The State of Ransomware Attacks in 2024

### CS445

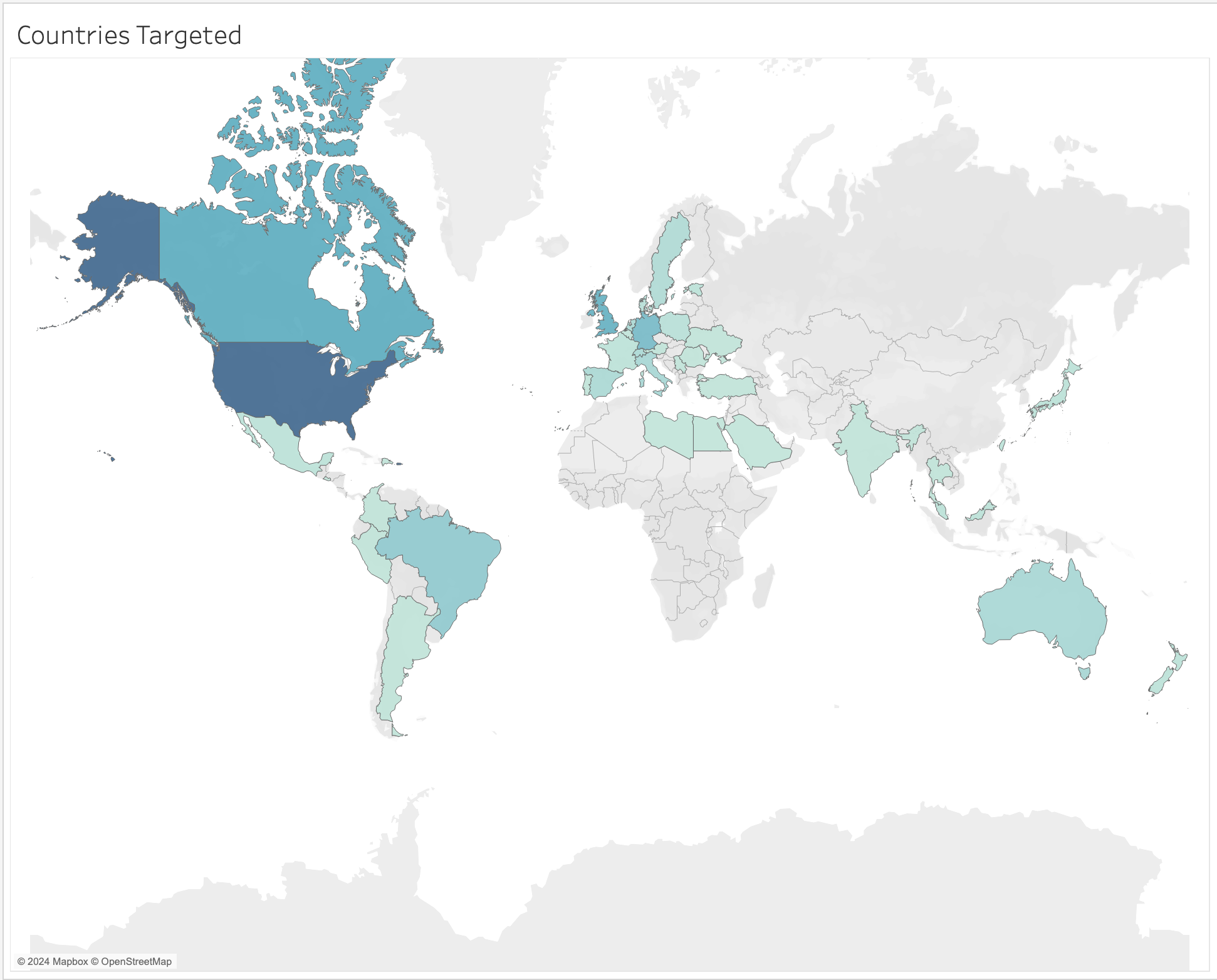
### Team 6:

#### Lim Wei Jie, Bryan Sia, Javier Tang, Dhruv Benegal

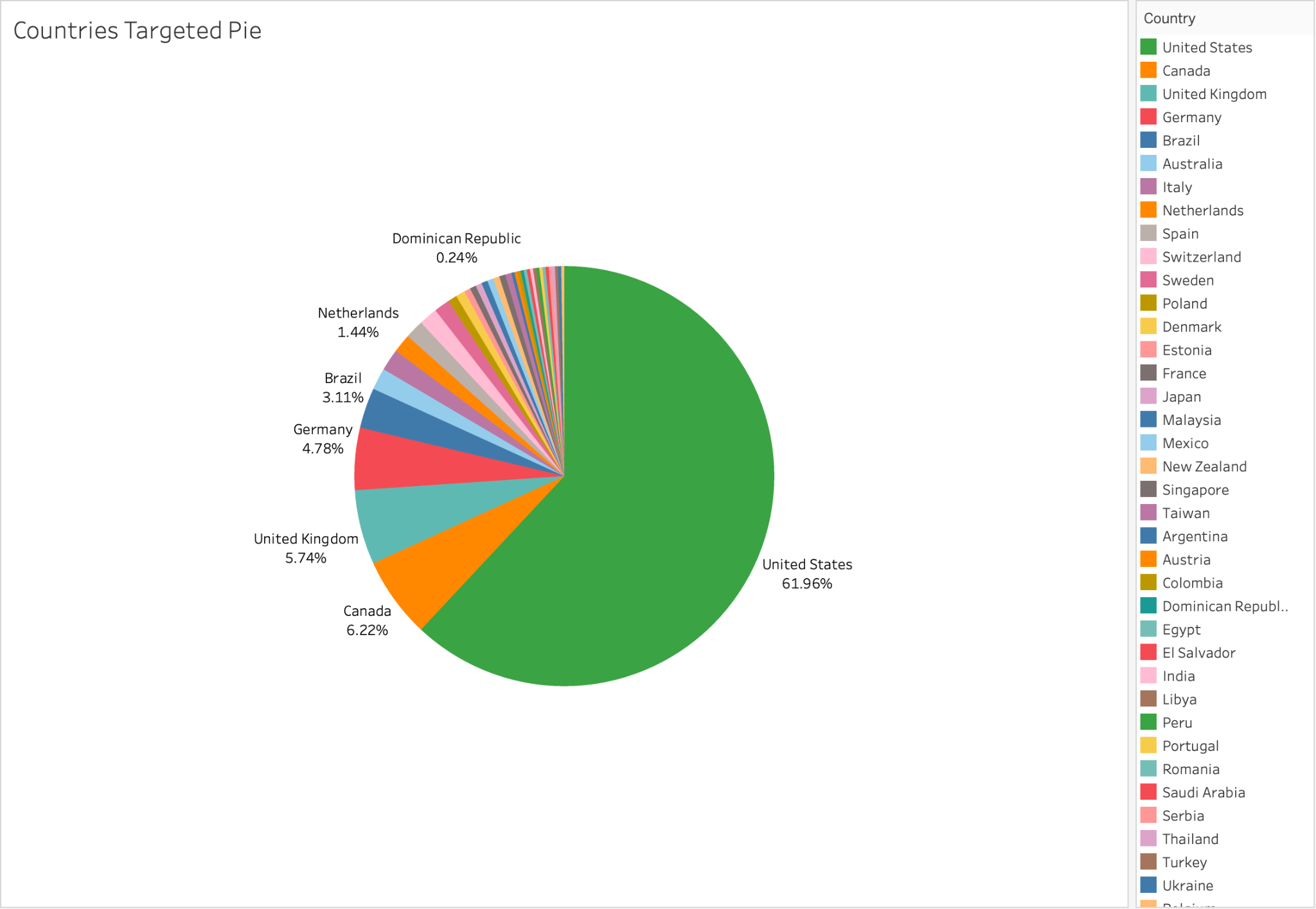
### Date:

24 October 2024

### **1. What is the % breakdown in Countries Targeted Globally?**



The map above shows the extent to which ransomware attacks are distributed worldwide. The darker colours indicate a greater number of attacks targeted at that specific region.



