
Banking and Finance	192

Rebrand

Victim Industry	Number of Public Victims
Manufacturing	50
Construction	25
Technology	24
Retail and Wholesale	20
Industrial Services	20

Splinter

Victim Industry	Number of Public Victims
Manufacturing	15
Healthcare	14
Retail and Wholesale	11
Banking and Finance	11
Technology	10

Ephemeral

Victim Industry	Number of Public Victims
Technology	41
Manufacturing	21
Banking and Finance	21
Healthcare	16
Education	15

Manufacturing was by far the most targeted industry among Full-Time ransomware group victims. This carries over to both Rebrand and Splinter groups, with only Ephemeral groups preferring to target the Technology sector over Manufacturing.

Following Manufacturing, Full-Time and Rebrand groups targeted Construction and Technology victims at near identical rates.

Splinter and Ephemeral groups are more likely to target sensitive industries like healthcare and education relative to their total victimology.

Retail and Wholesale appears in the top 5 industries for of all group types except Ephemeral.

Rebrand is the only group type that included Industrial Services in their top 5, of which Blackbasta accounted for 55% of victims.

Industry Targeting by Group Type

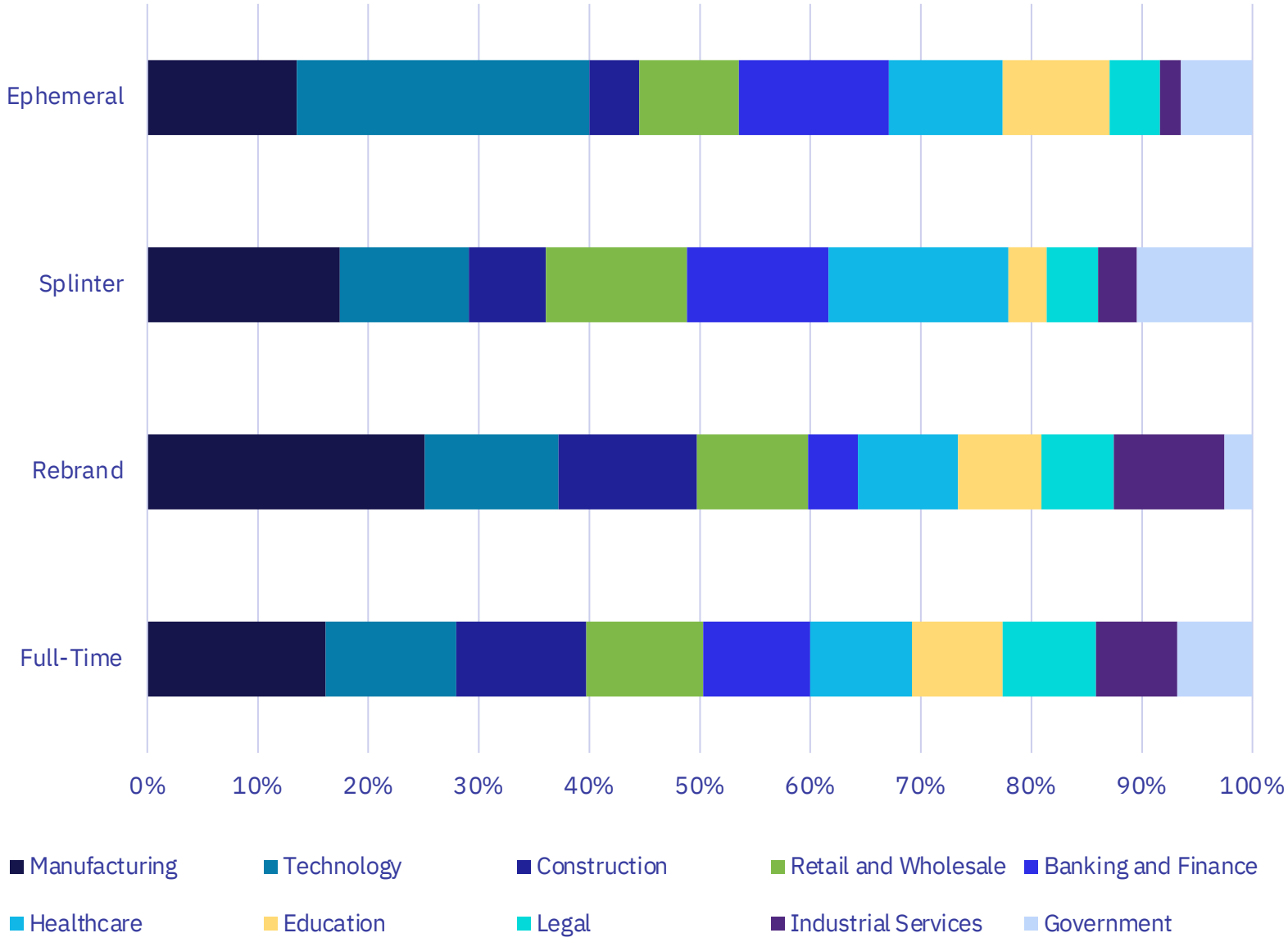
While Full-Time groups represent the most claimed victims across all categories, Rebrand groups disproportionately target Manufacturing victims relative to their total victimology.

