CS445: Cyber Threat Intelligence
Group Project

G1 Team 8
Carissa Lee May Kwan
Crissie Tan Kai Ning
Nicole Lim Jia Yi
Won Ying Keat

Table of Contents

Data Overview

In this report, we will be looking at four ransomware groups. They consist of Bianlian, Blackcat, Cuba and Quantum. This section will provide a brief overview of the different groups and additional information before delving into the analysis.

Background of Ransomware Groups

Bianlian

Primary Information

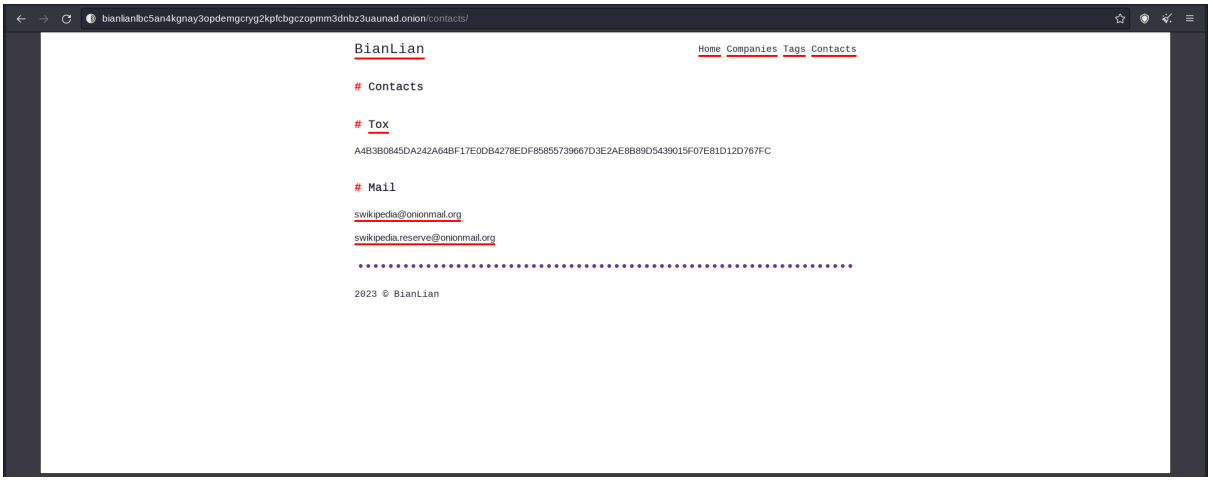


Figure 1: Screenshot of *Bianlian's* contact page

The copyright label on their Bianlian's site displays 2023, showing that the group has been actively keeping their website's details updated. From the site, their earliest post dates back to January 2021. Also, it can be observed that numerous companies' names are censored and this could possibly be due to ransom payment since these companies do not seem to have any data published on their site. Lastly, Bianlian can be contacted through email or TOX Messenger.

External Information

Discovered in late 2021, BianLian is GoLang-based ransomware that has been targeting companies in various sectors, including **healthcare and logistics**. They have been known to use double extortion tactics, in which they threaten to publish stolen data if the victim does not pay the ransom.

Blackcat

Primary Information

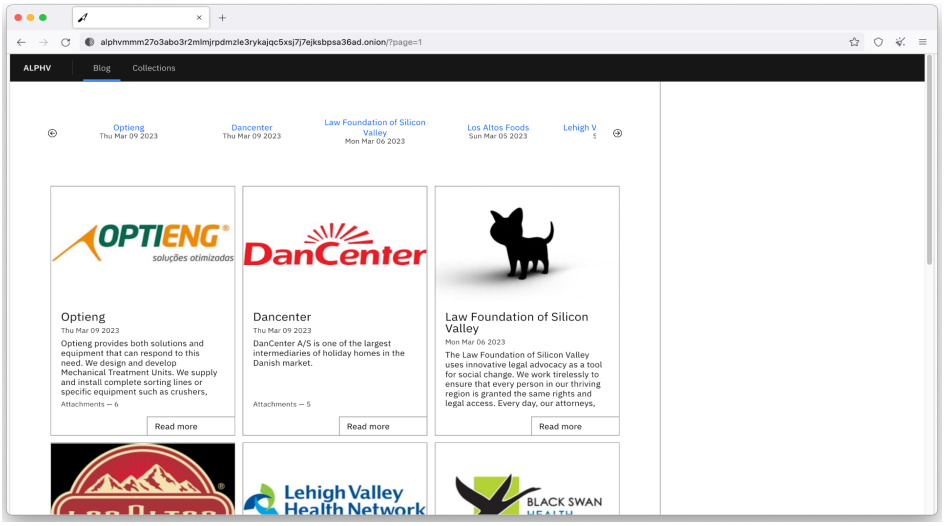


Figure 2: Screenshot of BlackCat's website showing blog posts of their latest targets

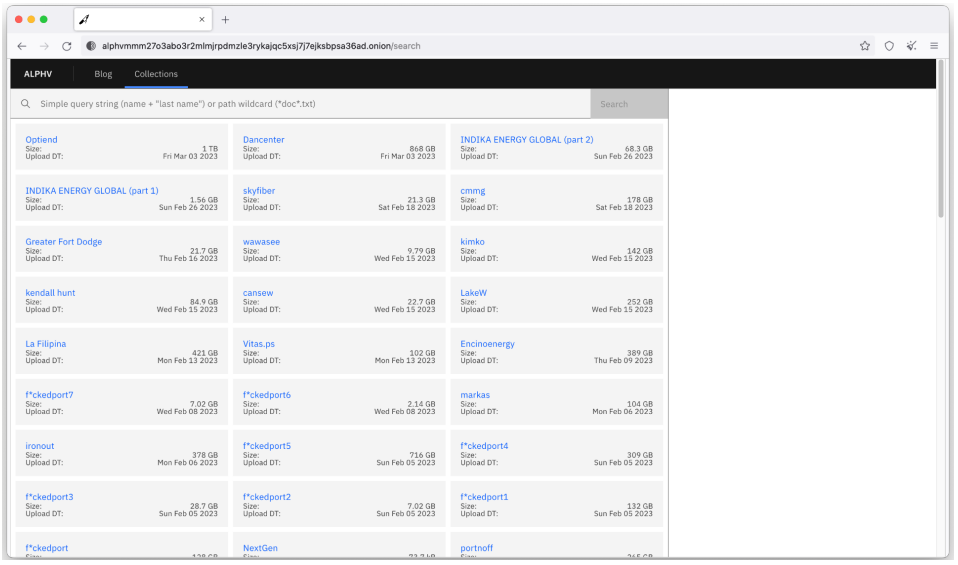


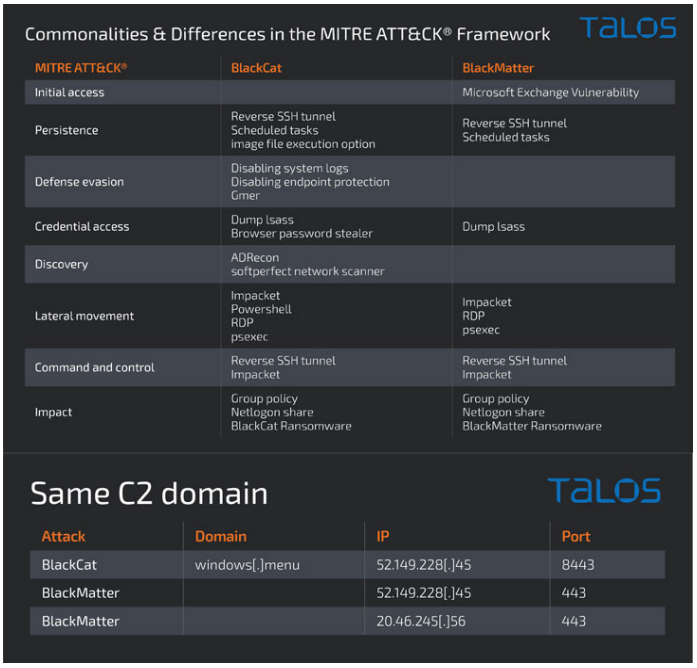
Figure 3: Screenshot of BlackCat's database containing companies with leaked data

BlackCat's site consists of a database to keep track of companies who have yet to or refuse to pay up their ransom. Information leaked about the victims include the size of leaked files and the entries creation date for each company. However, if companies have paid up their dues, BlackCat would remove the companies from the database.

External Information

Launched in November 2021, BlackCat (also known as AlphaVM, AlphaV, or ALPHV) is a professional ransomware that gained notoriety as the first major ransomware family written in Rust, a cross-platform language that allows customization of malware for different operating systems. This has made it particularly dangerous for enterprises. The ransomware has been on the news for its attacks on high-profile targets and use of **triple extortion**

(Tompkins, 2023), which includes threatening to launch DDoS attacks on victim's infrastructure in addition to exposing exfiltrated data on their searchable databases to coerce payment.



Commonalities & Differences in the MITRE ATT&CK® Framework

TALOS

MITRE ATT&CK®	BlackCat	BlackMatter
Initial access		Microsoft Exchange Vulnerability
Persistence	Reverse SSH tunnel Scheduled tasks image file execution option	Reverse SSH tunnel Scheduled tasks
Defense evasion	Disabling system logs Disabling endpoint protection Gmer	
Credential access	Dump lsass Browser password stealer	Dump lsass
Discovery	ADRecon softperfect network scanner	
Lateral movement	Impacket Powershell RDP psexec	Impacket RDP psexec
Command and control	Reverse SSH tunnel Impacket	Reverse SSH tunnel Impacket
Impact	Group policy Netlogon share BlackCat Ransomware	Group policy Netlogon share BlackMatter Ransomware

Same C2 domain

TALOS

Attack	Domain	IP	Port
BlackCat	windows[.]menu	52.149.228[.]45	8443
BlackMatter		52.149.228[.]45	443
BlackMatter		20.46.245[.]56	443

Figure 4: Evidence of similarities in TTPs between BlackCat and BlackMatter

Similarities were found within BlackCat's TTPs from the BlackCat and BlackMatter attacks - ransomware family that originated from DarkSide and were shut down in November 2021 - that suggested strong connections between the two (Abrams, 2022). Later on, in an interview with the BlackCat gang published by The Record further confirmed that they were affiliated with the BlackMatter gang (Smilyanets, 2022).