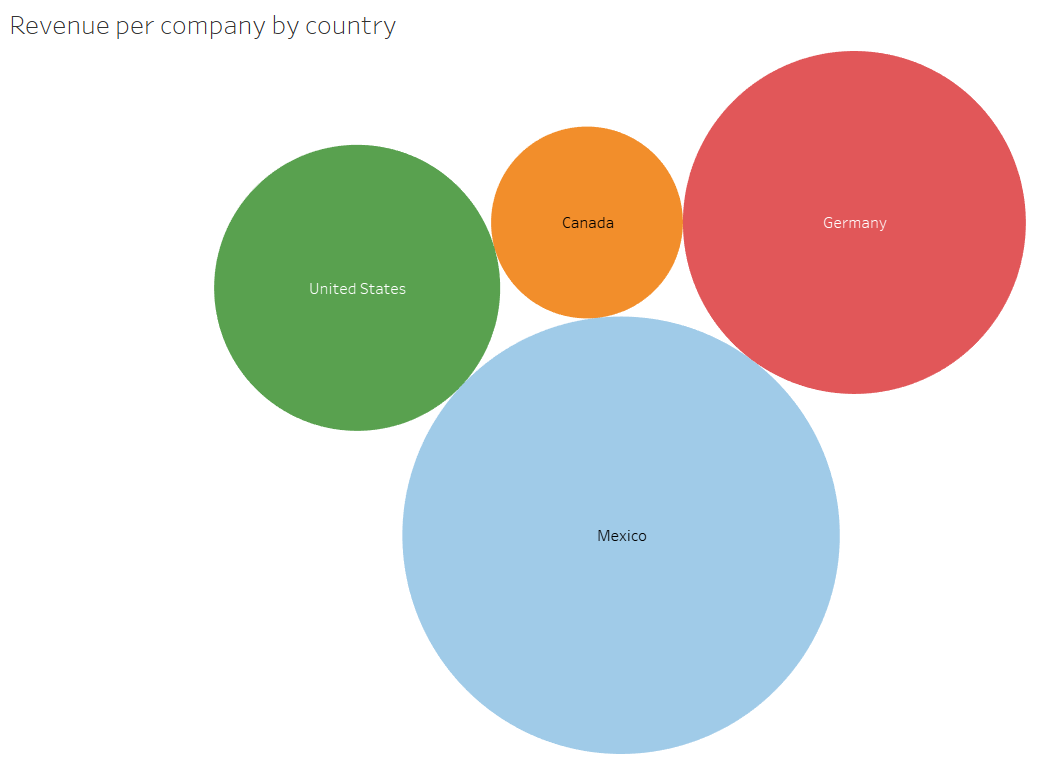
By analysing the pie chart above, we can see that the majority of the ransomware attacks were targeted at the United States of America, making up 61.9% of the total attacks monitored. This was followed by Canada, making up 6.22%, the United Kingdom, with 5.74%, Germany, with 4.78%, and Brazil, with 3.11%.

Although the coverage of the attacks on the map indicated 38 countries being targeted, we can infer that most groups favour targeting certain countries over others. This was further proven in a recent report in 2023 where the United States of America accounts for 65% of cyber attacks. Similarly, the report also shows countries have similar percentages from our finding, despite our sample size ([Blackberry Report 2023](https://blogs.blackberry.com/en/2023/02/top-10-countries-most-targeted-by-cyberattacks-2023-report))

### **2. Why are some countries more targeted than others?**

Our hypothesis is that the U.S. is targeted more frequently due to its sheer size, with more organisations increasing the likelihood of attacks. We believe gangs are primarily financially motivated, not targeting specific countries for other reasons.

Research supports this: since the emergence of ransomware, ransom payments have more than doubled, reaching around $1.5M by 2023 ([International ransomware gangs are evolving their techniques. The next generation of hackers will target weaknesses in cryptocurrencies](https://theconversation.com/international-ransomware-gangs-are-evolving-their-techniques-the-next-generation-of-hackers-will-target-weaknesses-in-cryptocurrencies-211233#:~:text=We%20can%20distinguish%20the%20degree%20to%20which%20ransomware,ransom%2C%20and%20the%20presence%20of%20money%20laundering%20services.)). Gangs now facilitate payments, build trust with organisations, and offer money laundering services. Off-the-shelf ransomware like Clop has lowered the barrier-to-entry for criminals without IT skills, while double extortion tactics have increased financial gains, allowing criminals to demand ransom for decryption keys and to prevent publication of data. The chart below shows the average revenue of companies by country, as gathered by our data.