Full-Time and Splinter groups have a similar percentage relative to their total.

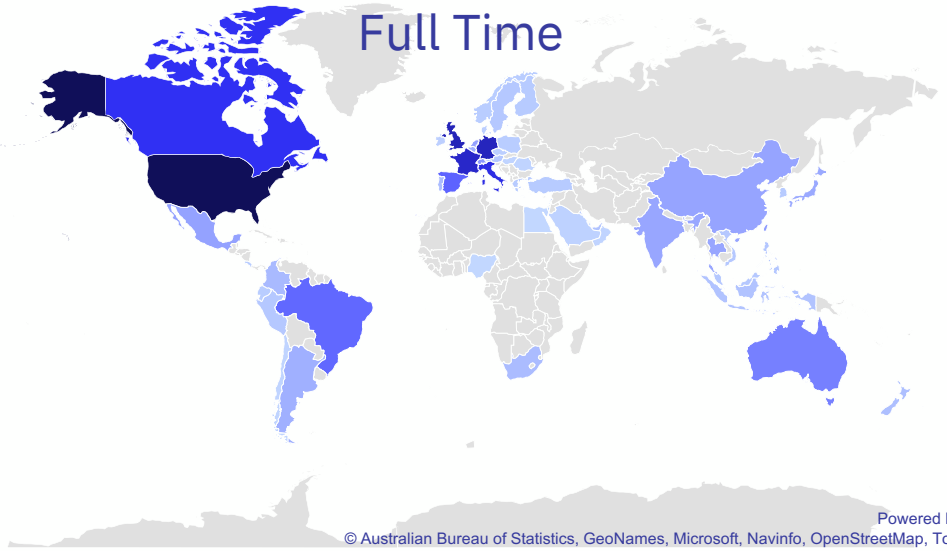
Ephemeral groups have the highest percentage of Technology victims relative to their total victimology while Full-Time, Rebrand, and Splinter groups have a similar relative percentage.

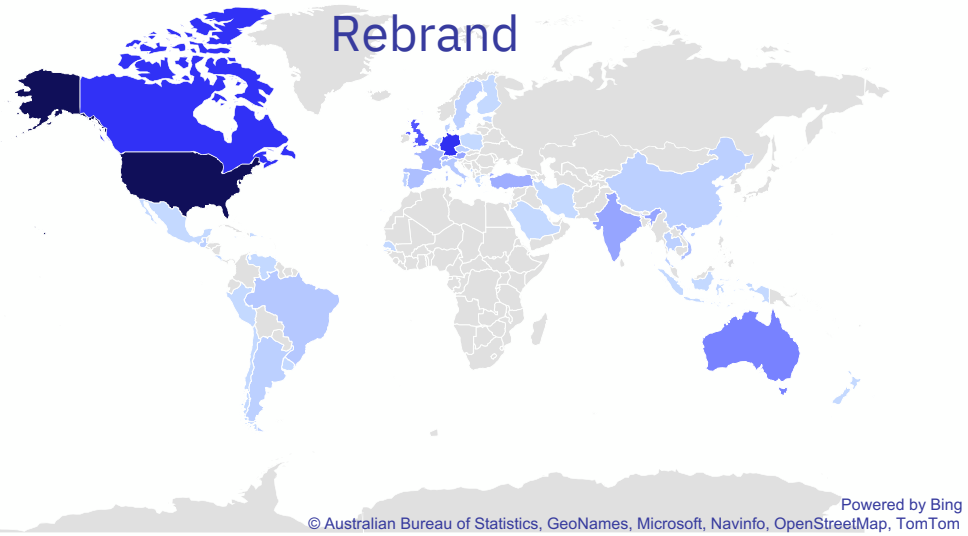
Splinter groups have the highest percentage of Healthcare and Government victims relative to their total victimology.

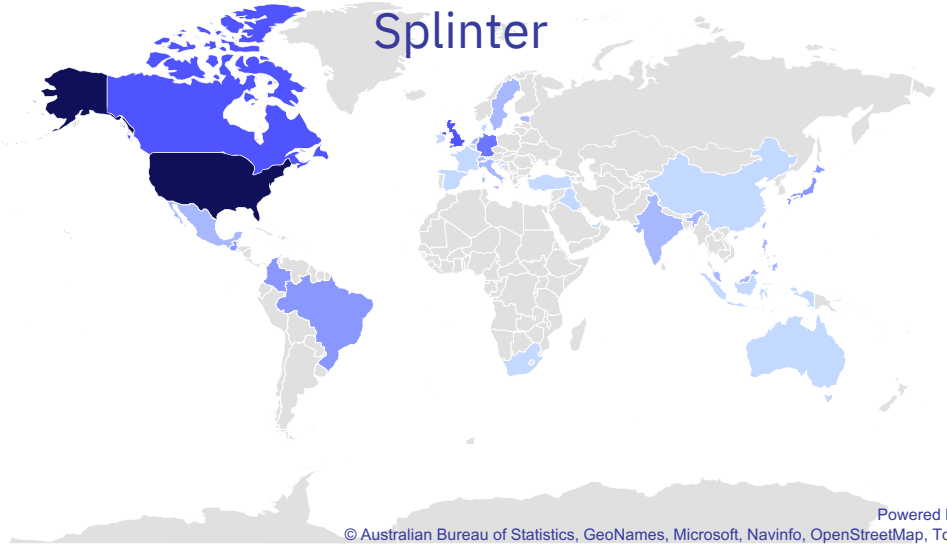
Rebrand groups have the lowest targeting of Banking and Finance and Government by far relative to their total victimology.