Cuba

Primary Information

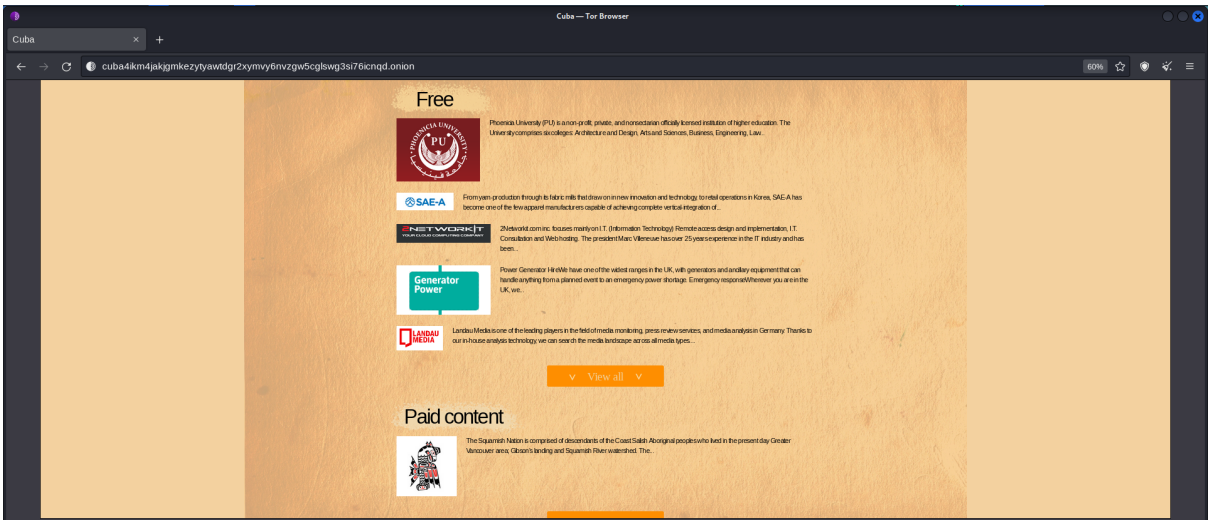


Figure 5: Screenshot of Cuba's homepage. 'View all' button is unresponsive sometimes

On Cuba's site, it offers both free and paid information of various companies. It was observed that every company posted on their website are linked to the same download link in which not all of the companies information is found inside the repository of leaked data. We believe that those companies that are shamed on the site but lack the actual leaked content could have paid Cuba the ransom to remove the data from the site.

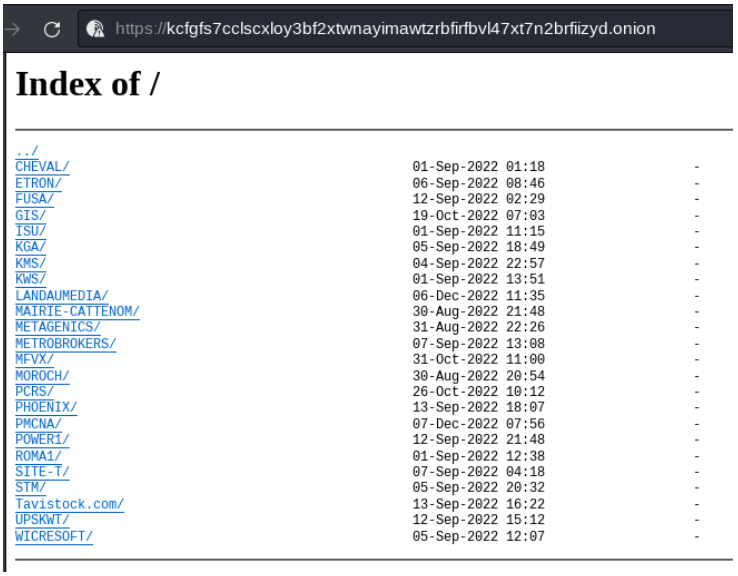


Figure 6: Screenshot of the stolen data shared after clicking on the download link

External Information

Cuba, also known as Fidel, is a ransomware group first discovered in 2019 and rose to prominence between 2021 and 2022 when they extorted **more than $60 million** in ransom payments from victims. The group mainly targets organisations who focus on financial services, government, healthcare, manufacturing and information technology. They achieved their objectives by distributing ransomware on compromised systems through *Hancitor*, a relatively unsophisticated information stealer and malware downloader, which can be disguised as a word document with malicious macro in it. This is followed by transmitting the word document via **phishing campaigns** to gain access to organisations' systems. (The BlackBerry Research & Intelligence Team, 2022)

It is suspected that Cuba originated **from Russia due to evidence showing that once it detects a Russian keyboard layout or language from the victims' environment it will terminate** (*Ransomware Spotlight: Cuba - Security News*, 2022).

Quantum

Primary Information

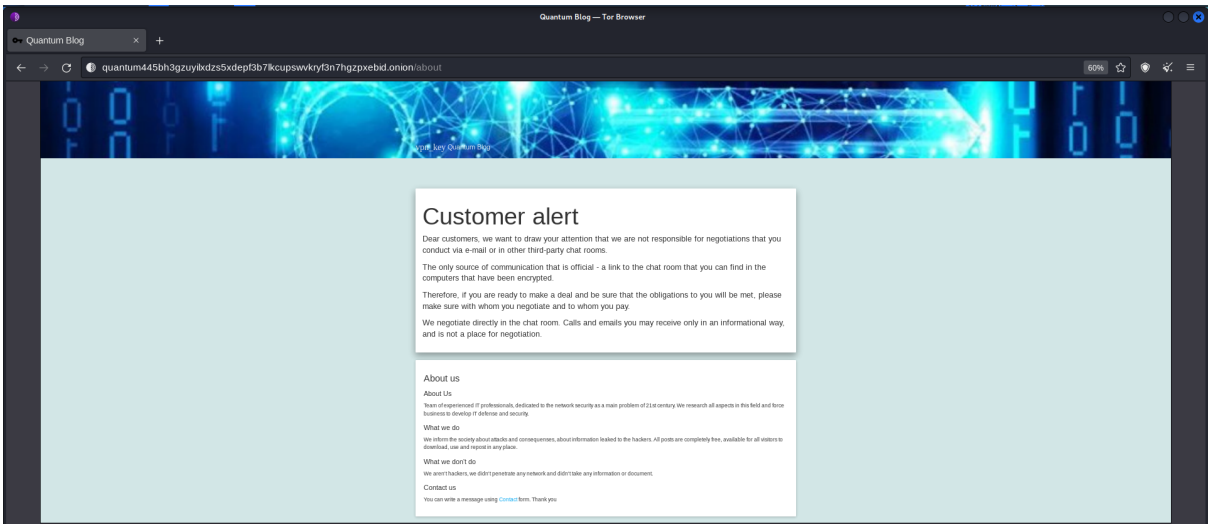


Figure 7: Screenshot of the Quantum Blog site

Based on what is seen on their onion site, Quantum claims to not be a hacker but rather a team of experienced IT professionals that seek to inform society about attacks and consequences. It was stated that they did not penetrate any network and take their information or documents.

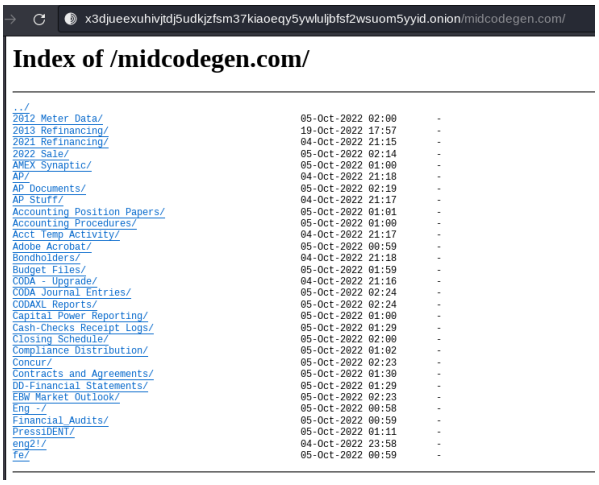


Figure 8: Screenshot of stolen data shared by Quantum

However, from their ‘Customer Alert’ content block, there seemed to be some form of payment, deals and negotiation happening which contradicts with what IT professionals whose goals are to raise awareness would engage in. Furthermore, sensitive data of existing companies are published for anyone to download in multiple posts.

External Information

Figure 9: History of ransomware used

Quantum, discovered in July 2021, is actually another rebranding of a notorious ransomware known as MountLocker which was launched in September 2020.

Similar to Bianlian, they are known to use **double extortion** tactics in which they demand varying amounts of ransoms from their victims within 72 hours and if otherwise, the stolen data is shared on their website for free downloads by the public (Cybereason, 2022).

Data Cleanup

During the preprocessing of our data collected, our team noticed that we were able to group many similar companies under the same industry. This would greatly help with our analysis as some industries are too specific to observe a notable trend. As such, our team has grouped some specific industries into a larger generalised groups as follow:

Industry	**Some Examples**
Others	Community Services, companies that do not fit any of the main categories e.g., YMCA, KlamoyaCasino
Professional Services	Inspection services, regulatory-focused solutions and services, relationship dating agency, consulting firms, counselling

Research Limitations

The information used for our data visualisation are primarily sourced directly from the ransomware groups' site via web scraping. Other information used in the analysis include but are not limited to secondary sources such as news articles, government reports and technology companies' reports.