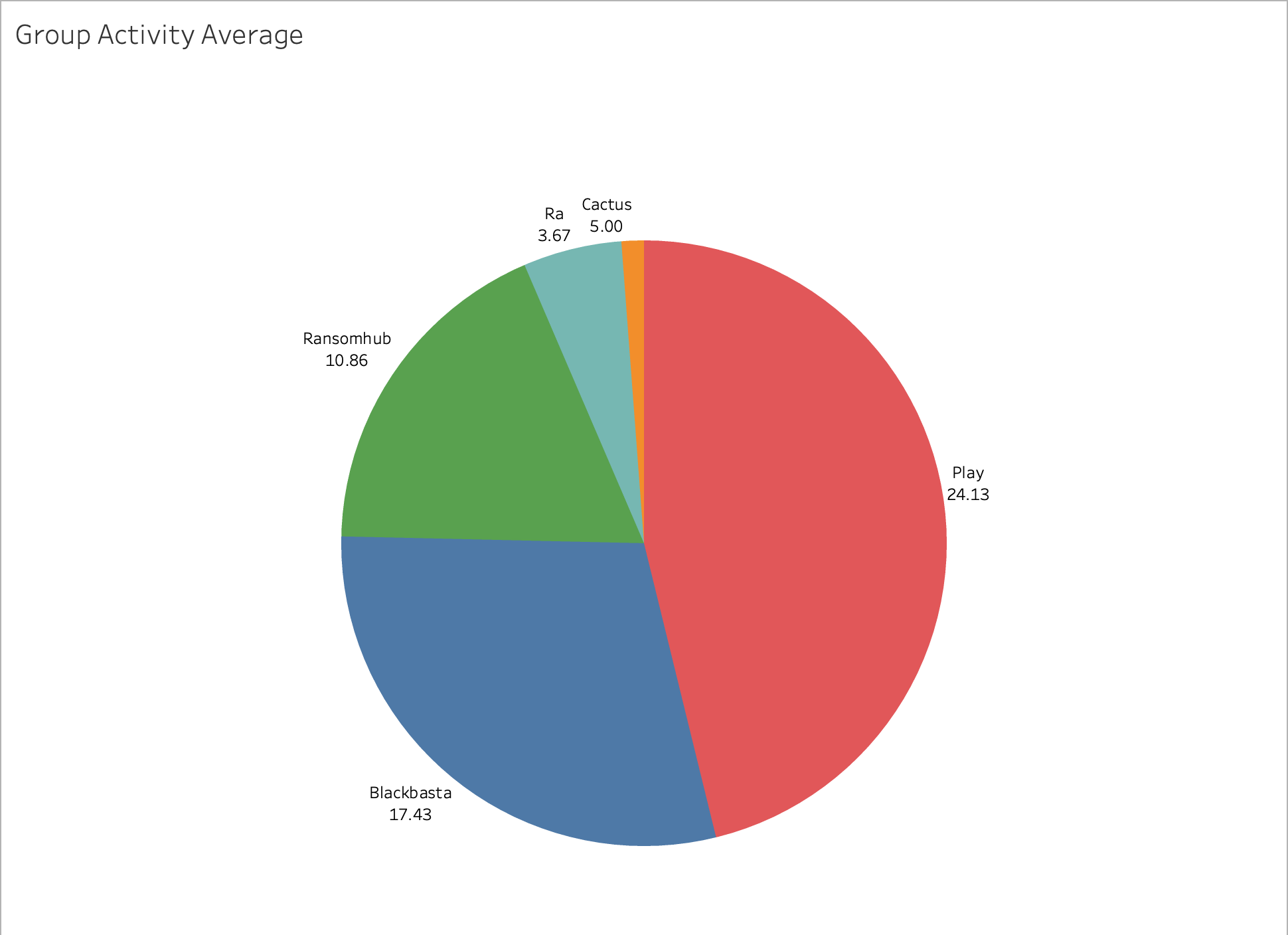
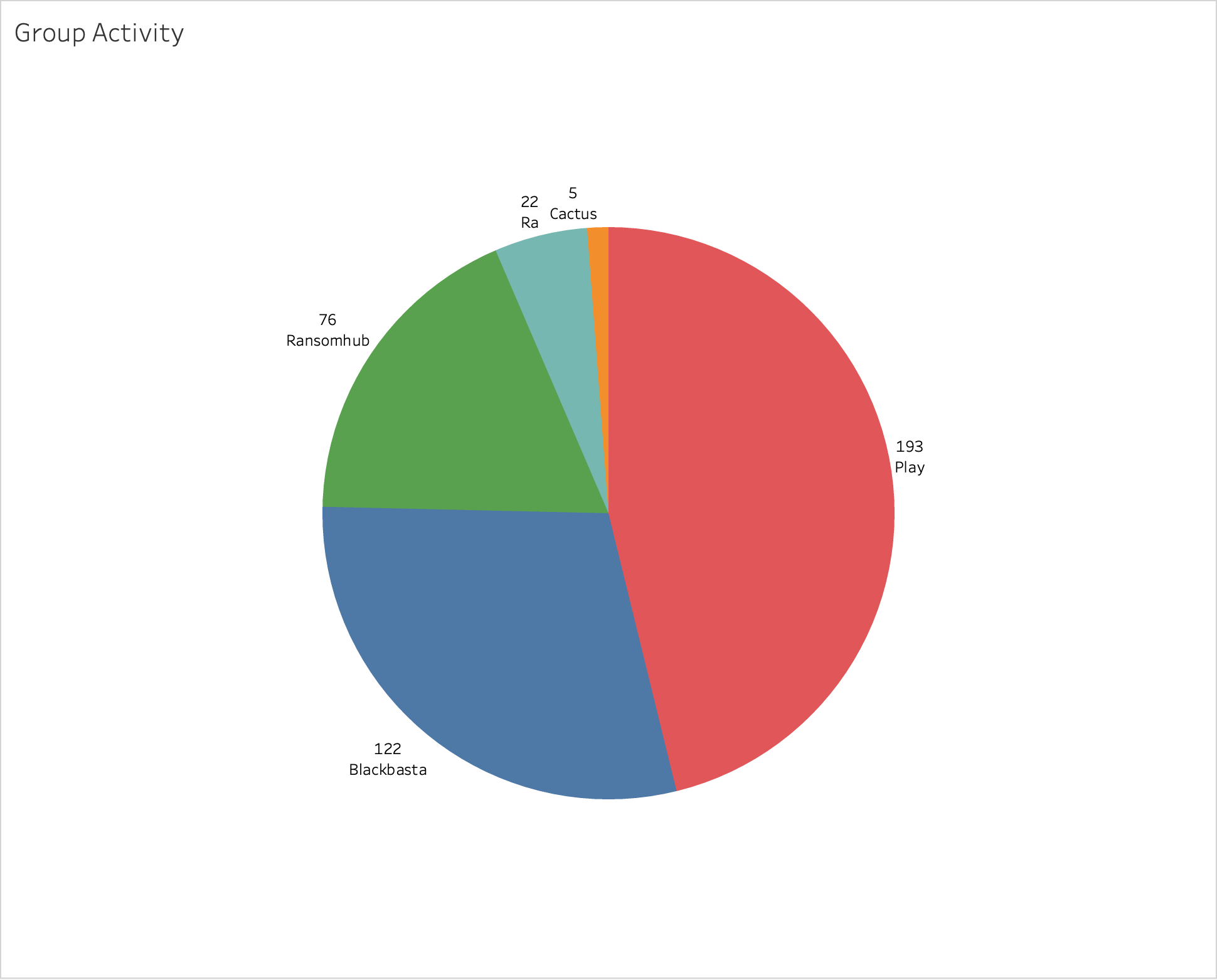


The chart shows that companies in the US have the fourth highest average revenue. This statistic supports our hypothesis that gangs are financially motivated and hence target countries that are among the richest, which is the US in this case.

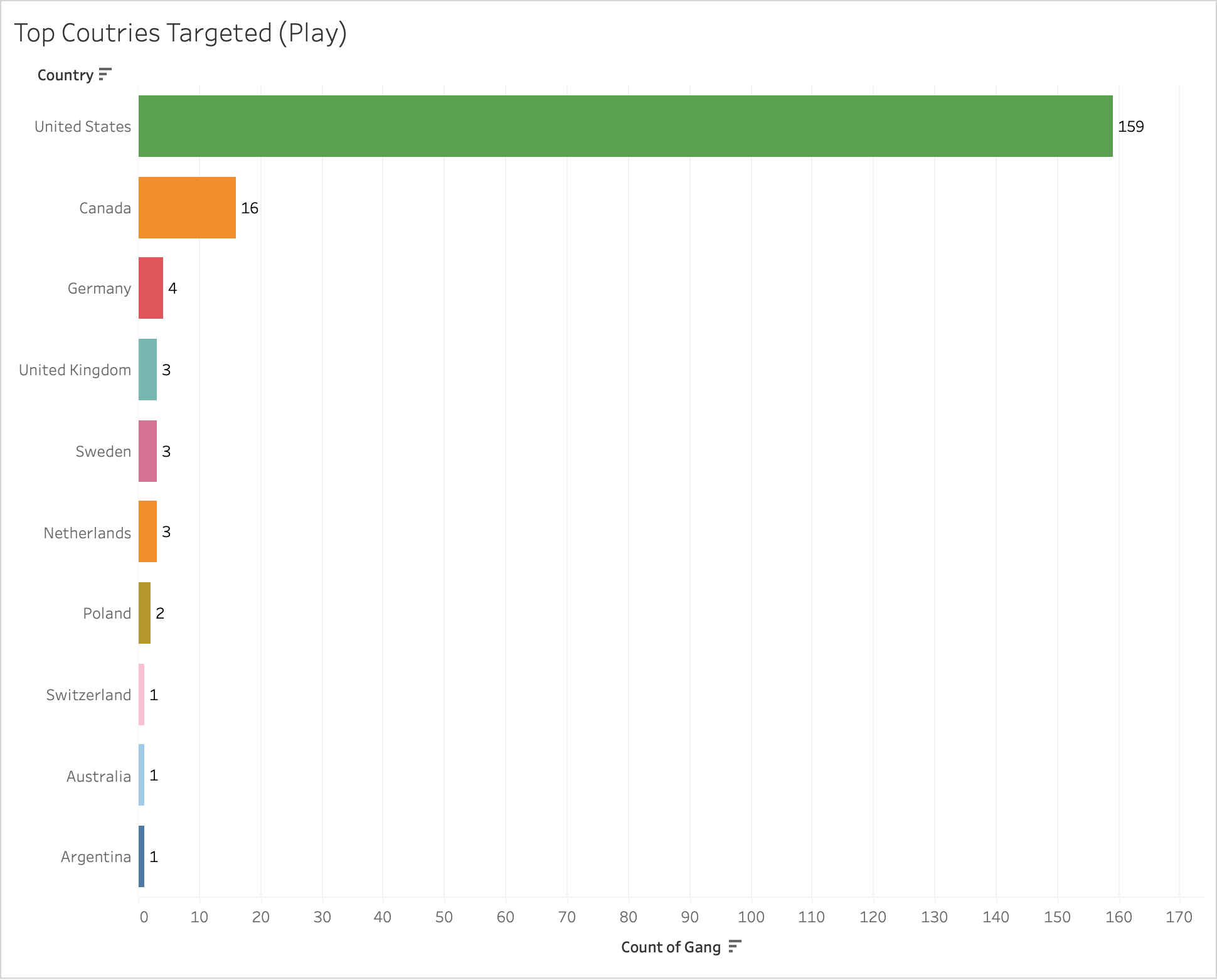
However, we also note that the revenue statistics were skewed because only the Cactus ransomware group had revenue data provided, so the chart reflects "revenue per company" only for their victims. In spite of this, we still lend some credence to this data due to our hypothesis that ransomware gangs, including but not limited to Cactus, do not target one country over another for reasons other than financial gains. Furthermore, the US economy dominates multiple industries across the globe. This makes assets and data stolen from US companies attractive to ransomware gangs.

