



# GRIT

## Ransomware Report

JULY – SEPTEMBER 2022



# 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



Quarterly numbers: the who, what, and where of ransomware this quarter



Year-to-Date Trends



Industry Spotlight: Legal



Threat Actor Spotlight:  
Sparta Ransomware Group





Q 3 2 0 2 2 :

# Ransomware Summary

September brought yet another ransomware-filled quarter to a close. Although GRIT observed a slight slowdown in ransomware activity from the rates observed during Q2, ransomware continues to be the most prolific threat that organizations face across all industry verticals.

While Q3 saw a slight decrease in the total number of publicly posted ransomware victims and a slow down in the average public postings per day, GRIT observed some interesting trends, including Lockbit's continued dominance among Ransomware as a Service groups, Hive's 104% increase in publicly posted victims, and eight new ransomware groups that emerged in Q3.

The manufacturing industry saw a sharp decrease in publicly posted victims while the technology industry saw a sharp increase in victims, however, despite these large changes, the manufacturing and technology industries tied for the most targeted industries in Q3.

The United States continues to be the most impacted country with respect to publicly posted ransomware victims; however, Q3 saw 16 countries that were targeted for the first time this year, with six countries being targeted for the first time altogether.

Total Publicly Posted Ransomware Victims	568
Number of Tracked Ransomware Groups	27
Average Posting Rate (per day)	6.24

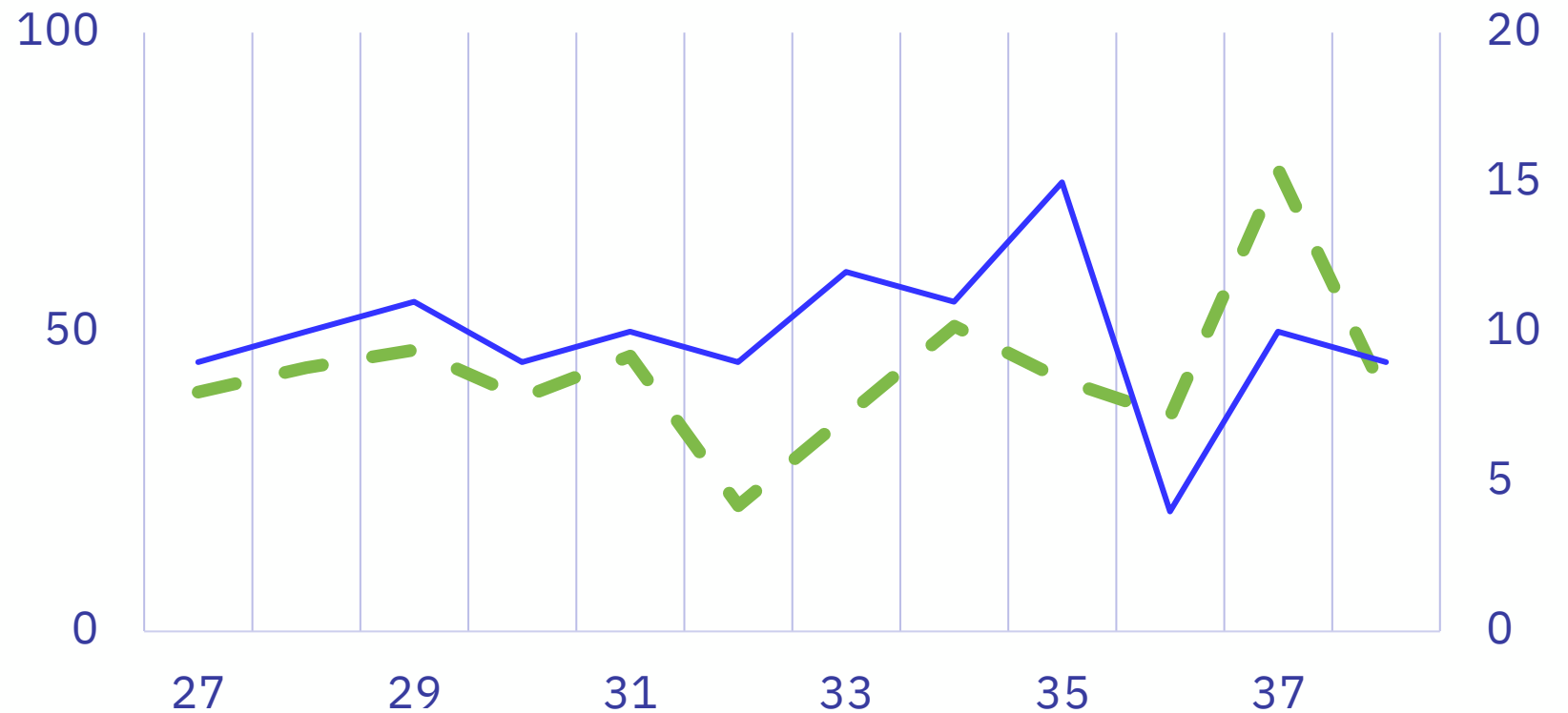


# Rate of Publicly Posted Ransomware Victims (Q3 2022)

Over the last quarter (covering July 1 to September 30, 2022), we tracked 27 active ransomware groups with a total of 568 posted victims. Both were a decrease from Q2, where we saw 30 active groups and 581 posted victims.

On average, there were 43 posted victims per week, and ten active ransomware groups per week.

The overall decrease in activity from Q2 to Q3 also lead to some weeks of surprisingly low victims and active groups. The second week of August saw only 21 victims, less than half of the average weekly activity for the quarter; and in the second week of September there were only four active ransomware groups, again less than half the average.