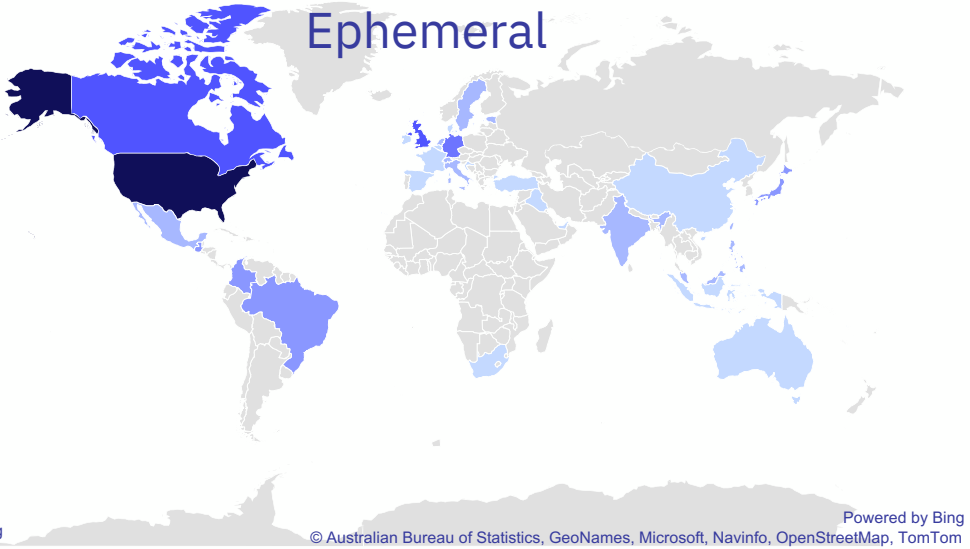


Country Targeting by Group Type









Top 5 Countries per Group Type

FULL-TIME
1. United States
2. United Kingdom
3. Germany
4. France
5. Italy

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

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

EPHEMERAL
1. United States
2. Spain
3. United Kingdom
4. Germany
5. United Arab Emirates

Top 5 Countries per Group Type

Regardless of group type, the United States was the most targeted country.

Full-Time groups are far more likely to target China with ransomware attacks (23 in 2022 compared to 4 combined for all other group types).

Full-time and Rebrand groups have a much more distributed targeting presence in South America compared to Splinter and Ephemeral groups, which were both exclusively focused on Brazil and Columbia.

Outside of targeting the United States, Full-Time and Rebrand groups are more likely to focus their efforts on western countries while Splinter and Ephemeral groups are much more evenly distributed around the world.

All group types show a lack of targeting former Soviet Union countries.

Major Events and Observations

2022 Recap

Major Events and Observations

- **In Q1, the industry observed Conti's internal struggles stemming from their back and forth support for Russia in their conflict with Ukraine.**
  - This ultimately resulted in a massive leak of their playbooks, infrastructure, source code, and more that led to an unrecoverable state for the group.
  - Conti disbanded early in 2022 in favor of pursuing operations after a thorough rebranding process into groups such as Blackbasta, AlphV, and more.
- **More ransomware groups are seeing the value of single extortion methodology**
  - Lockbit explicitly allows exfiltration of data of all industries, including critical infrastructure
  - More groups are seeing the benefits of leveraging data exfiltration for payment without encryption
- **Vulnerability exploitation was solidified as one of the most effective methods of achieving initial access into victim networks**
  - Many critical vulnerabilities were either being exploited in the wild at the time of initial disclosure while other vulnerabilities were being weaponized within days of disclosure.
    - Organizations are hardly, if at all, able to keep up in their normal patching cycles.

Major Events and Observations

- **ESXi encryption maintained a spot in the hearts of threat actors**
  - Even splinter and ephemeral groups are seeing the advantages of targeting ESXi hypervisor servers as a means of encrypting key parts of a victim's infrastructure simultaneously
  - Groups of all maturities understand the value of hypervisors and are using these to put significant pressure on victim organizations to pay ransoms
- **Relationships with initial access brokers are becoming more apparent with ransomware groups**
  - Ransomware groups are seeing the value of initial access brokers and are leveraging their access of personal and organization owned devices to improve their operational efficiency and improve ROI
- **Threat actors are still leveraging many of the same tactics and techniques to compromise victim organizations**
  - Open RDP and SSH to the internet remain commonly exploited by threat actors
  - Unpatched and dated vulnerabilities are still being successfully leveraged for initial access
- **Threat actors continue to demonstrate their flexibility**
  - Microsoft's change of default Office Macro behavior was a step in the right direction, but ultimately forced a rapid change in initial delivery methods for email-based attacks.