**3. Which Ransomware group is the most active? What is so unique about their TTP that makes them so “successful”?**

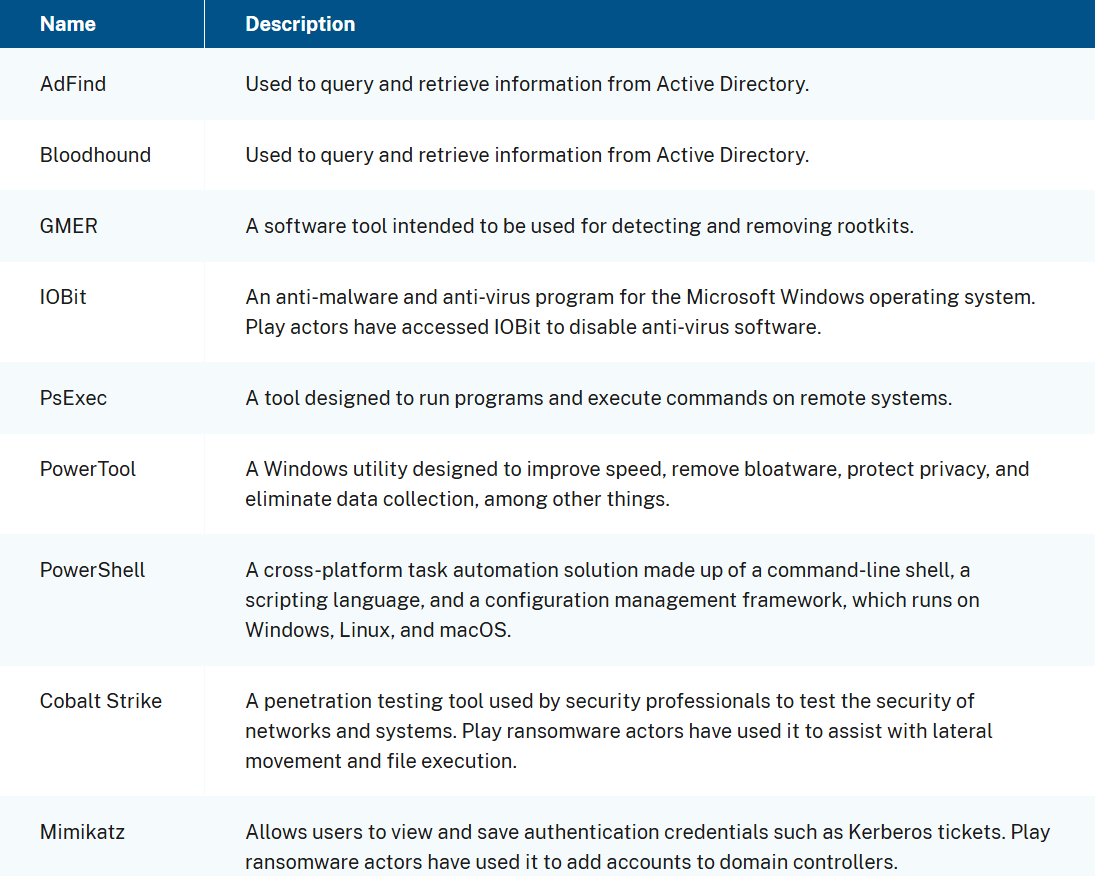
Our analysis showed that Play had conducted the most number of attacks out of all 5 gangs from January to August 2024, as shown on the left chart below. Play also had the largest average number of attacks per month, as shown on the right chart.



To find out more about what made Play so unique, we performed open-source research to better understand the TTPs of Play. Their first traces of attack originated in 2022 and targeted the Latin American region. Today, Play targets countries in other regions of the USA (of the world, in fact) as well, as shown in the chart below. This suggests that Play is primarily financially motivated, as most ransomware gangs are.

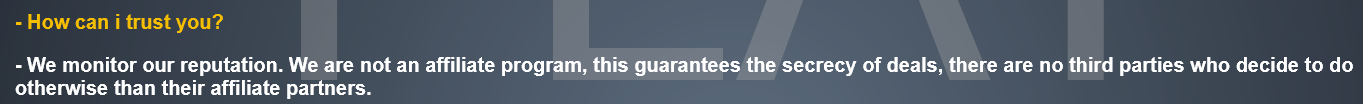


Play has been known to target exposed RDP servers and Fortinet FortiOS VPNs. Once in the system, they’ve been observed using commercial tools like PowerTool to disable the antivirus and delete log files with tools like AdFind to perform AD reconnaissance. They also use popular tools like Cobalt Strike, Mimikatz and LOLBins (living-off-the-land binaries) like psexec to perform lateral privilege escalation. The table below is an incomplete list of the tools that Play frequently uses. It should be noted that most of these tools are commonly employed by ransomware gangs other than Play.

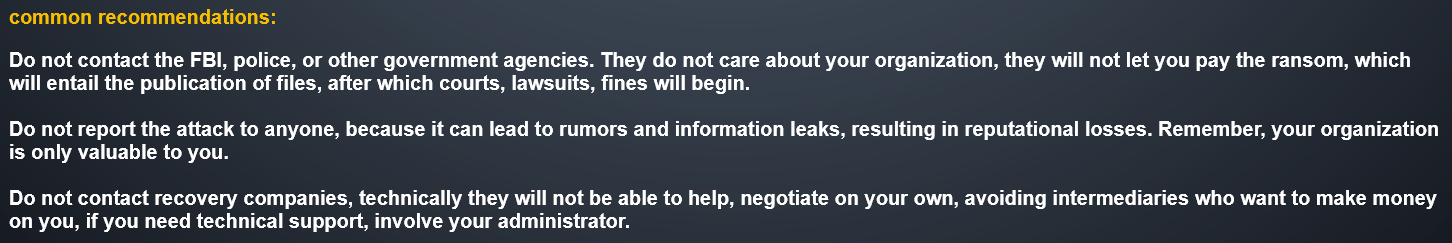


*Source:* [*#StopRansomware: Play Ransomware | CISA*](https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a)

Upon entering the system, Play employs a double extortion strategy where compromised data is split into compressed segments and then exfiltrated before local data is encrypted with AES-RSA hybrid encryption. Encrypted files are uniquely renamed with a ".Play" extension, hence giving rise to the group’s name. They threaten to release the stolen data if the ransom isn't paid within a set time. To pressure victims, Play often leaks portions of the data as a” proof of work”, increasing urgency. Instead of a fixed ransom demand, Play instructs victims to email them to negotiate, claiming this ensures confidentiality. The double extortion strategy is quite uncommon as it is more sophisticated, requiring attackers to take the extra step of exfiltrating the data stealthily prior to encryption.



In the first sentence of the gang’s DLS’ FAQ page, Play claims to value its reputation and guarantees confidentiality as a closed group with no third-party affiliations. This may win the trust of sceptical organisations, but is also cunning as direct communication with Play allows them to manipulate negotiations and adjust ransom prices based on the victim's response.