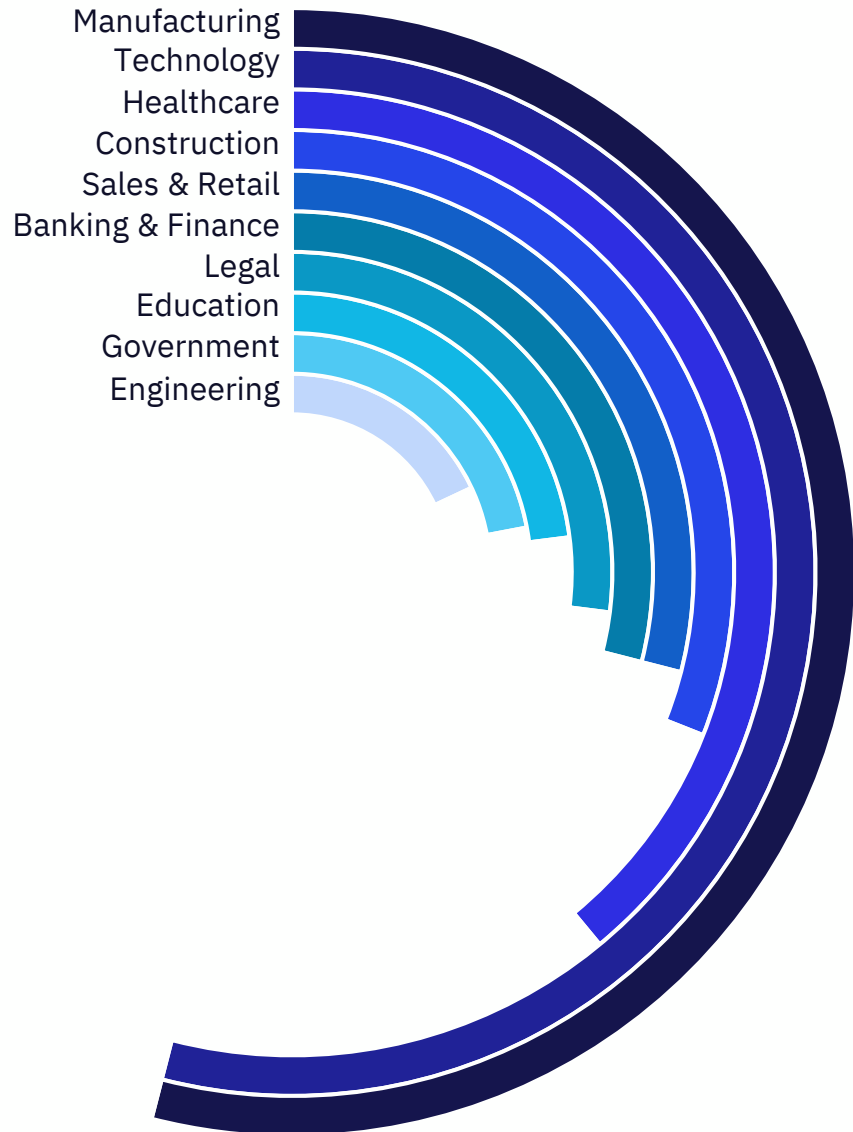


Calendar Week: July 1 – September 30

● Total Groups  
**27**

● Total Posts  
**568**





- Manufacturing
  - Lockbit
  - Blackbasta
  - Hive
- Technology
  - Lockbit
  - Icefire
  - Hive
- Healthcare
  - Lockbit
  - Hive
  - BianLian
- Construction
  - Lockbit
  - Alphv
  - Blackbasta

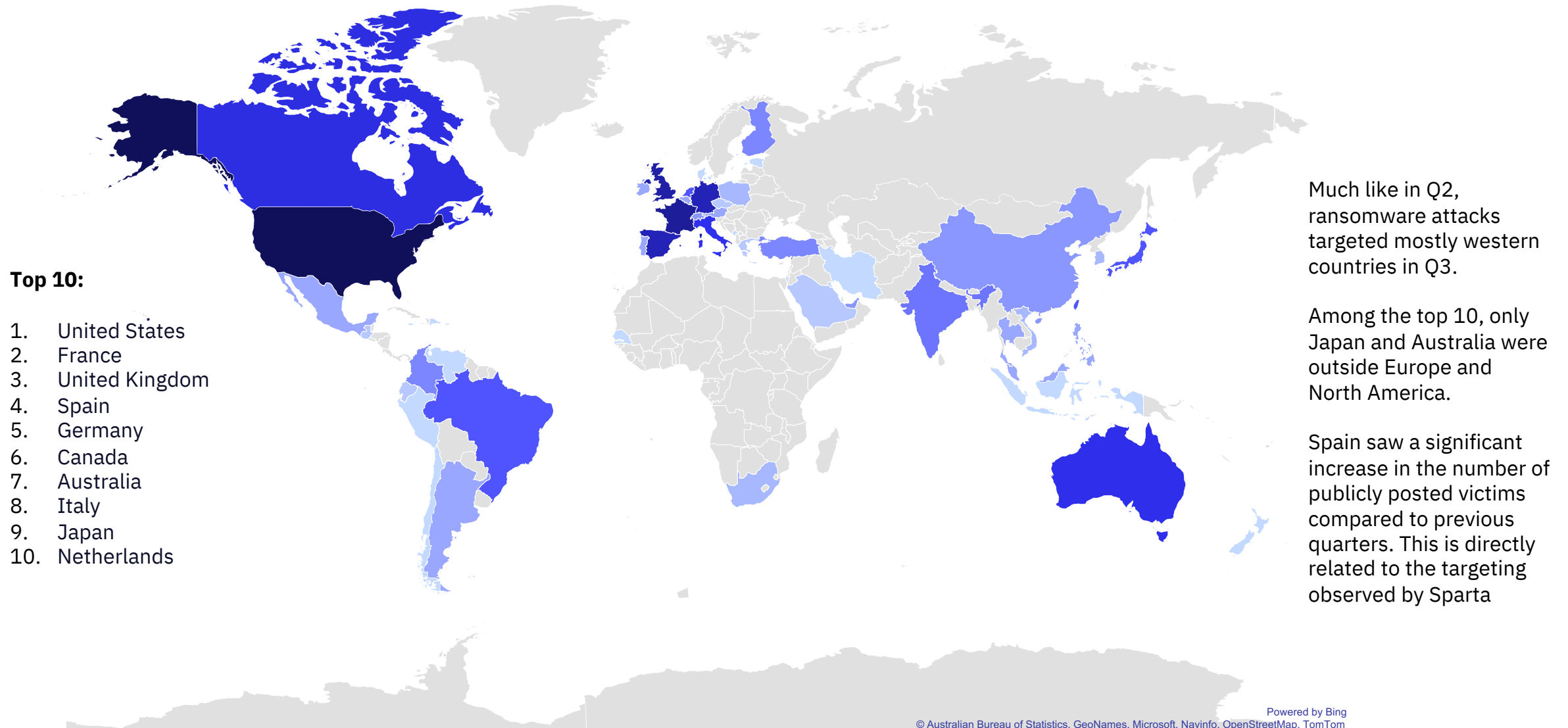
## Most Impacted Industries – Top 10 – Q3 2022

Though it still held its position as one of the most targeted industry in Q3, Manufacturing saw an 18% drop in public postings. At the same time, the Technology vertical saw a 20% increase in publicly posted victims, bringing the two to the same total number of 59 posted victims.

Quarter to quarter, there is very little change in the top 10 most targeted industries. However it is notable that outside of the top ten, the Hospitality and Insurance industries both saw large increases during Q3, which is a trend to keep an eye on as we move into Q4.