Analysis and Visualisations

1. What is the % distribution in the Victim Industry And Geography?

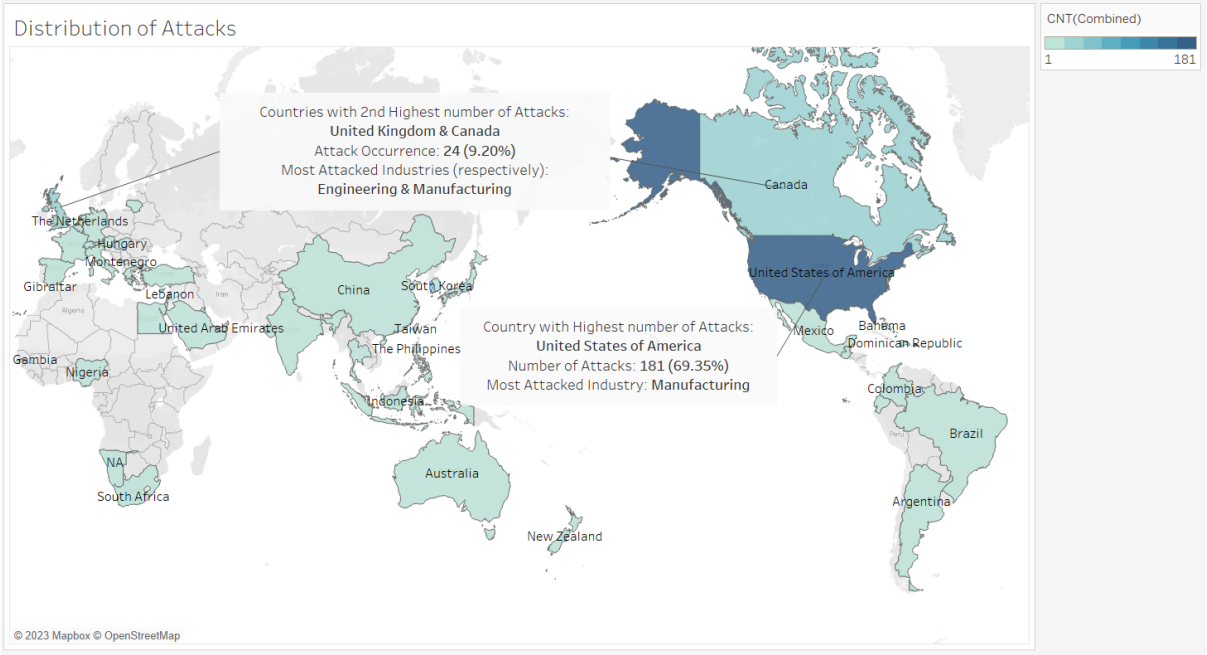


Figure 10: Distribution of Attacked Countries in 2022 (map view)

Attacked Regions (Table)

Region	Number of Attacks	% of Total Count of Combined along Table (Down)
Americas	219	59.19%
Europe	84	22.70%
Asia Pacific	50	13.51%
Middle East	12	3.24%
Africa	3	0.81%
NA	2	0.54%

Attacked Countries (Table)

Country	Number of Attacks	% of Attacks by Countries
United States of America	181	48.92%
Canada	24	6.49%
United Kingdom	24	6.49%
Australia	18	4.86%
Germany	14	3.78%
India	9	2.43%
Italy	9	2.43%
France	7	1.89%
Japan	6	1.62%
United Arab Emirates	5	1.35%
Austria	4	1.08%
Brazil	4	1.08%
Colombia	4	1.08%
Spain	4	1.08%
Hong Kong	3	0.81%
Kuwait	3	0.81%
Mexico	3	0.81%
Switzerland	3	0.81%
Taiwan	3	0.81%
Turkey	3	0.81%
Argentina	2	0.54%
China	2	0.54%
Dominican Republic	2	0.54%
Ecuador	2	0.54%
Indonesia	2	0.54%
NA	2	0.54%
New Zealand	2	0.54%
Saudi Arabia	2	0.54%
South Korea	2	0.54%
Thailand	2	0.54%
Bahama	1	0.27%
Belgium	1	0.27%
Cyprus	1	0.27%
Egypt	1	0.27%

Attacked Industries (Table)

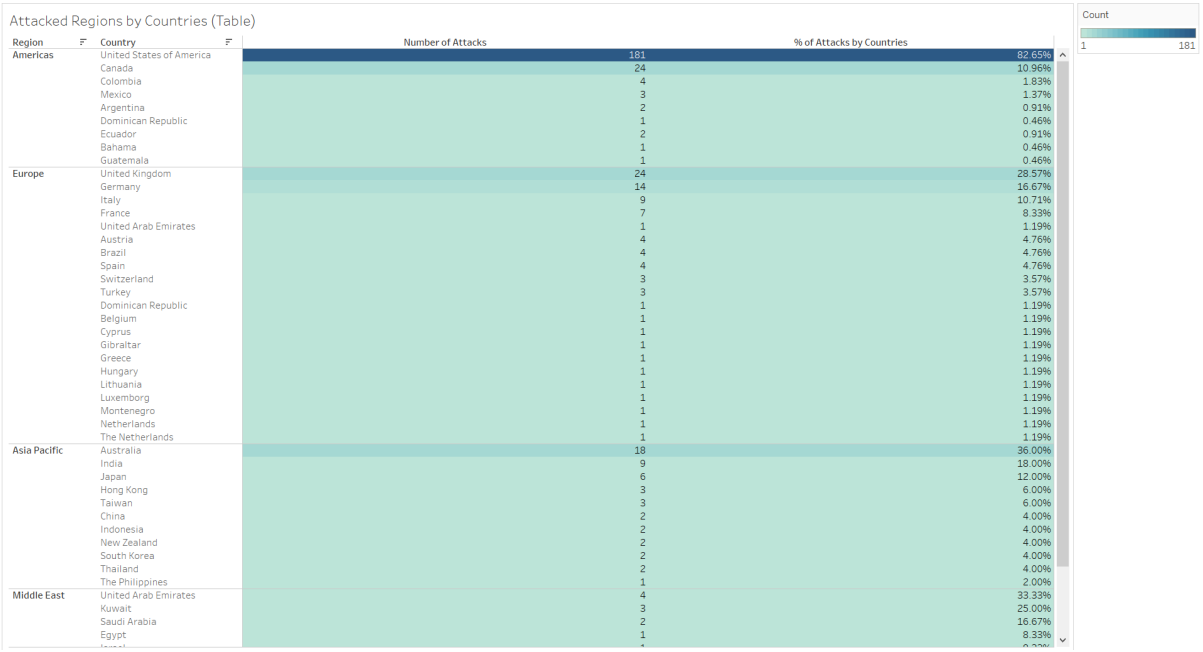
Count
1 181

Industry	Number of Attacks	% of Attacks by Industry
Manufacturing	47	12.70%
Information Technology	28	7.57%
Professional Services	26	7.03%
Finance and Insurance	25	6.76%
Education	22	5.95%
Law	21	5.68%
Healthcare	20	5.41%
Engineering	19	5.14%
Retail	17	4.59%
Government	16	4.32%
Transportation	16	4.32%
Arts and Entertainment	13	3.51%
Others	13	3.51%
Utilities	12	3.24%
F&B	11	2.97%
Construction	10	2.70%
Oil & Gas	10	2.70%
Consulting	8	2.16%
Real Estate	8	2.16%
Hospitality	5	1.35%
Agriculture	3	0.81%
Chemical Industries	3	0.81%
Casino	2	0.54%
Floriculture	2	0.54%
NA	2	0.54%
Non-Profit	2	0.54%
Pharmaceutical	2	0.54%
Telecommunication	2	0.54%
Tourism	2	0.54%
Automotive	1	0.27%

Figure 11: Dashboard of Overall Attacks based on Regions, Countries & Industries

From Figure 11, the manufacturing industry made up the largest percentage of ransomware attacks in 2022 at 12.7%. Surprisingly, the next few industries on the list have only about half the percentage relative to the manufacturing industry, ranging from about 6% to 7.5%

Next, in terms of **geography**, the highest percentage of attacks were observed in the Americas (59.19%), followed by Europe (22.70%), Asia Pacific (13.51%), Middle East (3.24%) and Africa (0.81%).



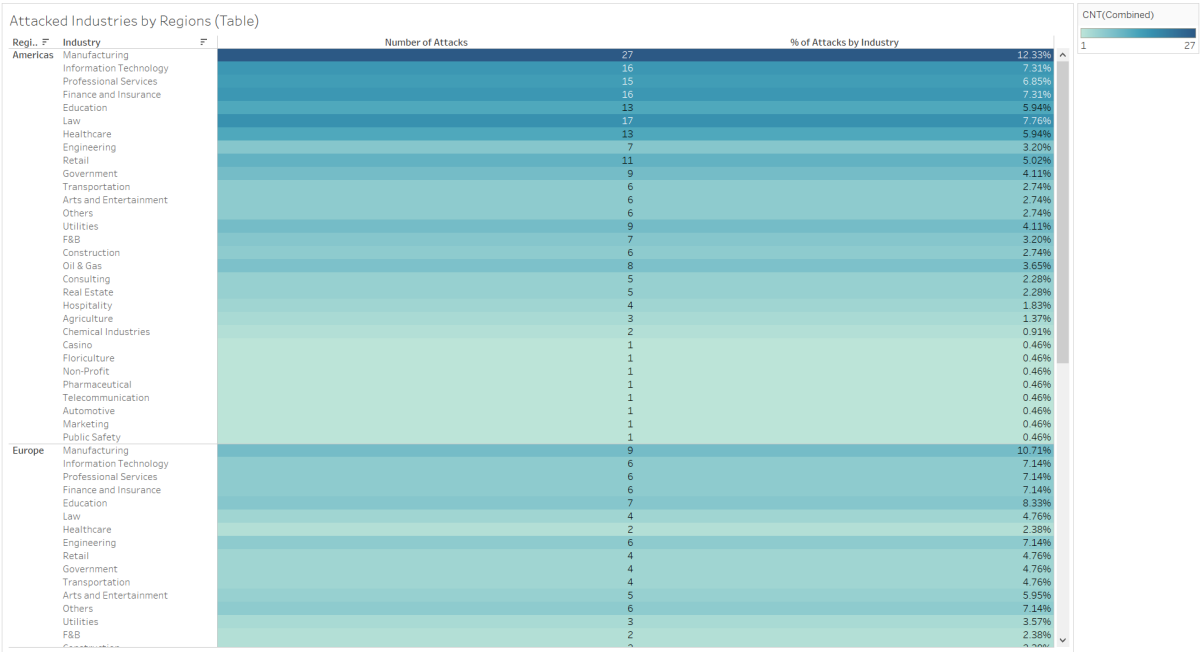
Attacked Regions by Countries (Table)