Q4 Ransomware Trends Recap

Q4 Summary

Now that we've taken a deep dive into overall ransomware activity in 2022, we wanted to take a step back and review the activity we tracked during Q4 of 2022.

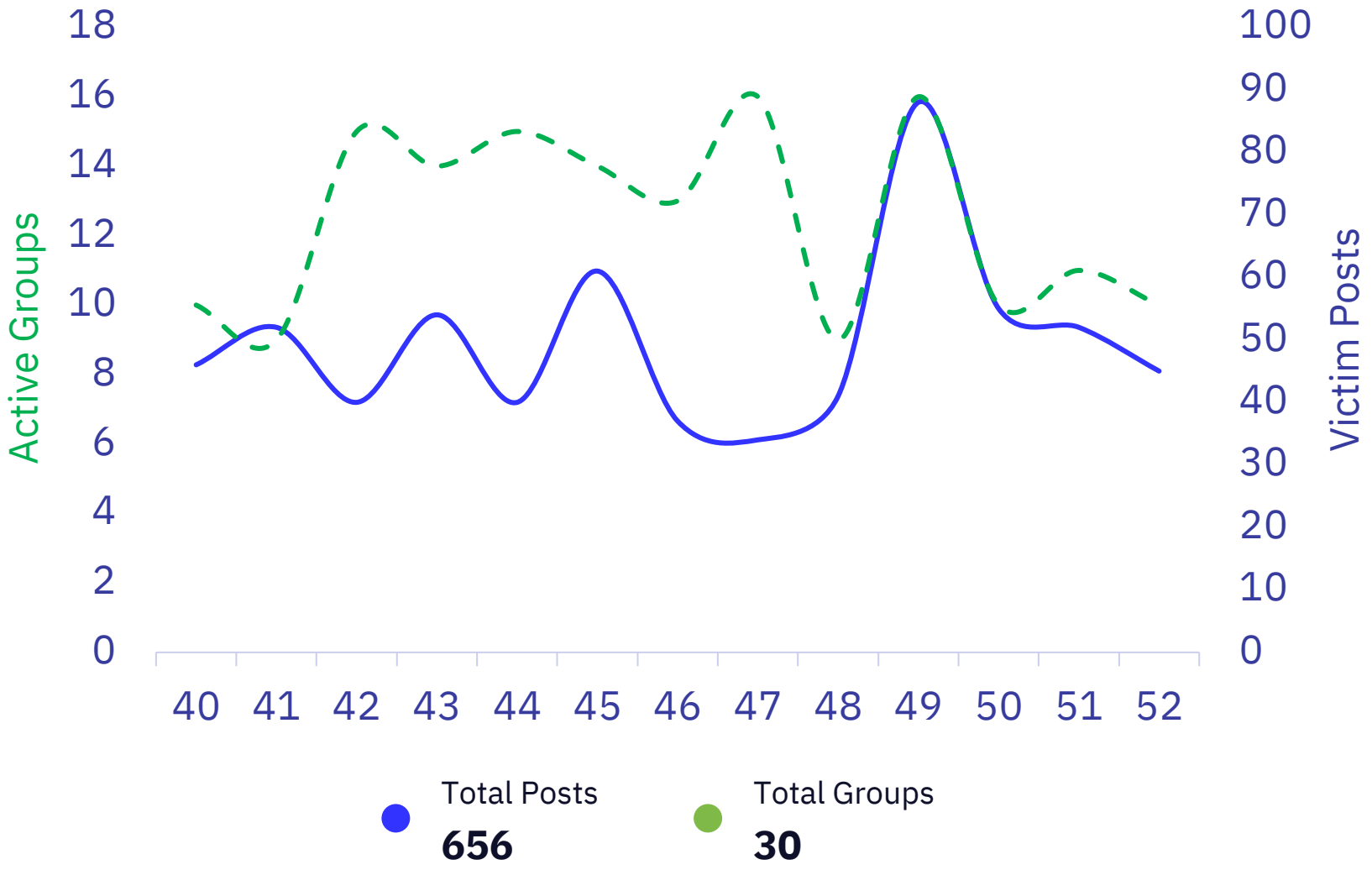
Q4 saw a rise back to Q1 victim posting rates after a two-quarter slowdown in publicly observed activity. Lockbit continued its reign as the most impactful ransomware group, while new groups like Royal entered the double extortion realm with a bang. Major players like AlphV, Bian Lian, and Blackbasta maintained their presence in the top ransomware groups of the quarter with consistent activity.

Interestingly, Lockbit publicly upheld their affiliate rules by banning an affiliate for encrypting a children's hospital in Canada, while other groups, like Vice Society, continue to prove that no industry is off limits.

As Q4 ended, we observed ransomware trends continue to hold their place as the most likely and impactful eCrime threat that all organizations across all industries face.