# Geographic Breakdown of Ransomware Victims (Q3 2022)



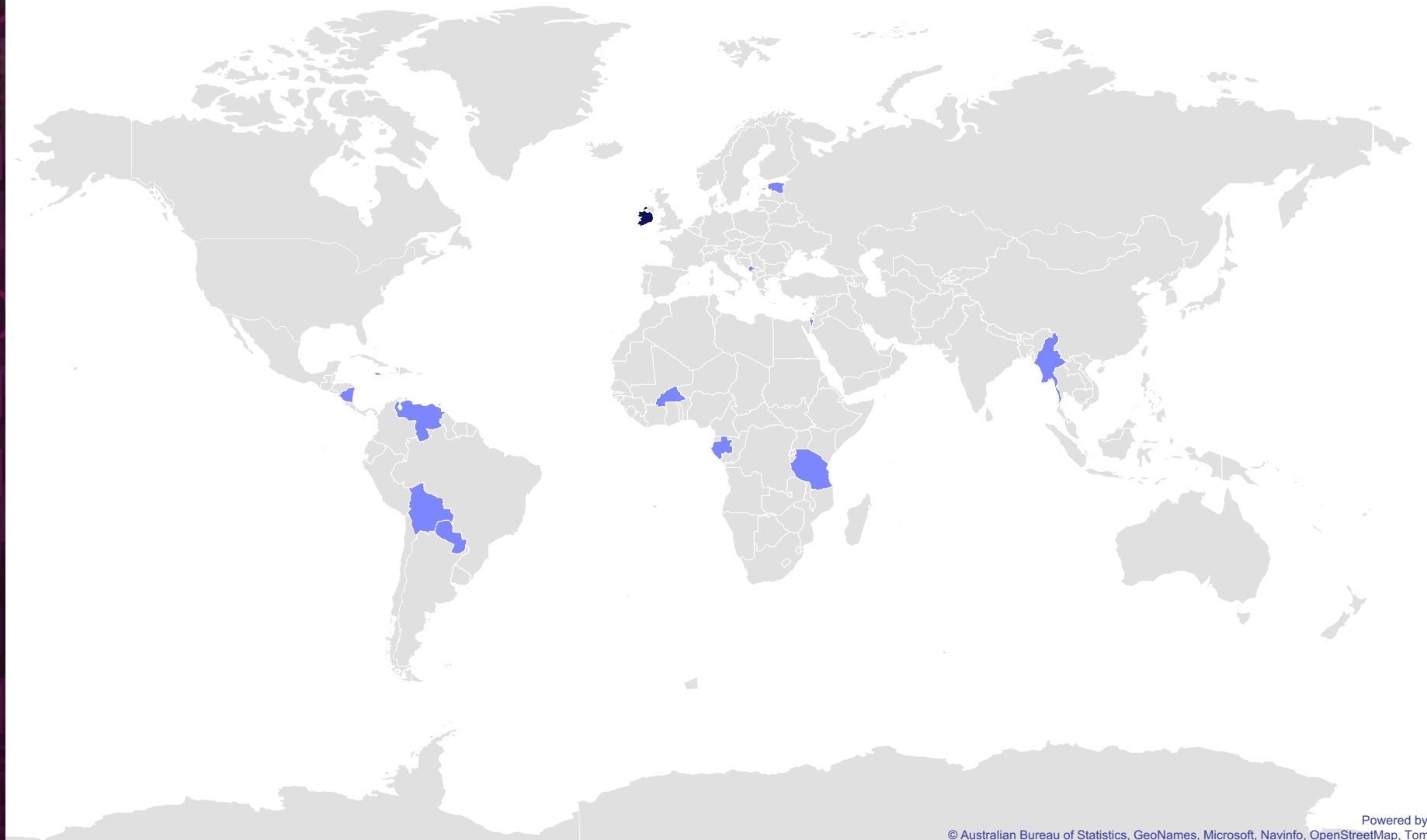


# Geographic Breakdown of Newly Targeted Ransomware Victims

Notably, Q3 saw 16 countries targeted for the first time this year.

Of those 16, six countries were targeted for the first time ever, three of which are countries in Africa. Those six countries were:

- Vatican City
- Seychelles
- Tanzania
- Montenegro
- Gabon
- Trinidad

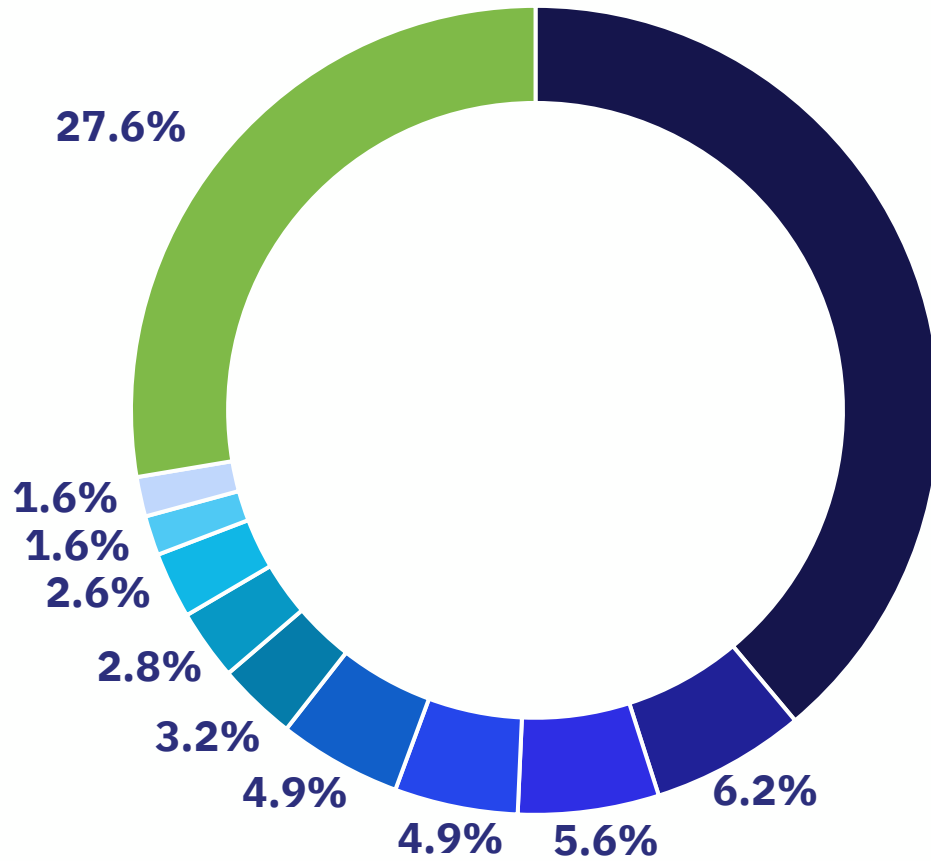




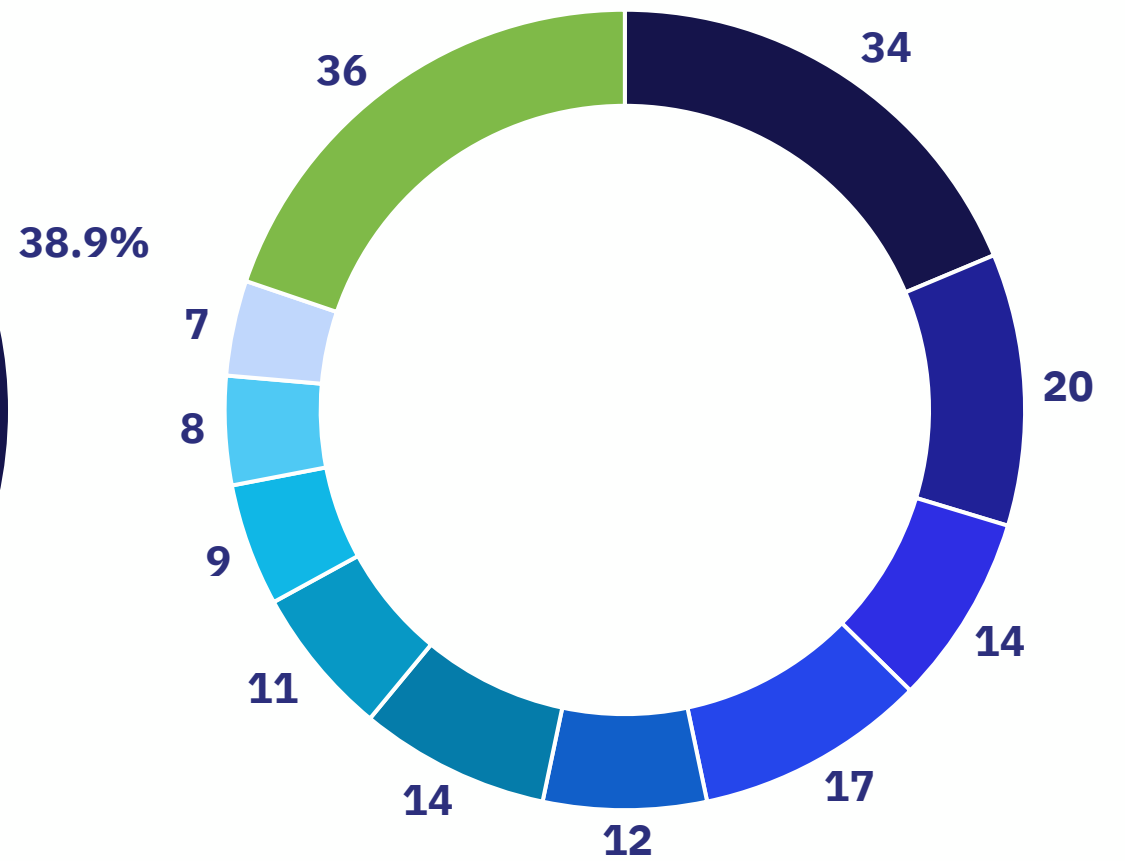
# Country Breakdown (All Threat Actors)

Percent of Total Victims

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

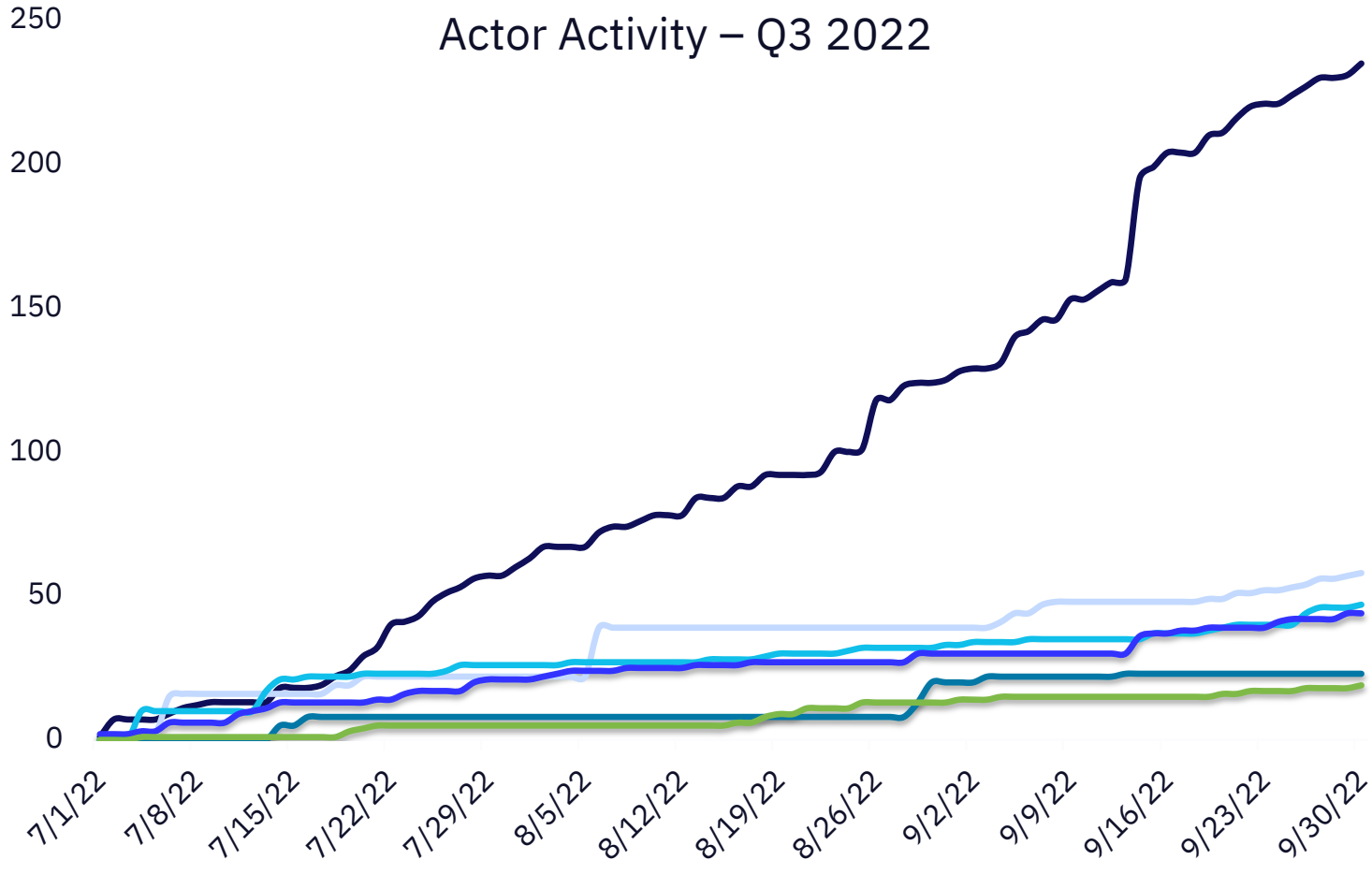


Number of Industries Targeted per country



# Cumulative Victims by Threat Group

Ransomware Threat Actor Activity – Q3 2022



Just like Q2, Lockbit is still by far the most prolific ransomware group. In total, Lockbit targeted 48 countries in Q3, including 19 which weren't Q2 targets. There were notable increases in targeting against France, the United States, and Netherlands.