Region	Country	Number of Attacks	% of Attacks by Countries
Americas	United States of America	181	82.65%
	Canada	24	10.96%
	Colombia	4	1.83%
	Mexico	3	1.37%
	Argentina	2	0.91%
	Dominican Republic	1	0.46%
	Ecuador	2	0.91%
	Bahama	1	0.46%
	Guatemala	1	0.46%
Europe	United Kingdom	24	28.57%
	Germany	14	16.67%
	Italy	9	10.71%
	France	7	8.33%
	United Arab Emirates	1	1.19%
	Austria	4	4.76%
	Brazil	4	4.76%
	Spain	4	4.76%
	Switzerland	3	3.57%
	Turkey	3	3.57%
	Dominican Republic	1	1.19%
	Belgium	1	1.19%
	Cyprus	1	1.19%
	Gibraltar	1	1.19%
	Greece	1	1.19%
	Hungary	1	1.19%
	Lithuania	1	1.19%
	Luxemborg	1	1.19%
	Montenegro	1	1.19%
	Netherlands	1	1.19%
	The Netherlands	1	1.19%
Asia Pacific	Australia	18	36.00%
	India	9	18.00%
	Japan	6	12.00%
	Hong Kong	3	6.00%
	Taiwan	3	6.00%
	China	2	4.00%
	Indonesia	2	4.00%
	New Zealand	2	4.00%
	South Korea	2	4.00%
	Thailand	2	4.00%
	The Philippines	1	2.00%
Middle East	United Arab Emirates	4	33.33%
	Kuwait	3	25.00%
	Saudi Arabia	2	16.67%
	Egypt	1	8.33%

Count
1 181

Figure 12: Attacked Regions ranked by countries

Diving deeper into the specific regions, the majority of the attacks in the Americas are dominated by the United States (US) and Canada at 82.65% and 10.96% respectively.



Attacked Industries by Regions (Table)

Regi..	Industry	Number of Attacks	% of Attacks by Industry
Americas	Manufacturing	27	12.33%
	Information Technology	16	7.31%
	Professional Services	15	6.85%
	Finance and Insurance	16	7.31%
	Education	13	5.94%
	Law	17	7.76%
	Healthcare	13	5.94%
	Engineering	7	3.20%
	Retail	11	5.02%
	Government	9	4.11%
	Transportation	6	2.74%
	Arts and Entertainment	6	2.74%
	Others	6	2.74%
	Utilities	9	4.11%
	F&B	7	3.20%
	Construction	6	2.74%
	Oil & Gas	8	3.65%
	Consulting	5	2.28%
	Real Estate	5	2.28%
	Hospitality	4	1.83%
	Agriculture	3	1.37%
	Chemical Industries	2	0.91%
	Casino	1	0.46%
	Floriculture	1	0.46%
	Non-Profit	1	0.46%
	Pharmaceutical	1	0.46%
	Telecommunication	1	0.46%
	Automotive	1	0.46%
	Marketing	1	0.46%
	Public Safety	1	0.46%
Europe	Manufacturing	9	10.71%
	Information Technology	6	7.14%
	Professional Services	6	7.14%
	Finance and Insurance	6	7.14%
	Education	7	8.33%
	Law	4	4.76%
	Healthcare	2	2.38%
	Engineering	6	7.14%
	Retail	4	4.76%
	Government	4	4.76%
	Transportation	4	4.76%
	Arts and Entertainment	5	5.95%
	Others	6	7.14%
	Utilities	3	3.57%
	F&B	2	2.38%

CNT(Combined)
1 27

Figure 13: Attacked Industries within each region

Similarly, the number of attacks in the manufacturing industry trumps other industries in each of the various regions. This data further supports the data shown previously in Figure 10 and Figure 11.

2. What Countries are most Targeted By Ransomware Actors? Why are some more targeted than others?

Attacked Regions by Countries

Country	Number of Attacks	% of Attacks by Countries
United States of America	181	48.92%
Canada	24	6.49%
United Kingdom	24	6.49%
Australia	18	4.86%
Germany	14	3.78%

Figure 14: Top 5 Most Attacked Countries in 2022
(Refer to Appendix Figure 25 for the full list of countries attacked)

In 2022, the **United States of America** (USA) was the most targeted country by ransomware actors, accounting for almost 50% of the attacks across the four ransomware groups. The next few countries are Canada, the United Kingdom (UK), Australia and Germany. In total, the top five countries accounted for 70.54% of the attacks. The remaining ~30% are spread across 44 other countries as seen in Figure 25 in the *Appendix.*

Looking at these countries, there are several reasons as to why they are more targeted than other countries.

Firstly, these countries are first world countries and are **highly developed** with a large number of businesses and individuals using digital technology. This makes them an **obvious target** for ransomware actors who seek to exploit vulnerabilities in computer networks and systems. Evidently, having a higher digital adoption rate would increase the attack surface and potential attack vectors, making ransomware attacks more likely to succeed.

Next, they are home to many **large corporations**, financial institutions, and government agencies, which are attractive targets for ransomware actors seeking for large ransom payments. A 2021 whitepaper from Sophos also revealed that larger organisations are about 10% more likely to be hit with a ransomware attack (Sophos Ltd, 2021).

Additionally, ransomware actors often demand payment in **cryptocurrency**, hence the chances of payment increases when targeting the population from a developed country as the people are more likely to be digitally equipped and knowledgeable. This is evident in an government report in which it stated that '...cryptocurrency, typically Bitcoin, has become a near universal form of ransom payment in ransomware attacks, in part, because cryptocurrency enables criminals to extort huge sums of money from victims across diverse sectors with incredible speed (Peters, n.d.). On the other hand, less technologically advanced countries might struggle to set up their cryptocurrency wallets and delay the payment of ransom.

Interestingly, the **cultural aspect** of these countries might have also contributed to the high percentage. Specifically, employees might be more likely to click on unknown email attachments and expose themselves to more threats simply because they believe the company is either **too insignificant** to be an actual target of ransomware or because they

have **adequate insurance** to guard against ransomware attacks. These two main reasons could explain that humans are ultimately the weakest link to cyber attacks. A more recent Sophos whitepaper in 2022 reveals that there is 98% pay-out rate on ransomware claims. Hence, having insurance to fall back on might have aggravated and contributed to increased recklessness of employees and their poor security hygiene (Sophos Ltd, 2022).

Lastly, the **origin of the threat actors and ransomware groups** could also be a factor for consideration as to why some countries are being targeted more. There is a pattern that ransomware groups are commonly situated in certain countries and they are less likely to target their own homeground. For example, the ransomware by Cuba has a kill-switch when it detects that the host is likely of Russian origin (*Ransomware Spotlight: Cuba - Security News*, 2022).

Overall, the combination of a highly digitised economy, high value targets, and cultural aspects make these countries prime targets for ransomware attacks.