Total Publicly Posted Ransomware Victims	656
Number of Tracked Ransomware Groups	30
Average Posting Rate (per day)	7.13

Rate of Publicly Posted Ransomware Victims



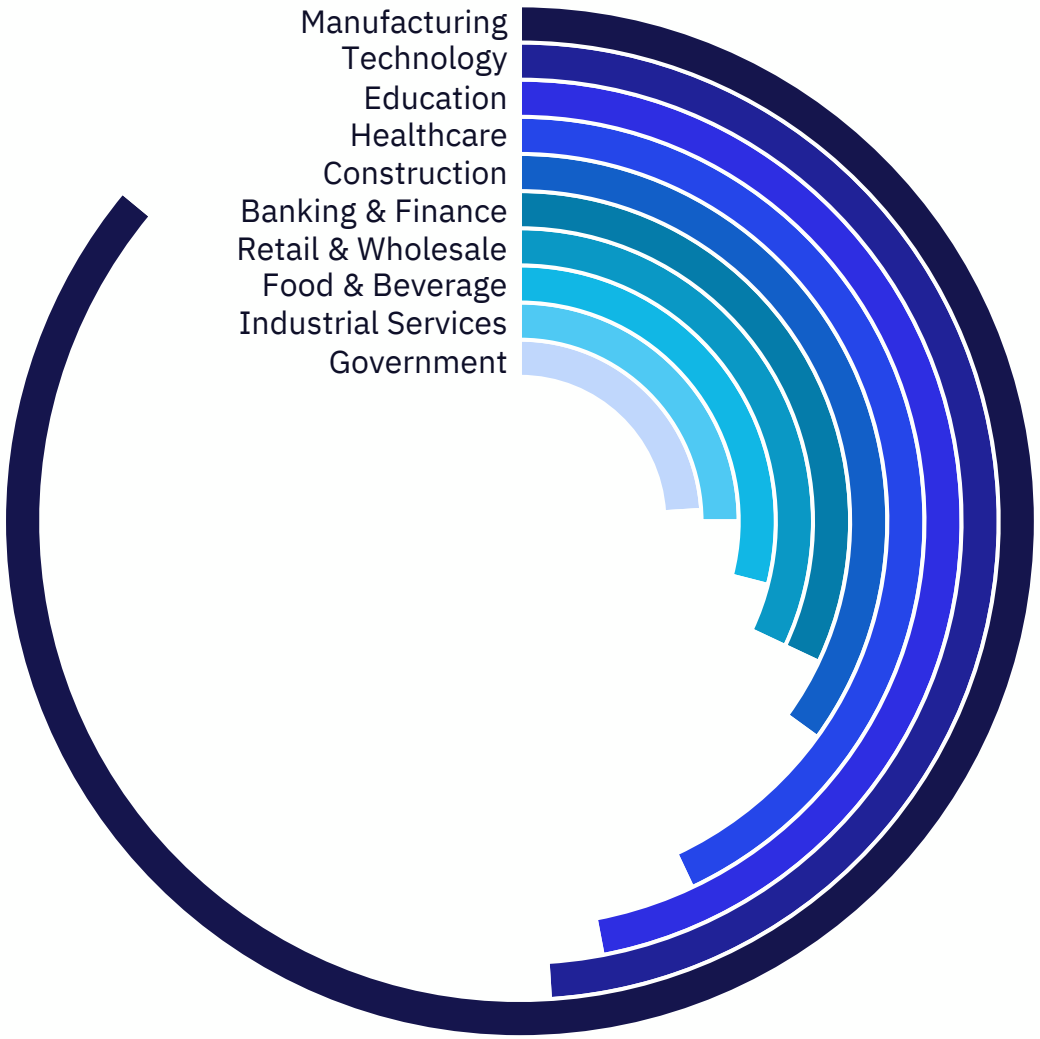
Victim posting rate was consistent in early Q4, but shortly after the mid-November start of World Cup in Qatar the rate dropped sharply.

The high number of groups active from week 42 through 47 also saw a steep drop after the World Cup, but the resurgence in mid-December may correlate to a lull in new attacks as they negotiated with victims, followed by a surge in posts when negotiations went south.

However, this pullback was short-lived, as we observed a surge in mid-December before returning to the average posting rate of Q4.

Overall, Q4 saw a 15.5% increase in reported victims and a minor increase from 27 active groups in Q3 to 30.