BlackBasta moved up from the 4th rank to the 2nd, with a 32% increase in reported victims this quarter. In a change of tactics, Blackbasta has recently been observed using QakBot to initiate attacks.

Finally, the third most prolific threat actor of the quarter was Hive, who we specifically spotlighted in our July 2022 ransomware report. Their targeting tactics remain focused on Healthcare, with 12.8% of all reported Hive victims in the industry, twice the rate of Lockbit (6.4%).

- Lockbit
- Blackbasta
- Hive
- AlphV
- Bianlian
- Vice Society

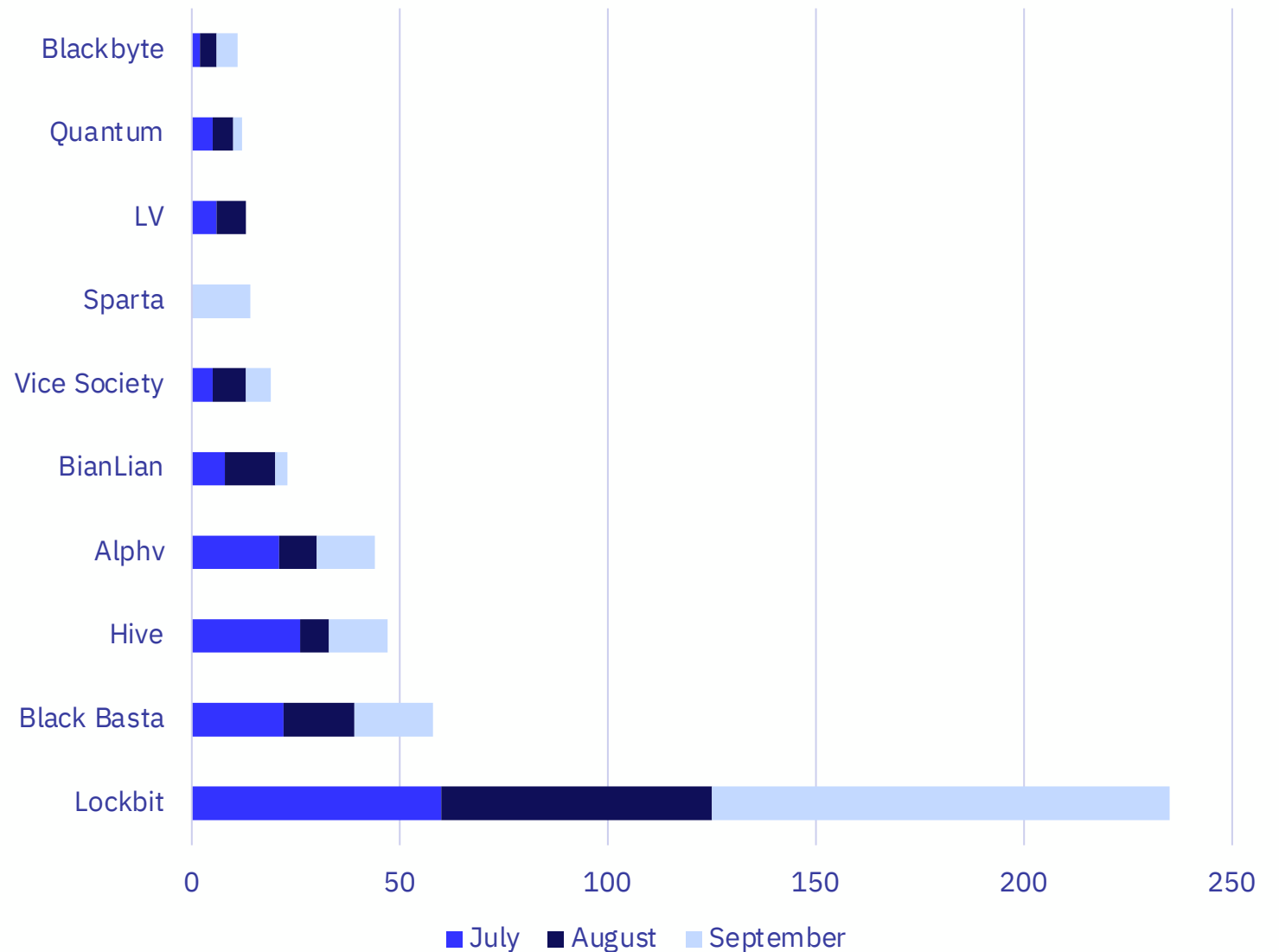


# Top 10 Ransomware Threat Actors

Through Q3, Lockbit held its position as a consistent threat, with an acceleration in activity through September.

Black Basta maintained a consistent amount of activity across all three months, with a slight slowdown in August but a rebound in September.

New to the top 10 this quarter is Sparta, which only became active in September but still managed to secure a spot just behind Vice Society.