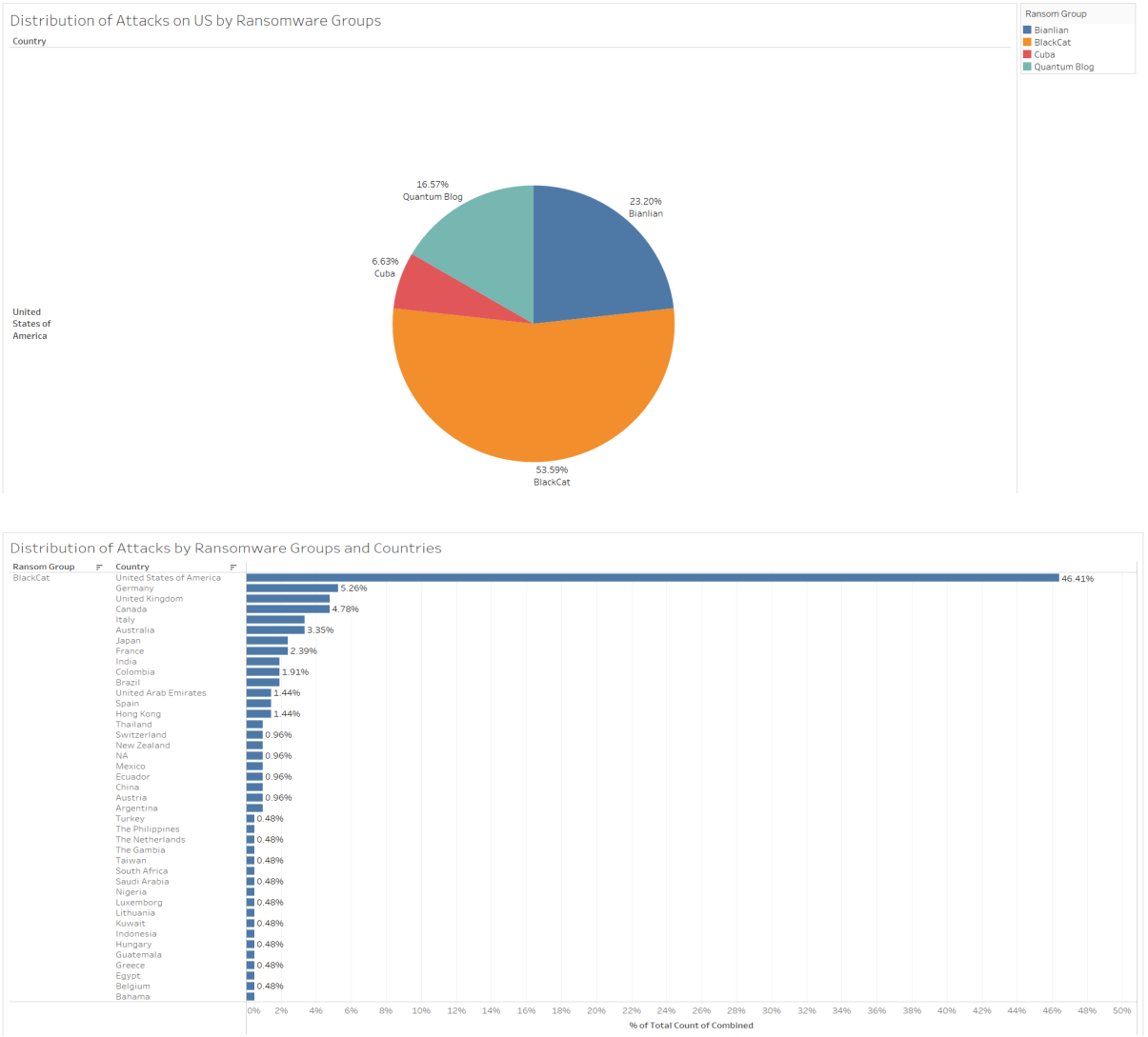


Figure 15: Distribution of attacks by groups (top) and within BlackCat (bottom)

Looking at the distribution by ransomware groups of US's threat actors, BlackCat accounts for 53.59% of their attacks.

Based on BlackCat's leak site, it is revealed that the group favoured enterprises based in the US, with 46.41% of their total attacks being attributed to US.

From our research, we found that BlackCat is suspected to have strong relations with past ransomware groups like Dark Side and Black Matter due to similarities in their TTPs. Diving into the past of Dark Side and Black Matter, both groups had announced that their targets are **organisations that can afford to pay large ransoms**. In support of this, past statistics have shown that both groups are predominantly targeting English-speaking countries such as the US, Canada and UK.

Under the assumption that BlackCat is indeed a successor of Dark Side or Black Matter, there would be a high possibility that BlackCat kept to the same tradition and hence, mostly target specific countries like the US.

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

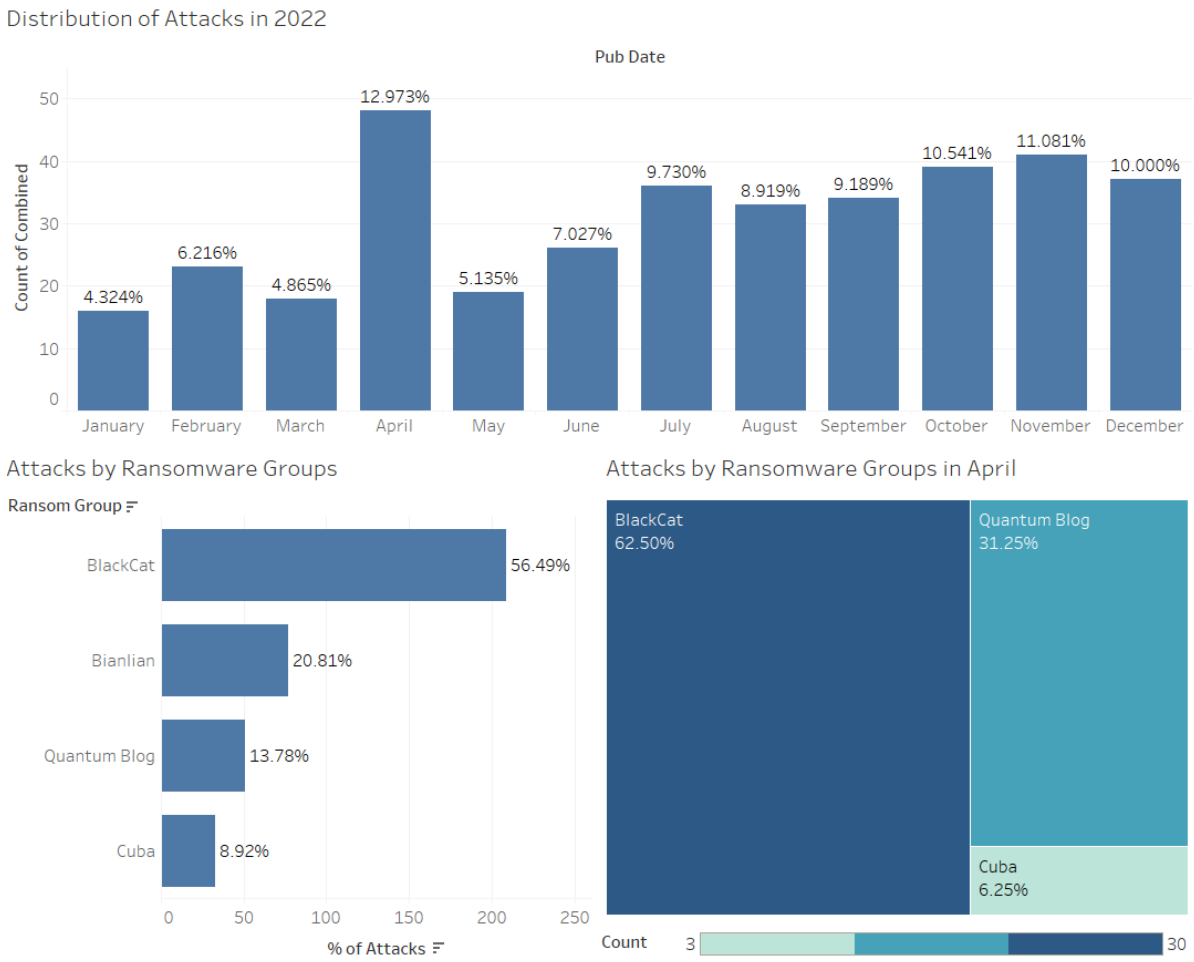


Figure 16: Dashboard of Ransomware Groups' Activities

Across the four groups, BlackCat is the most active, taking up more than half of the attacks in 2022 in absolute numbers. This could be attributed to several possible reasons.

Notably, there could be **incomplete data collection** from the various ransomware sites. Apart from law enforcement agencies and cybersecurity firms actively tracking into ransomware sites, ransomware groups may take down or abandon their site to avoid being caught. As such, the information on their site **might not be the full list** of attacks that they have conducted. For instance, our team noted that Cuba has over 100+ attacks conducted based on our secondary research (Ransomware Spotlight: BlackCat - Security News, 2022). However, the data on their site that we've obtained only consists of 34 records.

In addition, the article also mentioned BlackCat provides a **higher payout share** to its affiliates of up to 90%, which would nudge more affiliates from using the ransomware tools developed by BlackCat. Moreover, it also found that BlackCat had been extremely active in various forum sites to recruit new affiliates to carry out these attacks for financial purposes.

TTPs of Ransomware Group

BlackCat's unique tactics have made them a successful ransomware operation. Firstly, their ransomware is written in Rust, which provides attackers with several advantages, including making the **ransomware harder to analyse in sandbox environments**. Also, the chance of detection of their ransomware is considerably lower compared to their competitors in the market (Centre for Internet Security, n.d.). Conversely, other groups often utilised malware coded mainly for the Windows environment in C# (Galiette, A., Bunce, D., Santos, D., & Westfall, S., 2022) and target primarily the Windows operating system. Arguably, such software could be more **easily identified** by Windows Defender.

Next, the group often leverages Exchange Server vulnerabilities to gain initial access (Intelligence, M. D. T., 2022). Evidently, these industries and countries are very likely to use Microsoft Active Directory and other Exchange related services as a **de-facto solution** to manage their enterprise. Coupled with the need to connect to these systems remotely (VPN) due to a larger proportion of employees working from home due to Covid-19, the attack surface has been increased. These factors increased the success rates of BlackCat ransomware. Moreover, **variations in the exact TTPs used by BlackCat's affiliates** made it more difficult for defenders to detect and respond against BlackCat ransomware. On the other hand, the other groups mainly relied on Phishing for initial access and compromise (Anvilogic, 2022), which might be less reliable compared to a known exploit.

Also, BlackCat ransomware has functionalities for lateral movement, credential harvesting and persistence. These aspects, coupled with a "self-propagation" worm-like feature probably aggravated the impact of the ransomware and allowed it to easily spread to other systems, via vectors such as email etc (Palazolo, G, 2022; Intelligence, M. D. T., 2022). Such capabilities are often unavailable in other malware used by other ransomware groups.

Finally, BlackCat has launched one of the first public data leak sites on the public internet, which pressures victims even further to fulfil the attackers' demands. Overall, BlackCat's unique tactics have made them a formidable ransomware operation.