Most Impacted Industries – Top 4

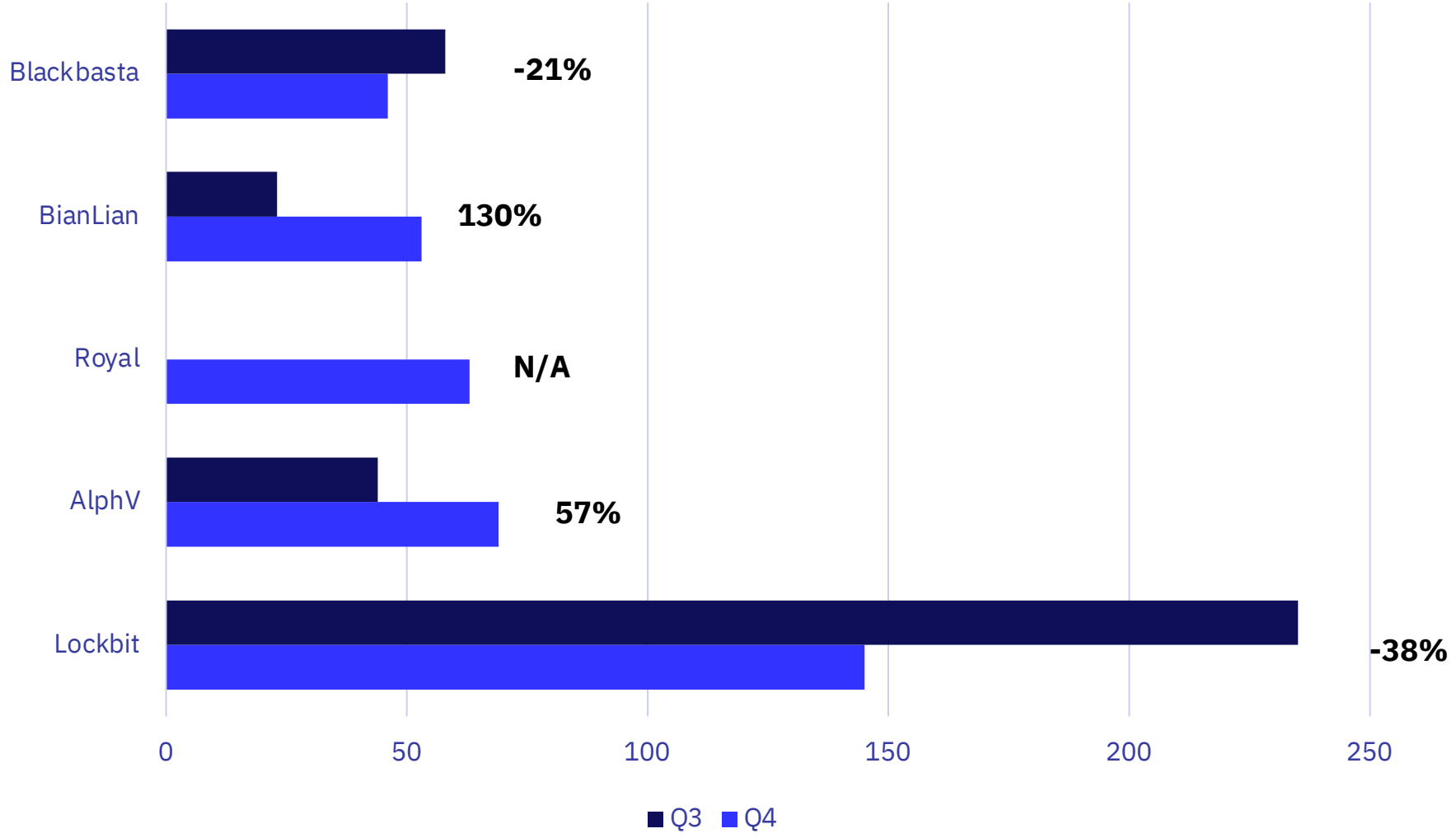


- Manufacturing
  - Lockbit
  - Blackbasta
  - Royal
- Technology
  - Lockbit
  - AlphV
  - Royal
- Education
  - ViceSociety
  - BianLian
  - Hive
- Healthcare
  - Lockbit
  - Everest
  - BianLian

In Q3 Manufacturing tied with Technology for most targeted industry, but in Q4 Manufacturing saw an aggressive 59% increase in public postings. At the same time, the Technology vertical saw a 9% decrease in publicly posted victims, widening the gap even further.

As noted in our last quarterly report, there is often very little change in the industries that make up the top 10 most targeted. However, in Q3 legal made a surge into the rankings and held a spot there through November, but was bumped from the list by the end of Q4.

Top 5 Ransomware Threat Actors – Changes from Q3 to Q4



Geographic Breakdown of Ransomware Victims (Q4 2022)

Similar to Q3, ransomware attacks targeted mostly western countries in Q4.