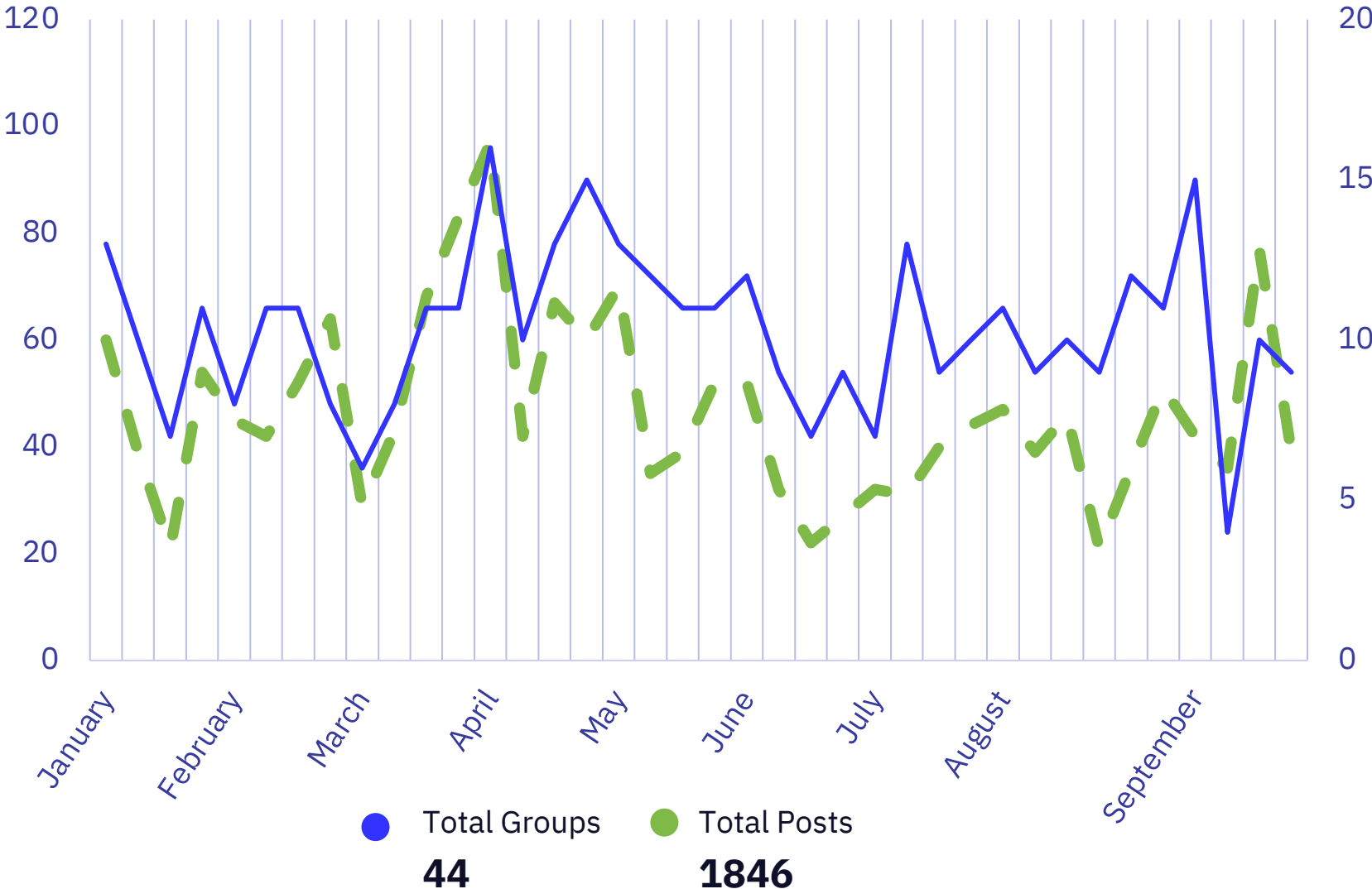




# Year to Date Ransomware Trends



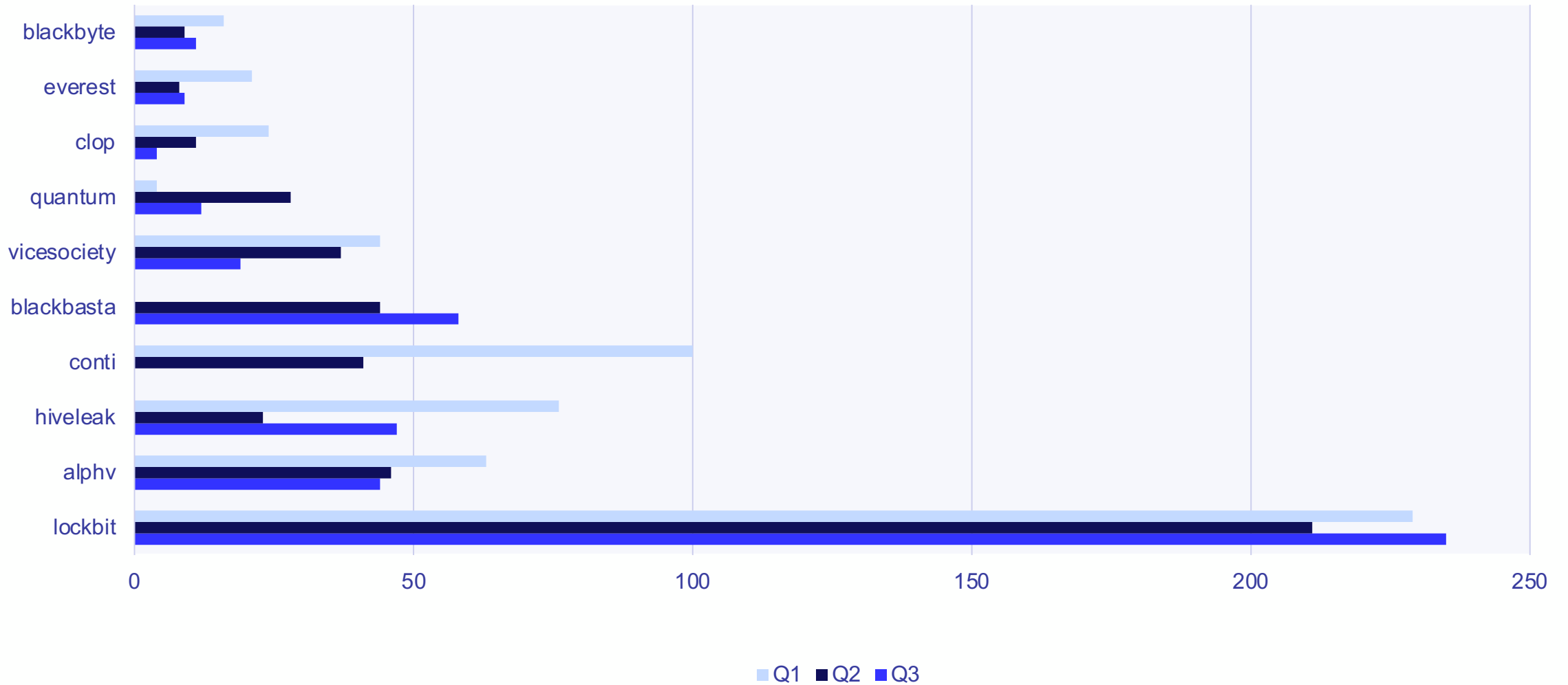
# Rate of Publicly Posted Ransomware Victims (Year to Date)



The significant fluctuations in activity observed through the end of Q2 continued into Q3. Year to date so far, 44 total groups have been observed with 1,846 total posted victims.

While Q3 continued the volatility of Q2, the significant spike and sharp decline in September may be attributable to Sparta's emergence and rapid posting of victims.