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

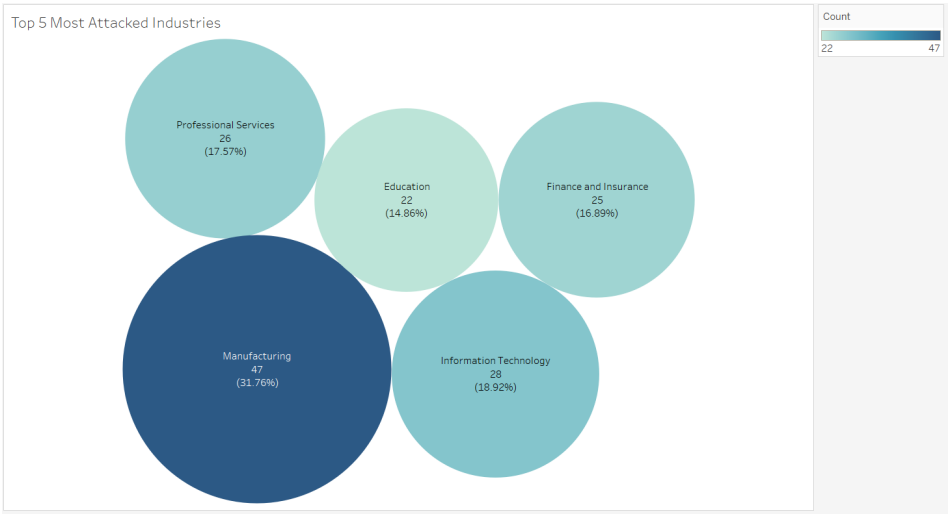


Figure 17: Top 5 Attacked Industries in 2022

Across the four ransomware groups, it can be seen that the **manufacturing industry** is the most prone to ransomware threats. This could be attributed to the fact that manufacturing companies have **complex supply chains** that include numerous vendors, partners and contractors, making it challenging to secure their systems and networks comprehensively. Coupled with ransomware that has worm-like functionalities such as BlackCats', this could have led to quicker and wider spread of the malware within the industry itself.

Secondly, manufacturing companies may also be using **outdated or legacy systems** since they are difficult to update or replace due to their criticality to the manufacturing process or high cost of replacement due to example, large systems being tightly coupled. Thus making their systems more vulnerable/susceptible to cyberattacks. This can be evident in a report published in 2021 by IBM, it states that 47% of the attacks within the manufacturing industry were due to vulnerabilities that companies did not patch.

Thirdly, there may be a **lack of cyber skills** within the company. According to an article by BlackBerry (2023), more than half of the manufacturers surveyed (54%) stated that they did not boost cybersecurity, despite investing in digital transformation and connectivity.

Another reason could be the **mindset** that security is the enemy of quick and fast progress. Having additional security checks and guardrails often slows down the deployment process of new software and hardware, hence making security seem like a **cost centre** in the short run. This probably explains why IT is the next largest industry to be attacked if stakeholders choose to prioritise short-term profits and neglect the long-term costs from recovering from a ransomware attack, which averages around USD 1.4M (Sophos Ltd., 2022)

Further Analysis based on Ransomware Groups

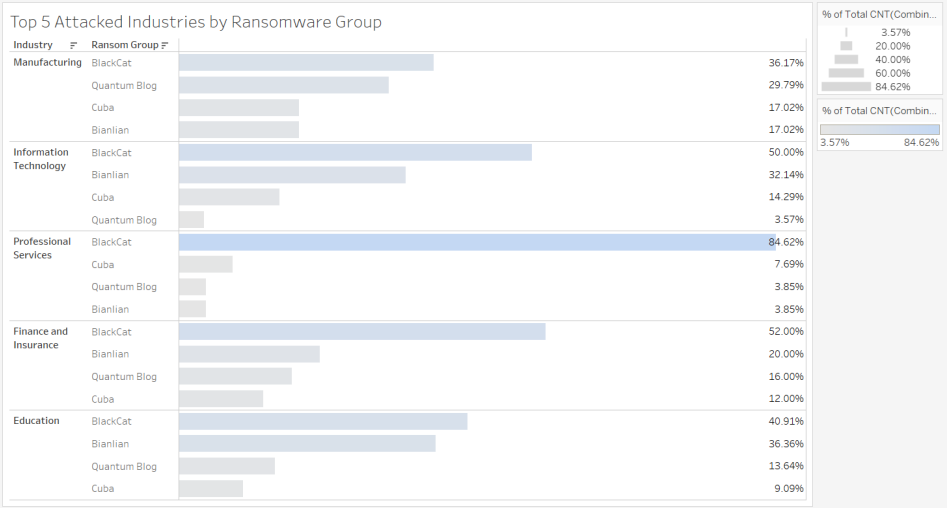


Figure 18: Top 5 Attacked Industries by Ransomware Groups

Diving into the attacks on the industries by ransomware groups, it can be observed that the number of attacks on the manufacturing industry are fairly distributed amongst the groups. Conversely, some industries have huge differences where BlackCat and Bianlian are evidently taking the lead in the number of attacks.

This could mean a few things:

1) Ransomware groups see a **value in targeting the manufacturing industry** (Avertium, 2022) and hence, there is a less difference in the percentage distribution of attacks among the adversary groups.

2) The manufacturing industry is **indeed more vulnerable to attacks**, possibly due to weaker cybersecurity defences and failure to invest in effective security technologies which further supports our general analysis.

3) Some adversary groups might have **specialised domain knowledge** of a particular industry that provided them an edge in compromising systems in that industry. For instance, BlackCat has a massive edge in targeting Professional services, suggesting that their group might have a deeper understanding of the workings within that industry in order to increase their success rates (and number of attacks) on that industry.

4) Some ransomware groups might be **smaller and have fewer affiliates**. Being smaller in group size would thus suggest fewer attacks. Perhaps, other groups less BlackCat had to prioritise on a few industries (low hanging fruits). The strategy of striving for depth instead of breadth could be extremely successful and thus adopted by these groups.

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.

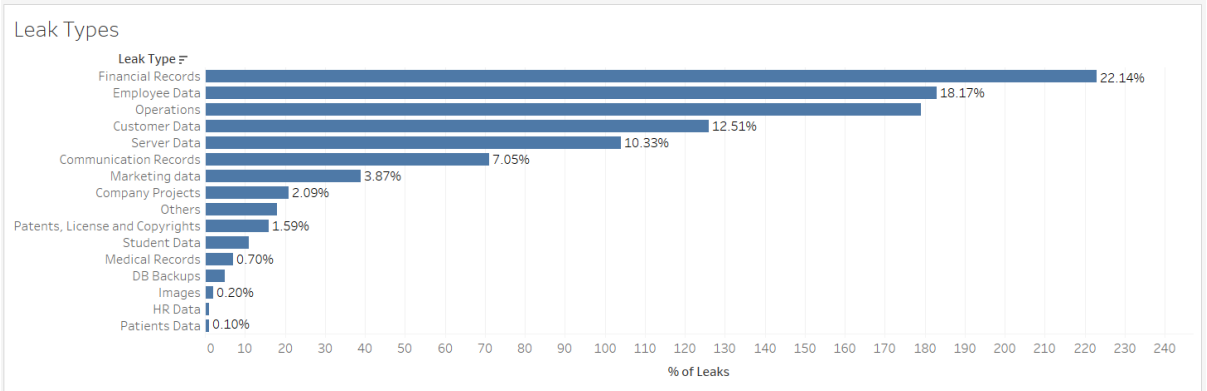


Figure 19: Overall Percentage of Leak Types

General Overview

Based on the chart above, it is evident that *'Financial Records'* which may include balance sheets, transaction records, bank account information etc, is the most sought after by threat actors. Followed by *'Employee Data'* which entails their name, contact, address and other personal information.

In the case of ransomware groups, firstly, they are able to use sensitive financial data as **leverage** to demand higher ransom payments from the victim company to avoid the public release or sale of their data.

Secondly, financial data, especially that of large companies, can fetch a **high price** on the dark web. As such, ransomware groups steal this data and sell it to other criminal groups or individuals, which can be a lucrative source of income for the group.

Thirdly, it can be used to **damage the company's reputation**. By publicly releasing sensitive financial data can cause them to lose customers, partners, and investors especially if the records reveal that the company does not have good financial standing or credibility.

These reasons made financial data especially enticing to be leaked, as companies might have strong incentives to prevent such information from being leaked to the public. Hence, with many groups operating as a *Ransomware-as-a-Service* (RaaS), financial data would be the ideal choice to achieve their objective of obtaining the highest possible ransom.

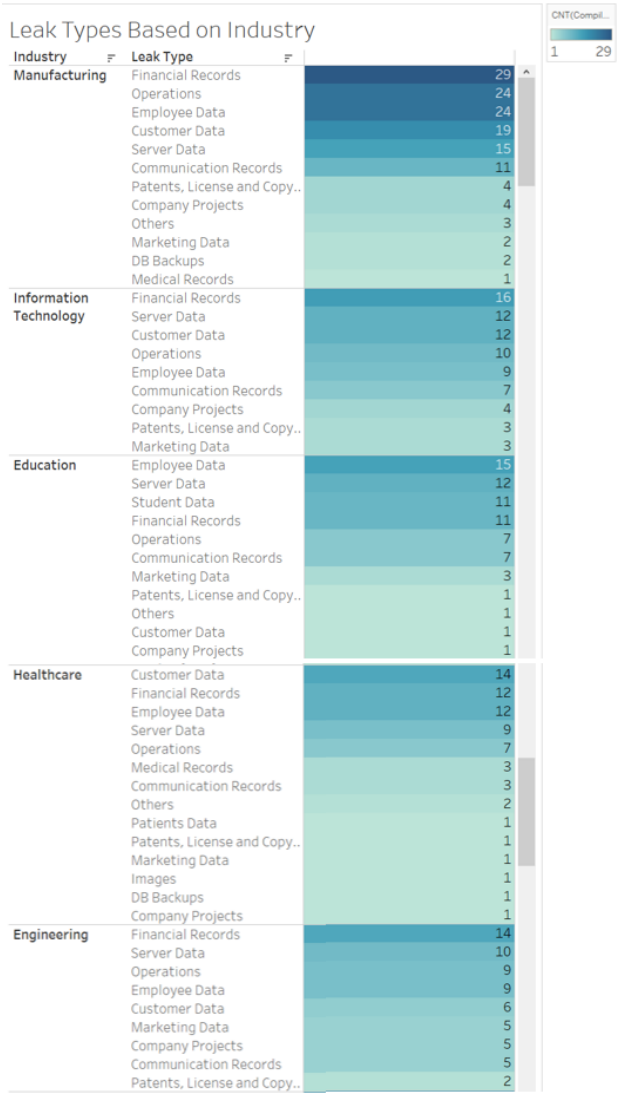


Figure 20: Top 5 Targeted Industries and their Leaked Types

For this analysis, we will be focusing on the top 5 most attacked industries and their stolen data. *You may refer to Appendix for the full list of industries and their data breakdown.*