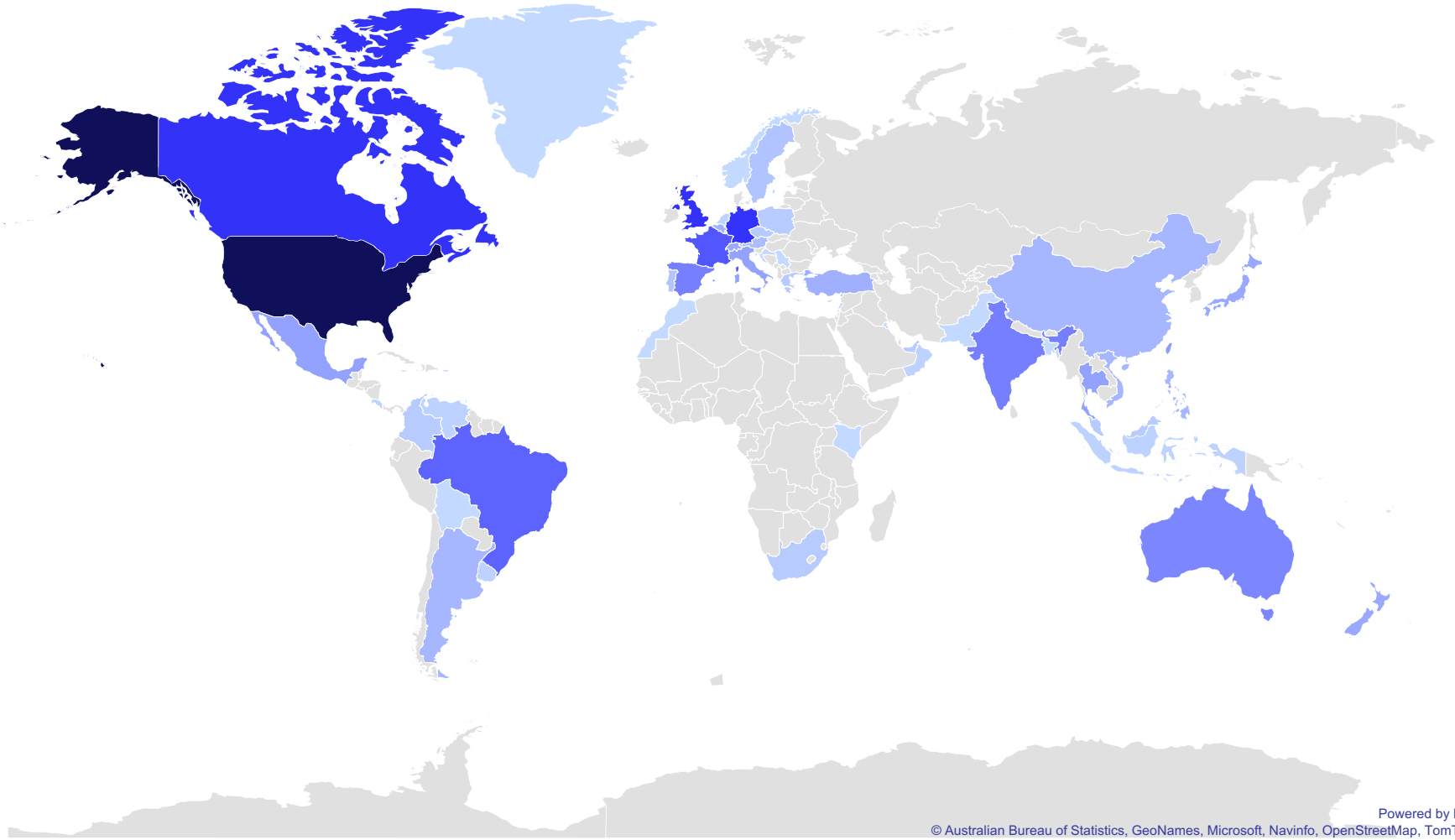
Among the top 10, only India, Taiwan, and Australia were outside Europe and the Americas.

There was a 32% increase in victim posts in the US. Compared to Q3, India saw a 100% increase in the number of posted victims, bringing them into the top 10.

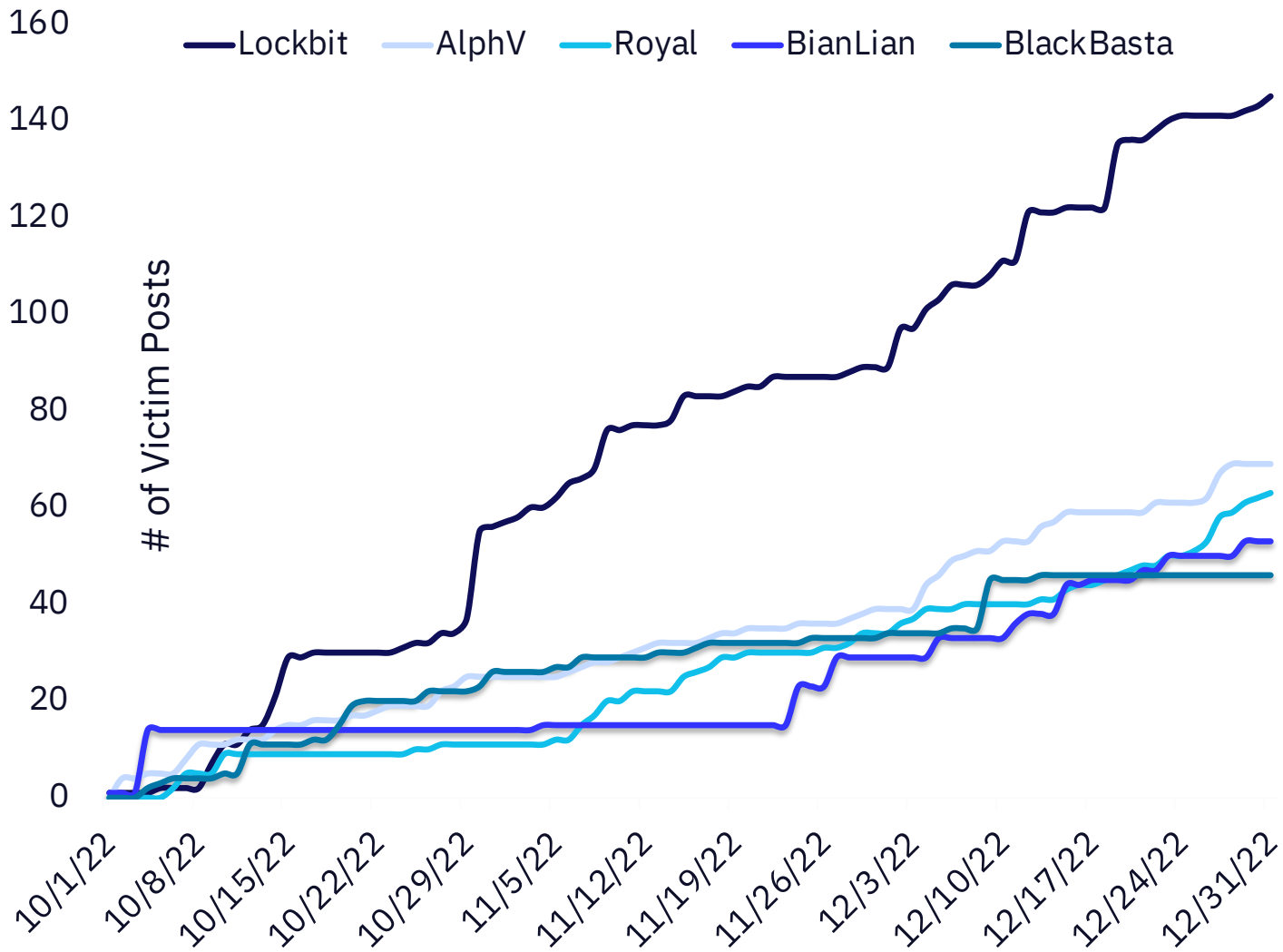
New victim countries (countries that have not been seen in reports since GRIT began tracking) for the quarter included Monaco, Gambia, Greenland, Gibraltar, and Vanyuatu.