# Top 10 Ransomware Threat Actors (Year to Date)







# Industry Spotlight

Legal

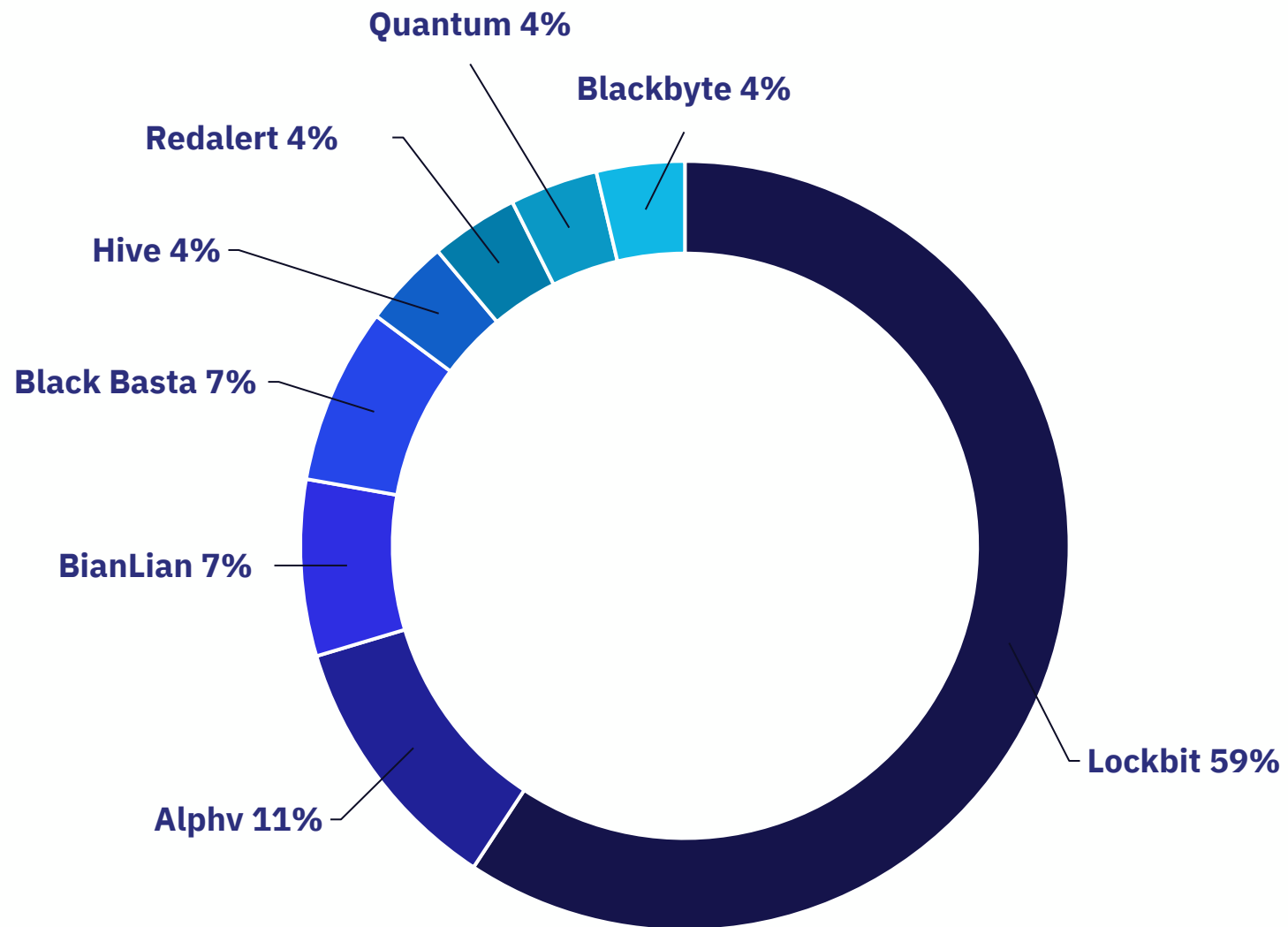


# Ransomware Threat Groups Targeting – Legal

In Q3, the number of groups targeting the legal industry grew from five groups targeting during Q2 to eight groups.

Lockbit's victim count in the Legal industry increased by 128%, though it's unclear if this shift was intentional targeting or simply an increase in attacks of opportunity.

Overall, Legal rose from the 16th most targeted industry in Q2 to the 7th most targeted in Q3, a trend that represents a significant risk for the industry as we move into Q4.