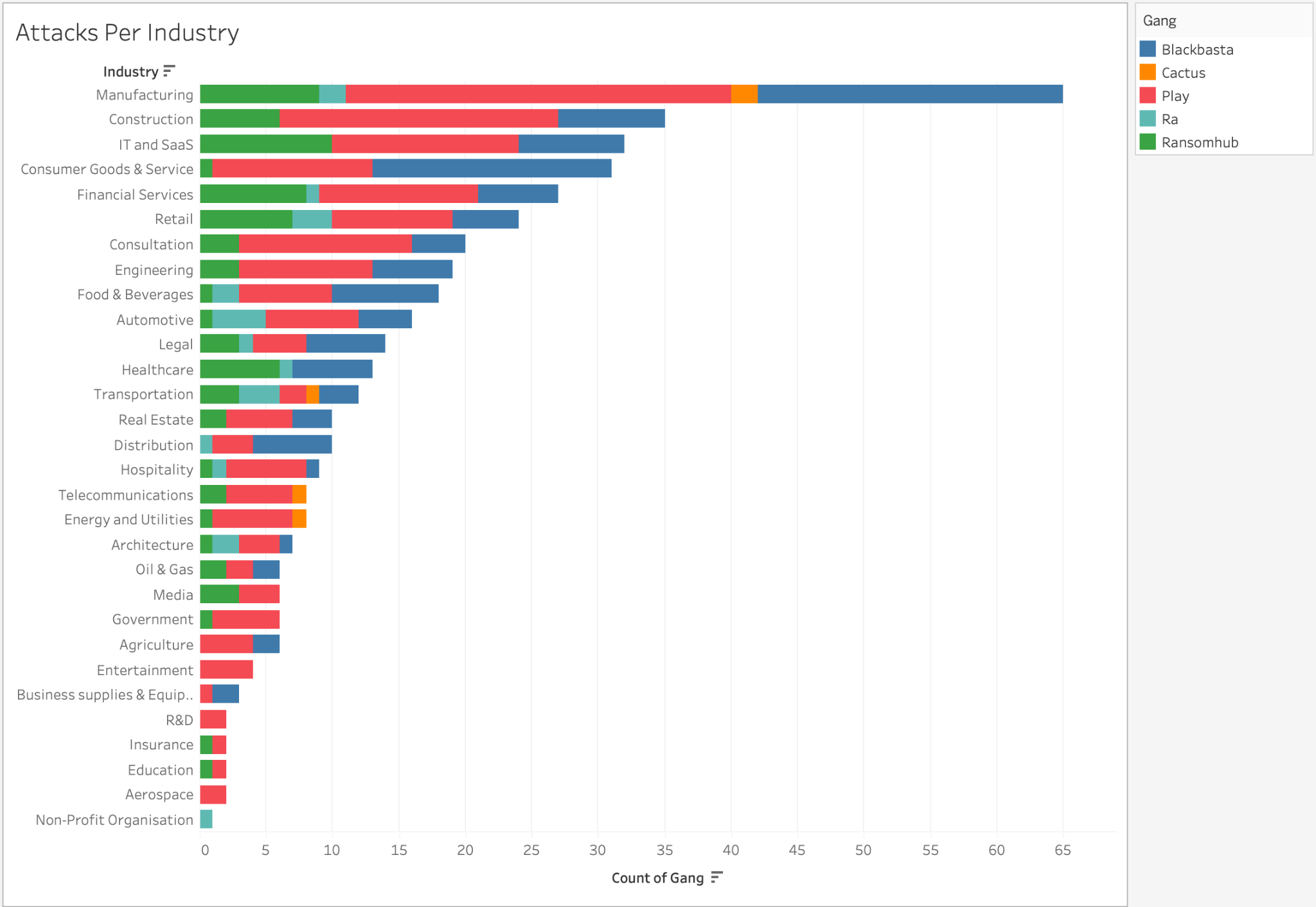
These statements display attempts to make the group seem reasonable, increasing the likelihood that organisations will pay the ransom.

Play also uses intermittent encryption to encrypt compromised files. It is a new encryption technique that encrypts only part of each file, making them unusable while avoiding detection by security tools. The process is also very fast, allowing them to exfiltrate large amounts of data and evade detection by most malware detection systems.

In summary, we found that while Play uses commonly available tools, their use of intermittent encryption has allowed them to elude many security systems, contributing majorly to the success of their many attacks. Their closed group nature attempts to win the trust of organisations and makes them more willing to pay the ransom. Lastly, they set a firm stance, giving strict deadlines and instructions to follow and possibly manipulate negotiations to their advantage via email.

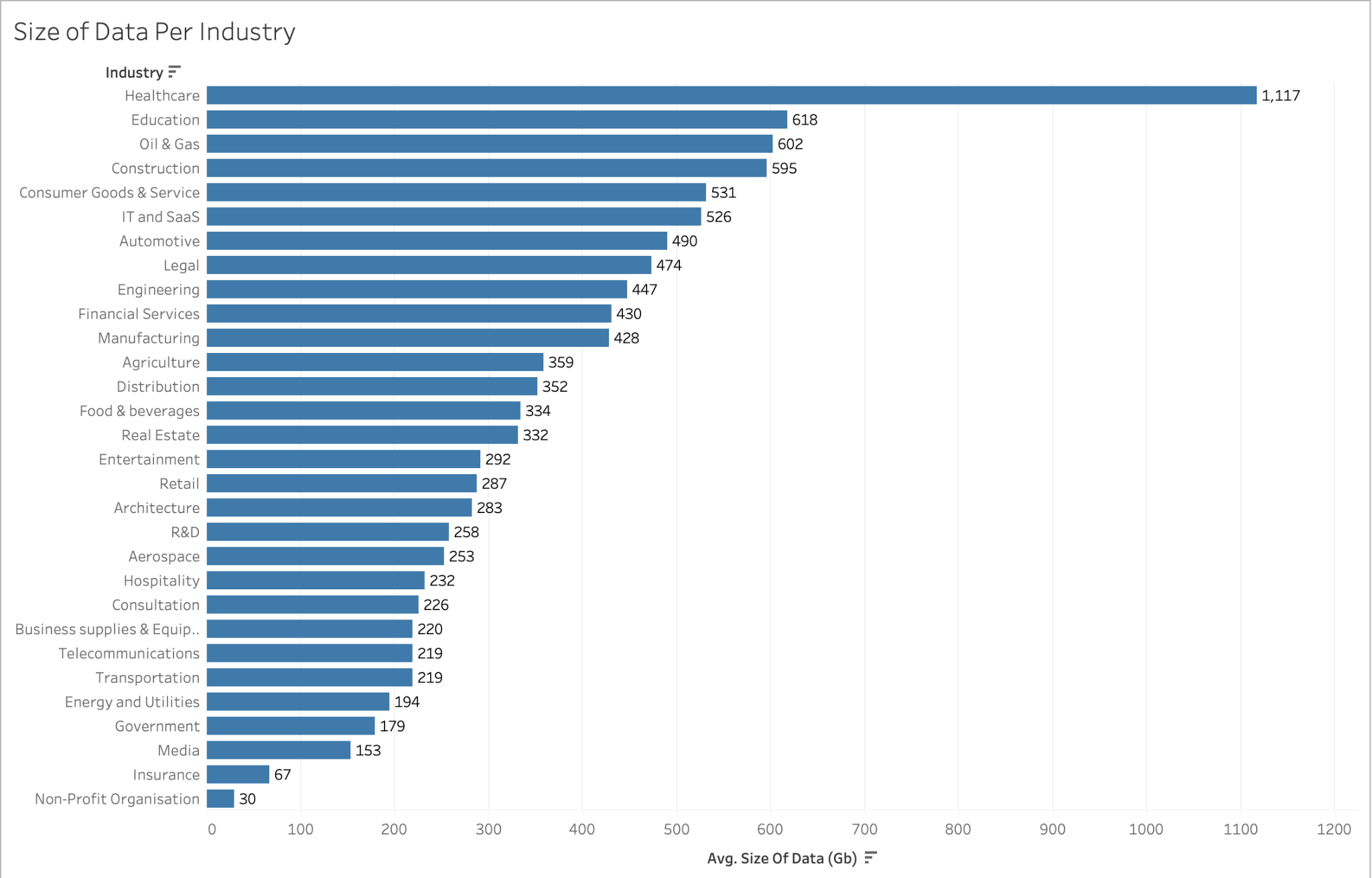
### **4. Which Industries Are More Prone To Ransomware Threats? Why?**

Our statistics show that the Manufacturing and Construction industries to be more targeted by ransomware gangs than other industries.