We are going to conduct our analysis, from the perspective of each industry and analyse the possible reason behind the exfiltration of each data based on our findings in Figure 20 (we will be looking at mainly the top 5 data types):

Manufacturing	Information Technology	Education	Healthcare	Engineering
1. Financial Records 2. Operations 3. Employee Data 4. Customer Data 5. Server Data	1. Financial Records 2. Server Data 3. Customer Data 4. Operations 5. Employee Data	1. Employee Data 2. Server Data 3. Student Data 4. Financial Records 5. Operations	1. Customer Data 2. Financial Records 3. Employee Data 4. Server Data 5. Operations	1. Financial Records 2. Server Data 3. Operations 4. Employee Data 5. Customer Data

Figure 21: Top 5 Targeted Industries and their Leaked Types

As starters, the theft of **personal information** be it of Employees, Customers or Students is very common, sitting at the top 3 most common leaked types in most industries. This is anticipated because personal information is almost always highly valuable when sold to the right people on the deep web marketplace or to competitors. Furthermore, personal information may also be used for **fraud, identity theft, and even blackmailing**. With the increased focus on the protection of personal identifiable information (PII) such as the General Data Protection Regulation (GDPR) in Europe, these PII would become increasingly attractive for sale.

Top on the list of data leakage types are **financial records**. They are a very common target for attackers as it ties in to the profitability and liquidity of the business. It could also give information about the companies' financial health which may directly influence their market shares and stock prices. Such data breach could also reduce the trust of the general public towards the business. Hence, in order to maintain the trust in their corporation, some corporations might be more willing to pay up to prevent such data from being leaked (Data Breaches 101: How They Happen, What Gets Stolen, and Where It All Goes - Security News, 2018).

Scoping into the various industries, for manufacturing companies, the manufacturing operations - consisting of non-disclosure agreements, intellectual properties, business operations and trade secrets - are the most targeted. This data is highly attractive, especially to competitors who wish to launch a competing product, as it could threaten the company's share in the market and spell the doom of some corporations in extreme circumstances. To illustrate, competitors might be able to produce the same goods at a cheaper price as they do not have to factor in the R&D costs should they simply steal the data (Arctic Wolf, n.d.).

Moving on to Information Technology (IT) companies, server data is the next most leaked after financial records. This mainly consists of data from an employee's computer like server backups, IT apps, system files, databases, scanned documents, notes, manuals and instructions etc. We believe this information is a crucial aspect of IT businesses, and by possessing the company's business plans and product ideas, ransomware groups are able to sell it for monetary gains easily (*The Types Of Business Data That Hackers Look For.*, n.d.).

In the Education and Healthcare industries, data breach of personal information is highly common, especially in the healthcare industry. Stolen records can be used to gain unauthorised access to sensitive information about an individual. Using the SingHealth hack in Singapore as a case study, this incident highlights the importance of having strong guardrails on such sensitive data. Specifically, there could be stigma associated with some health conditions such as AIDS. Worse, the stability of countries or companies could be compromised when health records of important head figures are leaked. These records could decrease others' confidence in their current and future ability to lead. For the Education industry, important information like driver's licence or passport information, social security numbers, or bank details could also be obtained from Employee's personal information (Ekran System, n.d.).

Lastly, for engineering, server data is the most leaked. Our group postulates that since many engineering firms have gone digital in the past decade, information containing corporate

intelligence, infrastructure, drawing plans etc. are stored digitally on servers. The leak of trade secrets could impact the company's operations and allow their competitors to gain unfair advantage over the company. Therefore, server data is highly targeted in a cyber attack against engineering firms (Bangcawayan, J, 2021).

6. Share 3 new interesting insights you observed.

Insight: Ransomware groups often have a different origin country than claimed

One question our team has in mind is whether the country of origin of the adversary is **really where they claim to be from**. Using the data collected, we believe that this assumption is **largely false** with high confidence. For example, adversaries like Cuba which seemed like they are from Cuba (or at least sounds that way) but may have originated from Russia. This is strengthened by evidence from a report by Trend Micro (2022) which shows that the malware used by Cuba had a kill-switch which was activated upon the discovery that the keyboard layout is in Russian. Perhaps industries should switch their keyboard layout to the less attacked countries in hopes of lowering the probability of being targeted!

On the same point, adversaries are generally made up of recruits that can come from various parts of the world and therefore do not equate to the people of a specific country of origin. For example, BlackCat might have multiple affiliates which performed the actual attack as a proxy, masking the true origin of the organisation itself.

Insight: Many factors might have led to an unusually high percentage of attacks in April and end-of-year of 2022

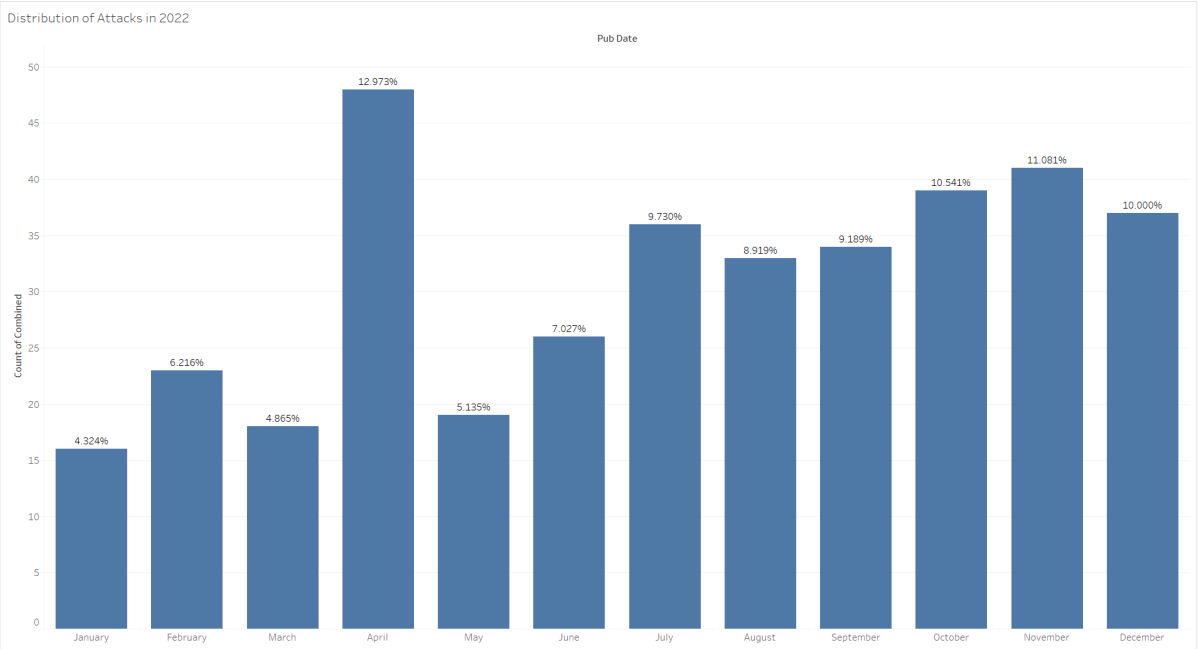


Figure 22: Distribution of Attacks in 2022 by Month

Our group identified some factors that might explain why April might be popular for these ransomware groups.

Firstly, April 1st, which is April's Fools Day, could lower the victims' guard because they would believe that the attacks might be a false alarm and disregard potential dangers. Moreover, being in a celebratory mood could also contribute to more opportunities for lapses as people become lax in their security posture.

Additionally, April is the month that public companies release their earnings. Earning season starts two or three weeks after the end of the quarter. This is a very active time in the market as participants (analysts, traders, and investors) review their earnings reports, which may affect their stock pricing (Langager, 2021). Hence, April is a prime time to target these corporations as they have a strong incentive to pay for the ransom to ensure smooth operations during this crucial tax filing period as it progresses towards the next financial year. Moreover, a negative PR due to a leak during this timing might result in more scrutiny in the various reports and financial statements which are published. These are definitely not what a corporation desires during this period of time, hence increasing the likelihood of paying the ransom.

Lastly, other than April, it is evident that the end of the year (Nov - Dec) also has multiple attacks. We postulate that the holiday season (Black Friday, Christmas, New Year) might have led to the relaxation of companies' security posture and allowed threat actors to compromise their systems more easily.

<u>Insight: Based on the leak data size, healthcare has the largest leaked data size despite being targeted less in absolute numbers</u>

Total Leaked Size by Industry

Industry	
Healthcare	17,716
Manufacturing	5,597
Information Technology	3,488
Engineering	2,828
Government	2,282
F&B	1,971
Finance and Insurance	1,841
Education	1,454
Transportation	1,299
Others	818
Real Estate	756
Law	589
Construction	550
Casino	480
Utilities	450
Professional Services	440
Retail	340
Arts and Entertainment	250
Agriculture	200
Chemical Industries	150
Consulting	11
Grand Total	43,510

Figure 23: Breakdown of data leak size by industry

From Figure 23, even though healthcare is not in the top 5 in terms of absolute number of data breaches, the leak data size is more than 3 times more than manufacturing i.e. the next industry in line for size of breach. This shows the contrast between the **quantity of leaks** in sheer numbers (manufacturing) and the **quality of each leak** that result in leaks with potentially higher impact and scale (healthcare).