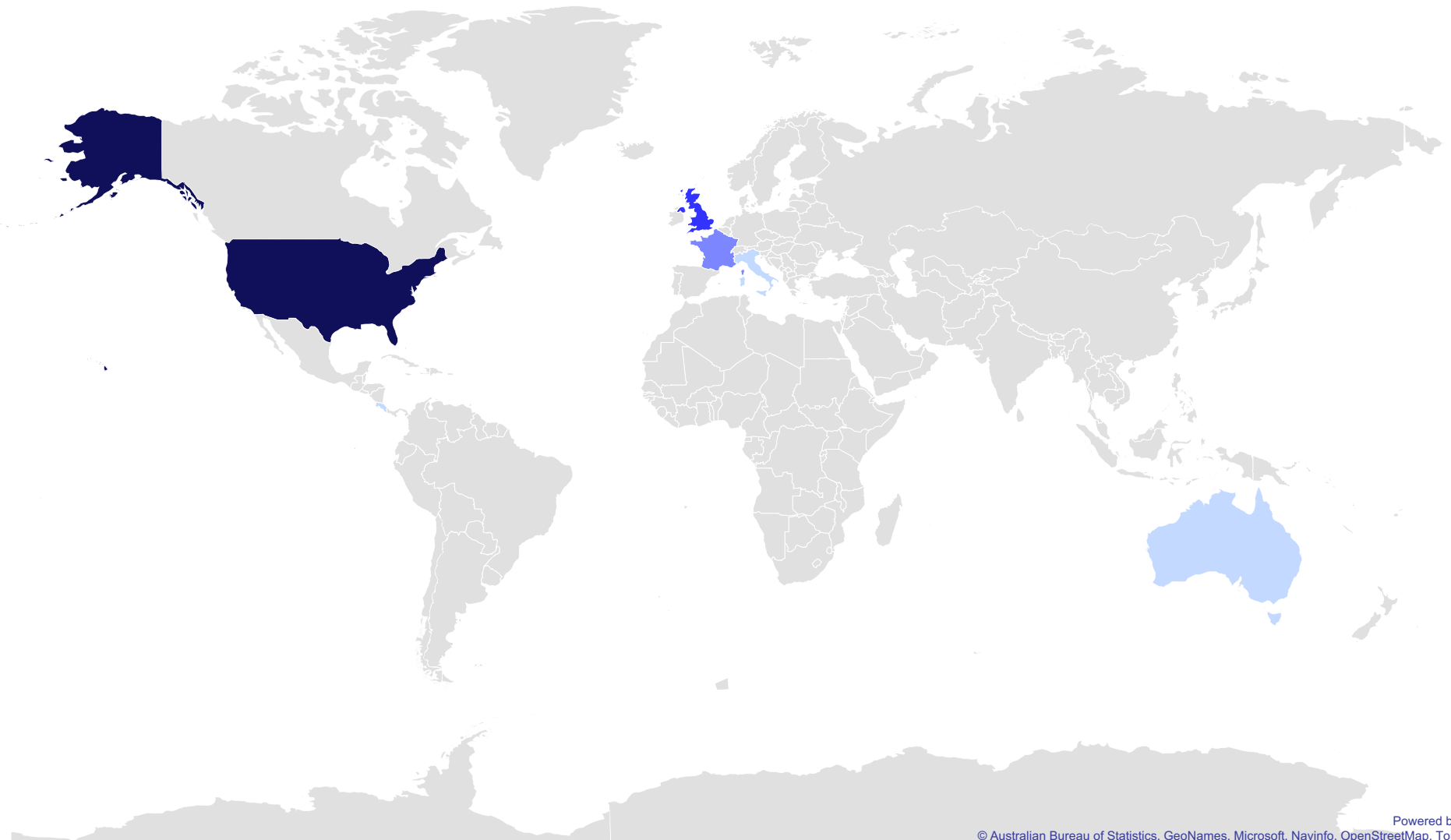




# Geographic Breakdown of Ransomware Victims (Legal Industry - Q3 2022)

## Countries Targeted

1. United States
2. United Kingdom
3. France
4. Seychelles
5. Italy
6. Costa Rica
7. Australia







# Threat Actor Spotlight

Sparta Ransomware Group



S P A R T A

# Threat Actor Statistics

Sparta is a new ransomware group that emerged in September 2022. As a relatively new group, few details are known about the group's tactics, techniques, and procedures (TTPs), however, there are a few details that have become clear based on their publicly leaked victims:

- All victims claimed by Sparta have been geolocated to Spain.
- As of the end of Q3, Sparta has targeted 11 industries, suggesting their targeting methodology is focused on location versus industry vertical.
- 12 of Sparta's total 14 victims were all claimed on a single day, September 13, 2022.

[Join Us](#) [Blog](#) [RSS 1.0 Feed](#)

**Sparta Blog**

- Based on observed Sparta ransom notes, the group appears to leverage email for communication, suggesting they are potentially less operationalized as other well-known groups such as Lockbit, Hive, or Blackbasta.

With Sparta's recent entry into double extortion-based ransomware, much remains to be seen with how this group will evolve, whether their targeting methodology will change, and whether we will see an increase in activity or whether they fade into a rebrand, which is becoming all too common across many ransomware groups at an increasing rate.

Don't worry, you can return all your files!

All your files like documents, photos, databases and other important are encrypted

What guarantees do we give to you?

You can send 3 of your encrypted files and we decrypt it for free.

You must follow these steps To decrypt your files :

1) Write on our e-mail : [REDACTED] ( In case of no answer in 24 hours check your spam folder or write us to this e-mail: [REDACTED])

2) Obtain Bitcoin (You have to pay for decryption in Bitcoins.

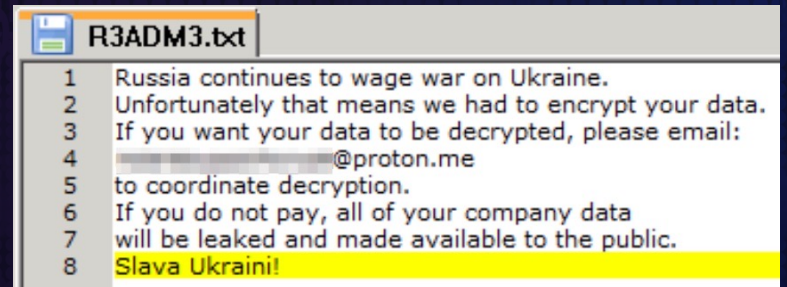
After payment we will send you the tool that will decrypt all your files.)



# Additional Threat Actor Trends

Q3 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:

- Lockbit continues to increase their operations across all industry verticals and countries.
  - During Q3, they maintained a 42% share of all publicly posted ransomware victims, increasing from 211 claimed victims in Q2 to 235 claimed victims in Q3.
- There were several notable rate increases for the following groups:
  - Hive increased their number of public victims by 104% from Q2 to Q3.
  - Blackbasta increased their number of public victims by 32% from Q2 to Q3.
- Similarly, some groups that were very active became less active as we analyzed rates from Q2 to Q3:
  - Vice Society had a 48% drop in claimed victims from Q2 to Q3.
    - However, the group claimed the Los Angeles Unified School District as a victim during September 2022.
  - Quantum had a 57% drop in their public claimed victims from Q2 to Q3.
- Q3 matched the rate of Q2 for newly observed groups.
  - Q2 and Q3 both produced eight new ransomware groups.
  - With the close of Q3, September 2022 became the 21st month in a row since January 2021 without a new ransomware group emerging to conduct double-extortion operations.
- As initially reported by @vxunderground, an unknown individual or groups is beginning to target Russian companies with ransomware and is alleging that the major motivation for targeting is because “Russia continues to wage war on Ukraine.”



A screenshot of a ransomware note titled "R3ADM3.txt". The text is as follows:

```
1 Russia continues to wage war on Ukraine.
2 Unfortunately that means we had to encrypt your data.
3 If you want your data to be decrypted, please email:
4 [redacted]@proton.me
5 to coordinate decryption.
6 If you do not pay, all of your company data
7 will be leaked and made available to the public.
8 Slava Ukraini!
```





# Quarterly Wrap Up

The third quarter of 2022 continues the trend of ransomware's dominance in the threat landscape. Across all industry verticals and countries, ransomware continues to demonstrate its ability to claim victims and pursue destructive double extortion methodologies that remain effective despite the blue team's sustained efforts to improve cybersecurity from proactive and reactive perspectives.

Q3 saw a slight slowdown in ransomware activity. However, as we enter Q4, many industries are ramping up operations for holiday seasons, especially in western countries, that is likely to bring increased targeting from prolific ransomware groups such as Lockbit, Hive, Blackbasta, and others whose goal is to financially profit from the victims they claim.

As Q4 begins, GRIT will continue to monitor for new ransomware groups and trends and highlight the changes to the ransomware threat landscape with hopes that the increased awareness will directly translate to improved defenses. With increased awareness, blue teams can focus their efforts on proactively improving their security postures, implementing core cybersecurity concepts, and ensuring that, in the event of a ransomware attack, they stand ready to respond effectively.

Ransomware continues to be a serious threat month after month, however, as a community, if we can share intelligence to collectively improve our defenses, disrupting ransomware operations on a larger scale is not out of the question.