A GlobalData report shows that between April 2023 and Match 2024, the Manufacturing and Construction sectors are among the top most targeted sectors, with the Construction sector being the third most targeted ([MEED | Construction is the third most targeted sector by ransomware](https://www.meed.com/ransomware-targets-construction-companies)). This roughly correlates with our findings, as shown in the chart above.

Next, we looked at the size of data exfiltrated across the industries.



Since the average size of data exfiltrated from companies in the manufacturing sector is not one of the highest, it suggests that gangs don’t necessarily target the manufacturing sector for the quantity of data they expect to exfiltrate either.

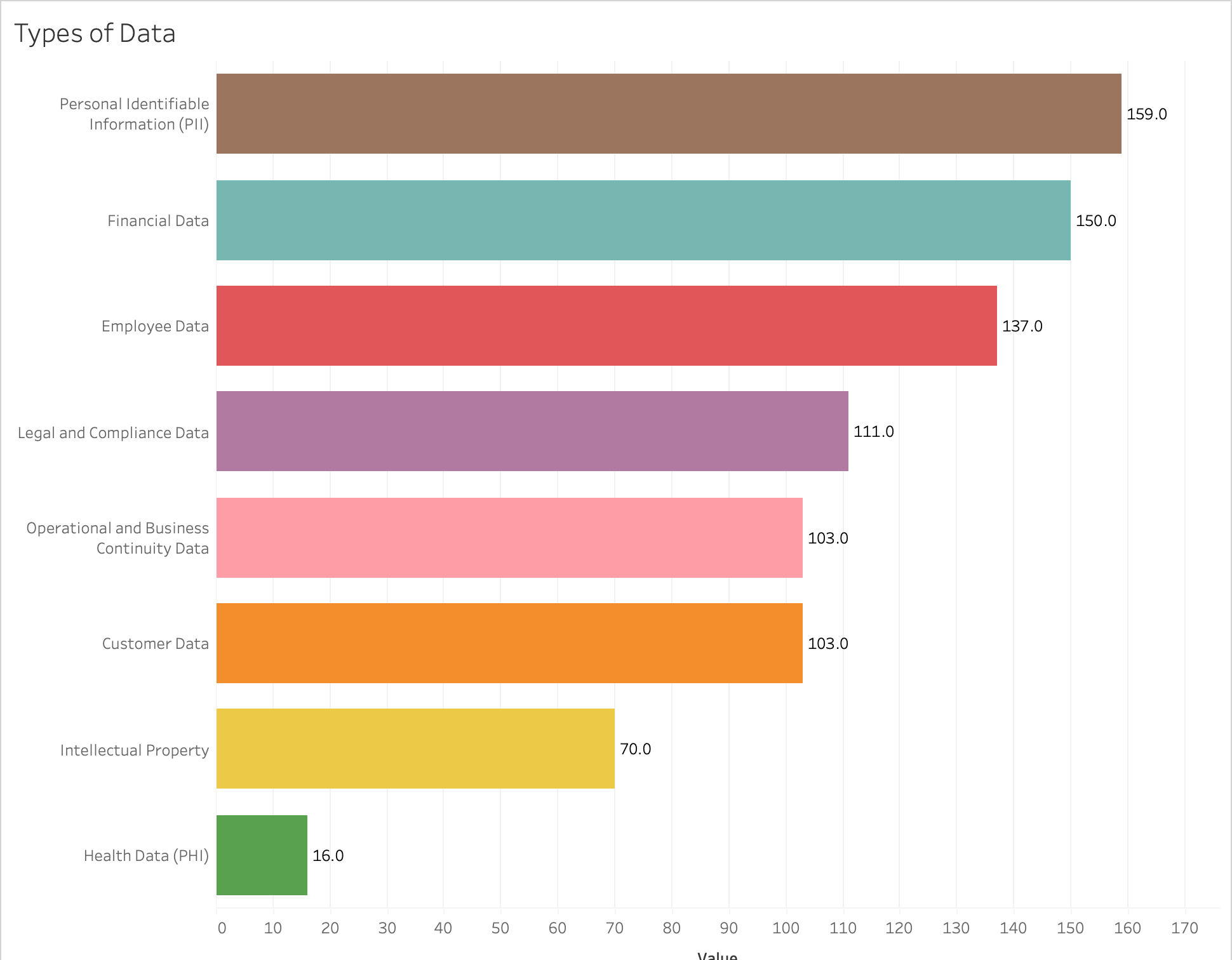
However, the thought occurred to us that larger data size does not equate to data that is of higher value. So we hypothesised that companies in the manufacturing and construction sectors are easier targets for hackers, potentially due to their reliance on outdated technologies.

Research has shown that replacing outdated machinery can be costly and unsustainable. Many companies hence resort to retrofitting machinery with new hardware and software capabilities for performing their goals, gathering and analysing data ([Industry 4.0: a systematic review of legacy manufacturing system digital retrofitting | Manufacturing Review](https://mfr.edp-open.org/articles/mfreview/full_html/2022/01/mfreview220051/mfreview220051.html)). However, different systems may integrate poorly due to high complexity and diversity of protocols and vendors. This is especially true for SMEs, which have lower levels of digital maturity, as the research also shows. This may leave them more vulnerable to cyber-attacks.

Additionally, many organisations are unprepared to migrate their data to the cloud in light of the upcoming Fourth Industrial Revolution. Research by Basis Technologies supports this. It reveals that about 43% of companies that use SAP’s ECC, a popular ERP software, are unprepared for migration to S/4HANA, which is SAP’s modern cloud-based ERP system ([The True State of S/4HANA in 2024 - Basis Technologies](https://www.basistechnologies.com/blog/the-true-state-of-s4hana)). SAP is a tech giant that boasts more than 230 million cloud users across the globe and provides numerous solutions for businesses. Their solutions are widely used by many organisations in the manufacturing industry. Hence, this unpreparedness for migration highlights the key concern, which is that the use of legacy systems is quite rife and leaves numerous organisations exposed to cyber threats.