Top 10:

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



Cumulative Victims by Threat Group



Ransomware Activity – Q4 2022

LockBit continues to be the most prolific ransomware group in Q4, despite a slowdown in victim posting. They hit a daily high of 18 victim posts in October, which makes it their third highest posting day in all of 2022. Compared to Q3, LockBit made a significant shift away from targeting in the legal industry this quarter.

We observed a a 57% increase in AlphV's reported victims in Q4. Alongside this increase, 34% of their annual Manufacturing and Technology victims were posted this quarter.

Royal's leak site went live at the beginning of Q4 in October, and by the end of the year had already claimed 63 victims. Despite their recent emergence, the group tied for the most targeting of the Food and Beverage industry in Q4. Even with that focus, their victims span 24 industries across 14 countries.

2023 Predictions

2023 Predictions

First, we believe 2023 will continue to see an increase in ransomware rebranding.

- GRIT's 2022 threat actor trends show an increase in rebrand, splinter, and ephemeral group's share of total victims as 2022 progressed
- There has been at least one new group for every month of 2022, this will likely continue throughout 2023

Second, vulnerabilities will continue to be heavily researched and utilized for initial intrusion into networks.

- The time to weaponization of these vulnerabilities is likely to decrease as 2023 progresses

Third, as organizations rely on the fundamentals of security to establish effective security programs and make the threat actors' lives harder, ransomware groups will likely move to single extortion attempts based on exfiltration of data where no encryption event occurs. We believe this will be especially true for critical infrastructure and sensitive industries.

Fourth, and this will aid in our second prediction, emerging technologies like ChatGPT, OpenAI, and others will be leveraged to automate social engineering and other initial intrusion capabilities.

Finally, as multifactor authentication and zero trust architecture continue to be adopted, personal devices will likely be targeted to establish initial intrusions into business networks.

- Info stealers such as redline stealer, raccoon stealer, etc. will continue to be an extremely viable resource for threat actors to leverage as an initial intrusion vector.

2022 Wrap Up

After years of ransomware activity, it seems safe to say that ransomware is here to stay, for quite awhile at least. Ransomware groups are claiming victims at a staggering rate and new ransomware groups are formed, and sometimes disbanded, on a monthly basis. At the end of the day, the ransomware problem is still very real.

GRIT's goal with this research is to educate cybersecurity professionals and leadership, and to encourage security researchers to continue to work together to further our defensive and threat intelligence capabilities. If we continue to share intelligence and establish open and dynamic methods of communication, it's possible that we can start to keep up with the ransomware threat. Through collaboration, we can start to be flexible and adaptable, just like our adversaries.

Ransomware groups will continue to target us on a regular basis and leverage any means necessary to accomplish their goals, but that doesn't mean it's all "doom and gloom" moving forward. Through well-established cybersecurity foundations we can start to limit the risk associated with unpatched vulnerabilities and lack of visibility. We can focus on ensuring coverage with our security tools and that our analysts and leadership are well equipped to handle potential incidents as they arise. Admittedly, this is a large task for almost any team, but, if we focus on small wins, and we maintain forward progress, we will make it exponentially more difficult for ransomware groups to be successful.

GRIT has already begun researching ransomware trends in 2023 and we plan to continue to extend our research capabilities to give granular and informative insights into ransomware groups. Through our continued research we hope to disrupt ransomware groups by arming cybersecurity professionals with knowledge and intelligence.

So, here's to 2023 and another successful year of intelligence sharing. Happy hunting!