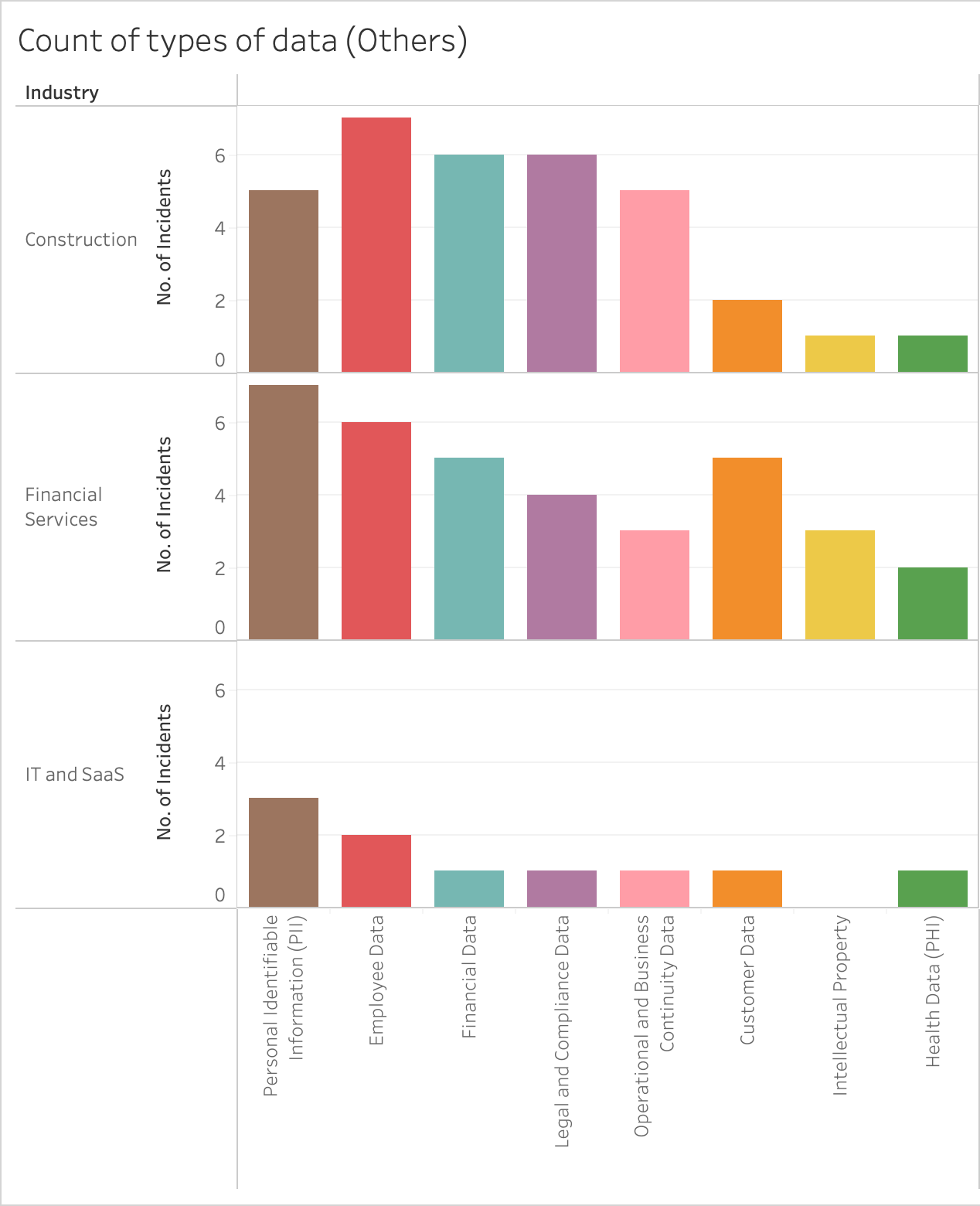
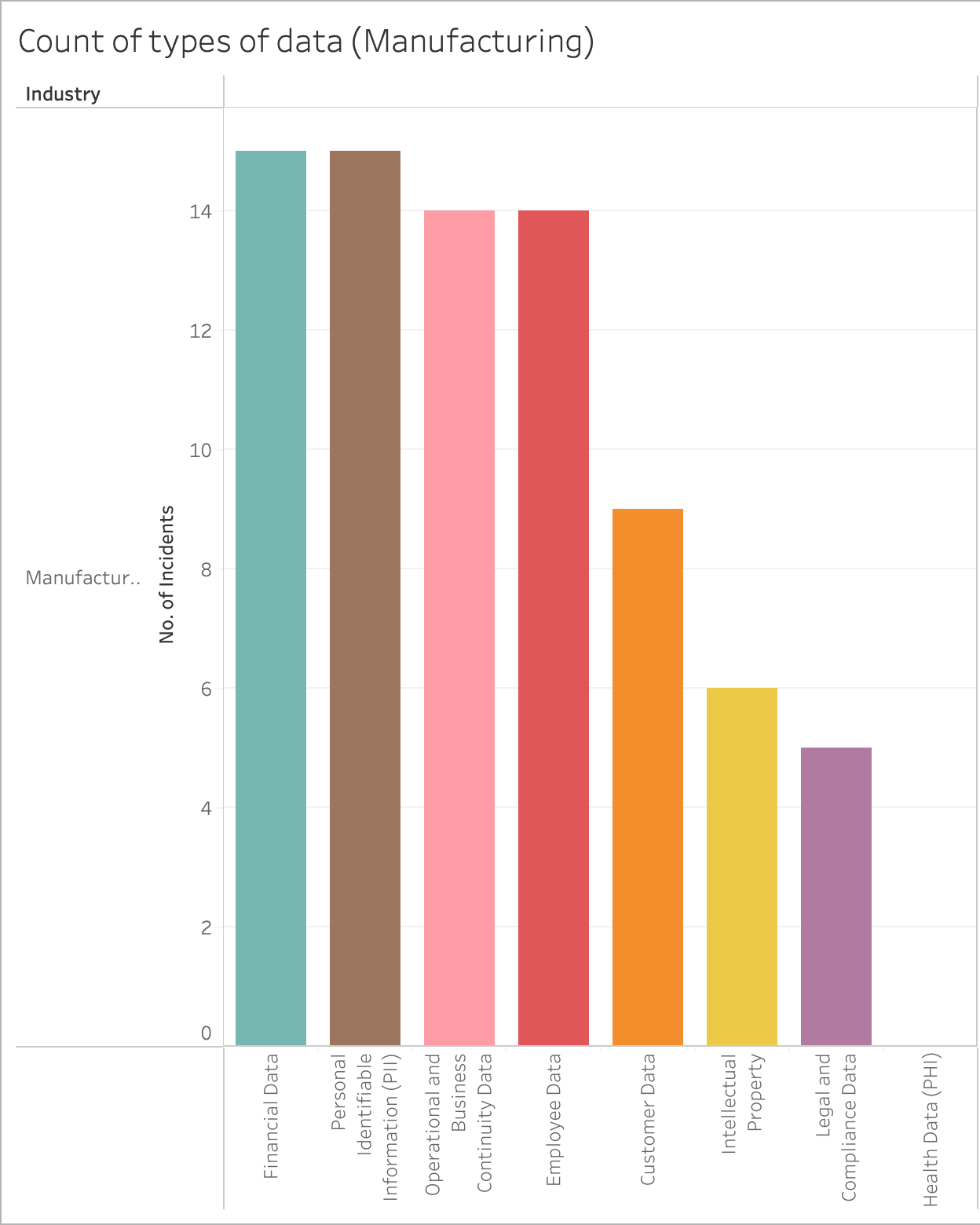
### **5. We know actors target sensitive data, but what kind of data do actors usually target? What are the kinds of data targeted in each industry? Show a breakdown comparing types of data stolen.**

The chart below shows a breakdown of the types of data stolen by ransomware gangs globally. It should be noted that multiple types of data can be stolen in a single incident. As such, the sum of the numbers does not represent the total number of incidents.



Appendix 1.1

PIIs, Financial Data and Employee data are shown to be most commonly exfiltrated by ransomware gangs. Next, we narrowed down our statistics to the specific industries.



The left chart represents the distribution of exfiltrated data types in the manufacturing sector, which has seen the most number of attacks. The right one shows similar distributions across a few other industries.

We see that generally, across all industries, PIIs, employee data and company financial data are among the most widely exfiltrated types of data. This suggests that the manufacturing sector does not stand out in terms of a particular type of data being more targeted than others.

However, we analysed that even though PIIs are commonly found in breached databases, the quantity of PIIs stored differs across industries. In the healthcare industry, for example, a larger volume of PIIs would likely be compromised in an attack as databases contain the PIIs of tens of thousands of patients whereas in other industries like the manufacturing industry, only the PIIs of its employees (much smaller in number) would be compromised. This is supported by the size of data per industry chart shown previously, which highlights that healthcare companies experience the largest average data exfiltration size, significantly surpassing the second-largest sector, Oil & Gas.

As for the Financial Services sector, the high number of Customer data being exfiltrated is within our expectations since we expect them to be dealing with numerous customer data in their daily operations. One observation, however, that seems to differ from our initial thought is that there is no Intellectual Property data being exfiltrated in the IT and SaaS industry. Given that these IPs are their bread and butter to their company existence, we suspect that most attackers will be eyeing for that. One possibility that we concluded could be the reason is that due to its highly confidential nature, this data is separated and held in an “air gap” network, hence making it difficult for attackers to be able to infiltrate these highly secured areas.

### **6. Share 3 interesting insights you observed.**

* While skimming through the DLS site for Ransomhub, we noticed certain leaks where the ransomware group attempts to address the clients of the targeted company. In these situations, it was noted that they were trying to unmask the “true nature” of these companies and how people shouldn’t provide their personal information and trust these firms for their services. This is quite uncommon for a ransomware group since they are majorly driven by financial gain and normally wouldn’t care as long as the ransom was timely fulfilled. (refer to Appendix 2.1)
* For Blackbasta, we noticed a section on their DLS webpage where they had posted an interest in recruiting individuals that had knowledge about specific zero-days attacks that they can leverage from. However, it is weird to post a recruitment on a shaming website that exposes company data. This led us to believe that they intend to recruit/contact security researchers that view their shaming website that wanna join the dark side (refer to Appendix 2.2).
* We also noticed that the posts on a gang’s PR page don’t provide a full picture of ransomware incidents. These posts typically show a deadline or “Published” status if data has been leaked. However, companies that pay the ransom often have their posts removed, and many choose not to disclose payment to avoid embarrassment and damage to their reputation. As a result, the true number of organisations targeted by gangs is often unclear through scraping at a single instance, making it difficult to track how many choose to pay the ransom. This statistic, crucial for understanding how different gangs’ tactics influence payment decisions, is hard to obtain and would require prolonged monitoring of the shaming sites for which we did not have the time and resources for.

### **7. Share lessons learnt, what were your struggles in executing the project and how did you overcome them?**

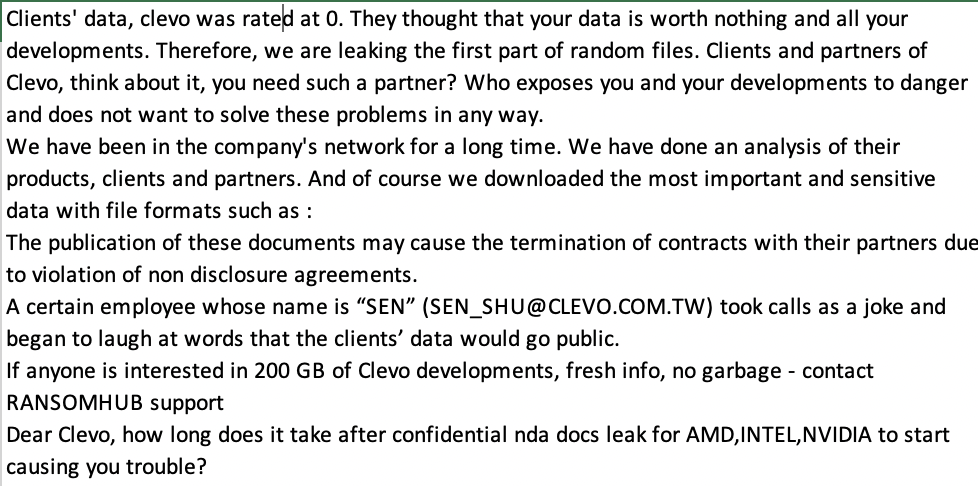
During our attempt to source top ransomware sites for the project, we faced challenges because several popular sites lacked the necessary data points on their landing pages, and some notorious groups, like Lockbit, had their onion sites taken down during our scraping process. To overcome this, we relied on open-source research and forums to identify active gangs. For many of us, this was our first experience accessing the dark web and configuring a secure sandbox environment took longer than expected, especially when running Tor proxies. Initially, we tried using Tor on a VM but encountered issues with the Python environment, leading us to use the browser on our host machines with higher safety precautions. Learning to use web scraping tools like Selenium and BeautifulSoup was challenging, but helpful videos guided us through writing scripts. These Python tools, along with data visualisation software like Tableau, will be invaluable for our future projects and work.

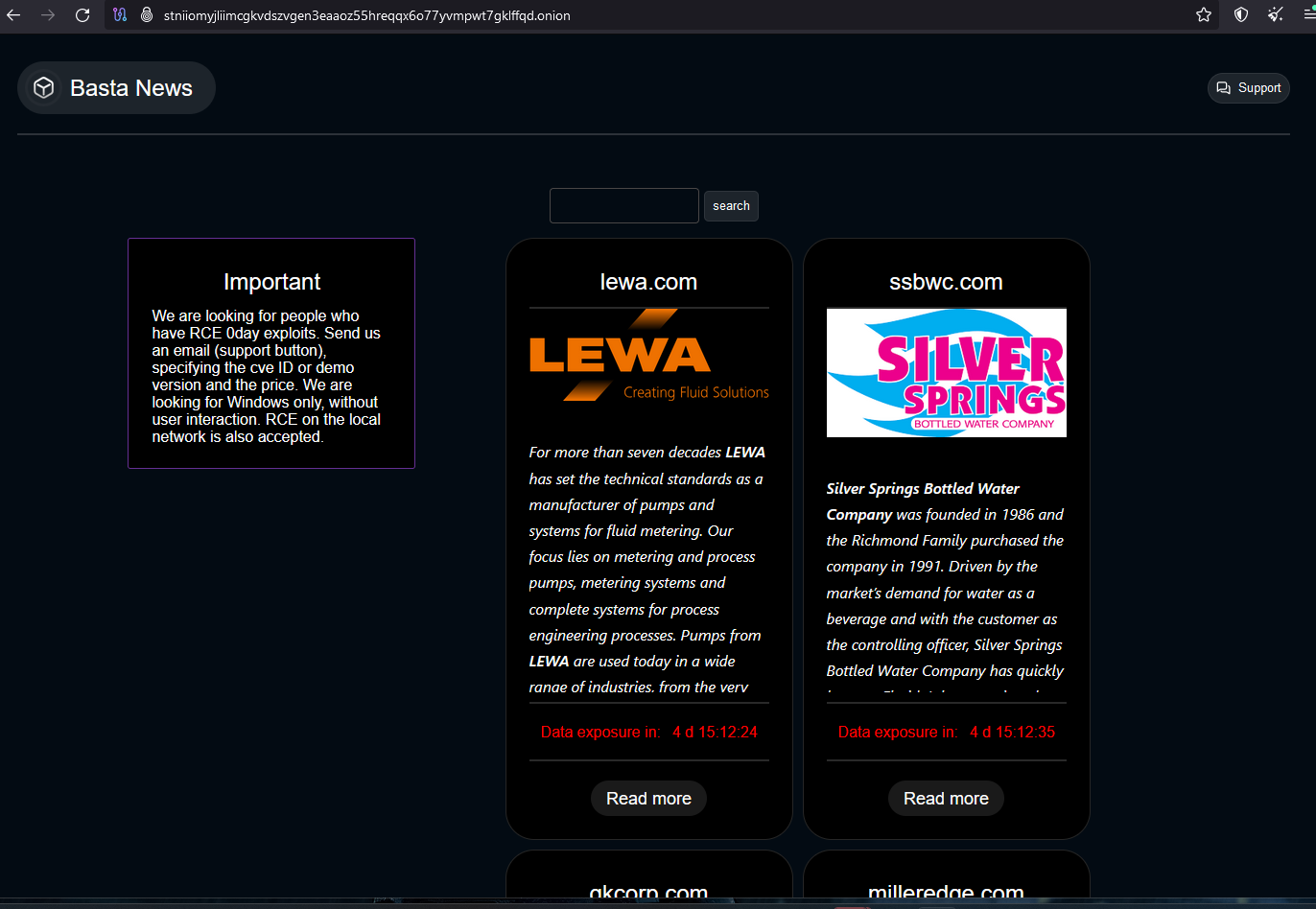
**APPENDIX:**

Table for the Data Types collected:

| **Data Types** | **Description** |
| --- | --- |
| 1) Personal identifiable Information(PII) | Name, address, social security number, email, phone number, biometrics |
| 2) Financial Data | Credit card numbers, bank account details, transaction history, tax information, income data. |
| 3) Intellectual Property | Patents, trademarks, copyrights, trade secrets, designs, research data. |
| 4) Customer Data | Contact information, purchase history, preferences, feedback, demographics. |
| 5) Employee Data | Personal details, job titles, salaries, performance reviews, payroll, benefits, background checks. |
| 6) Legal and Compliance Data | Contracts, compliance reports, licences, regulatory filings, legal records. |
| 7) Operational and Business Continuity Data | Disaster recovery plans, internal processes, supply chain information, risk management. |
| 8) Health Data (PHI) | Medical history, insurance details, diagnoses, treatments, prescriptions, patient identifiers. |

Appendix 1.1

Appendix 2.1



Appendix 2.2