Our group believes with medium-high confidence that this is probably because the data from healthcare are potentially more valuable since they contain personal health records which are valued highly in the black market, hence posing more incentive to leak more data.

Another reason could be that healthcare is still lagging behind in terms of their cyber security for their IT infrastructure which led to a larger scale breach compared to other industries. The report from Sophos (2022) shows that allocating budget mindlessly into security has nearly **no positive impact** on preventing or mitigating ransomware attacks. This could be the key into why some industries continuously get targeted despite rising investments in security.

Lastly, a simple reason could also be that industries like IT and manufacturing often archive past data into other servers meant for long term storage to save costs, similar to the Glacier servers in AWS. They could afford to do this because those data are likely only kept for audit trails and serve little importance currently. Healthcare, on the other hand, cannot afford to archive patients' data since they would need to be accessed frequently and irregularly, whenever they visit a clinic or hospital. This forces them to keep the data hot in the servers, leading to a larger data breach size and scale when they are attacked.

Total Leaked Size by Industry and Ransomware Groups

Ransom Group	Industry	
Blanlian	Healthcare	17,000
	Information Technology	2,188
	Engineering	2,011
	Education	1,078
	Manufacturing	1,019
	F&B	876
	Real Estate	636
	Law	500
	Casino	480
	Retail	340
	Agriculture	200
	Chemical Industries	150
	Professional Services	40
	Total	26,518
Quantum Blog	Manufacturing	4,578
	Government	2,282
	Finance and Insurance	1,841
	Information Technology	1,300
	Transportation	1,299
	F&B	1,095
	Others	818
	Engineering	817
	Healthcare	716
	Construction	550
	Utilities	450
	Professional Services	400
	Education	376
	Arts and Entertainment	250
	Real Estate	120
	Law	89
	Consulting	11
	Total	16,992
Grand Total		43,510

Figure 24: Breakdown by size based on the 2 groups we had data on

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

One of the main challenges the team faced was cleaning up the data that we had gathered through web scraping. The data was obtained from various sources and in **different formats**, which made it difficult to **integrate and analyse**. This presented several challenges in terms of data quality, data completeness and data consistency, and made it difficult to draw meaningful visualisations or insights from the data.

To overcome this challenge, we first created a detailed data cleaning plan that included identifying the sources of data, defining the data cleaning rules, and creating a process for identifying and addressing data quality issues. Next, we used various tools and techniques to standardise the data, including transforming data formats, filling in missing values, and identifying and removing duplicates. We all worked closely together as a team to validate the accuracy of the data and ensure that it met our quality standards.

Another major challenge we faced was to locate the exact country of the companies targeted by ransomware groups for attacks. It was unclear if some companies targeted originated back to the parent company location, or if it is another branch with the parent company name. For example, Company ABC's main office is located in Singapore, but the ransomware group attacked the Vietnam branch of Company ABC instead. Would it be to state the country of Company ABC, as Singapore or Vietnam is something that we asked ourselves when cleaning up the data before data visualisation. One way to address this issue was to locate the office address on the company's website because a postal code is a giveaway to where the office is located and it is unique. If the website does not provide any office address, we stick with using the parent company's address instead to fill up the country column.

Appendices

Attacked Countries

Country	Number of Attacks	% of Attacks by Countries
United States of America	181	48.92%
Canada	24	6.49%
United Kingdom	24	6.49%
Australia	18	4.86%
Germany	14	3.78%
India	9	2.43%
Italy	9	2.43%
France	7	1.89%
Japan	6	1.62%
United Arab Emirates	5	1.35%
Austria	4	1.08%
Brazil	4	1.08%
Colombia	4	1.08%
Spain	4	1.08%
Hong Kong	3	0.81%
Kuwait	3	0.81%
Mexico	3	0.81%
Switzerland	3	0.81%
Taiwan	3	0.81%
Turkey	3	0.81%
Argentina	2	0.54%
China	2	0.54%
Dominican Republic	2	0.54%
Ecuador	2	0.54%
Indonesia	2	0.54%
NA	2	0.54%
New Zealand	2	0.54%
Saudi Arabia	2	0.54%
South Korea	2	0.54%
Thailand	2	0.54%
Bahama	1	0.27%
Belgium	1	0.27%
Cyprus	1	0.27%
Egypt	1	0.27%
Gibraltar	1	0.27%
Greece	1	0.27%
Guatemala	1	0.27%
Hungary	1	0.27%
Israel	1	0.27%
Lebanon	1	0.27%
Lithuania	1	0.27%
Luxemborg	1	0.27%
Montenegro	1	0.27%
Netherlands	1	0.27%
Nigeria	1	0.27%
South Africa	1	0.27%
The Gambia	1	0.27%
The Netherlands	1	0.27%
The Philippines	1	0.27%

Attacked Industries

Industry	Number of Attacks	% of Attacks by Industry
Manufacturing	47	12.70%
Information Technology	28	7.57%
Professional Services	26	7.03%
Finance and Insurance	25	6.76%
Education	22	5.95%
Law	21	5.68%
Healthcare	20	5.41%
Engineering	19	5.14%
Retail	17	4.59%
Government	16	4.32%
Transportation	16	4.32%
Arts and Entertainment	13	3.51%
Others	13	3.51%
Utilities	12	3.24%
F&B	11	2.97%
Construction	10	2.70%
Oil & Gas	10	2.70%
Consulting	8	2.16%
Real Estate	8	2.16%
Hospitality	5	1.35%
Agriculture	3	0.81%
Chemical Industries	3	0.81%
Casino	2	0.54%
Floriculture	2	0.54%
NA	2	0.54%
Non-Profit	2	0.54%
Pharmaceutical	2	0.54%
Telecommunication	2	0.54%
Tourism	2	0.54%
Automotive	1	0.27%
Marketing	1	0.27%
Public Safety	1	0.27%

Figure 25: Dashboard of Overall Attacks based on Countries & Industries

Distribution of Attacks by Industries & Countries

Count: 1 – 21

Industry	Country	Number of Attacks	% of Total Count of Combined along Country
Manufacturing	United States of America	21	44.68%
	Canada	4	8.51%
	United Kingdom	2	4.26%
	Germany	1	2.13%
	Italy	3	6.38%
	Japan	3	6.38%
	Hong Kong	1	2.13%
	Mexico	2	4.26%
	Switzerland	2	4.26%
	Taiwan	3	6.38%
	China	1	2.13%
	Indonesia	1	2.13%
	South Korea	2	4.26%
	Netherlands	1	2.13%
Information Technology	United States of America	15	53.57%
	Canada	1	3.57%
	Germany	2	7.14%
	India	2	7.14%
	Italy	1	3.57%
	United Arab Emirates	1	3.57%
	Brazil	1	3.57%
	Turkey	1	3.57%
	New Zealand	1	3.57%
	Saudi Arabia	1	3.57%
	Cyprus	1	3.57%
	Israel	1	3.57%
Professional Services	United States of America	13	50.00%
	Canada	1	3.85%
	United Kingdom	1	3.85%
	Australia	2	7.69%
	Germany	1	3.85%
	India	1	3.85%
	Hong Kong	1	3.85%
	Kuwait	1	3.85%
	Turkey	1	3.85%
	Bahama	1	3.85%
	Greece	1	3.85%
	Hungary	1	3.85%
	Lithuania	1	3.85%

Figure 26: Distribution of Attacks based on Countries & Industries

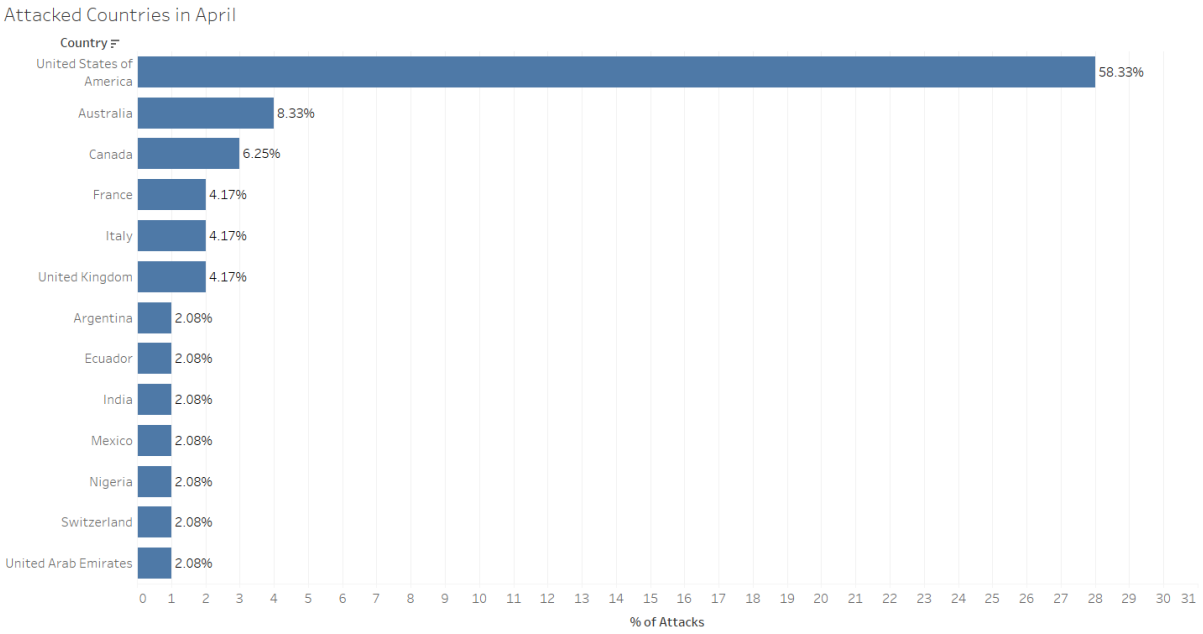


Figure 27: Percentage of Attacks by Countries in April

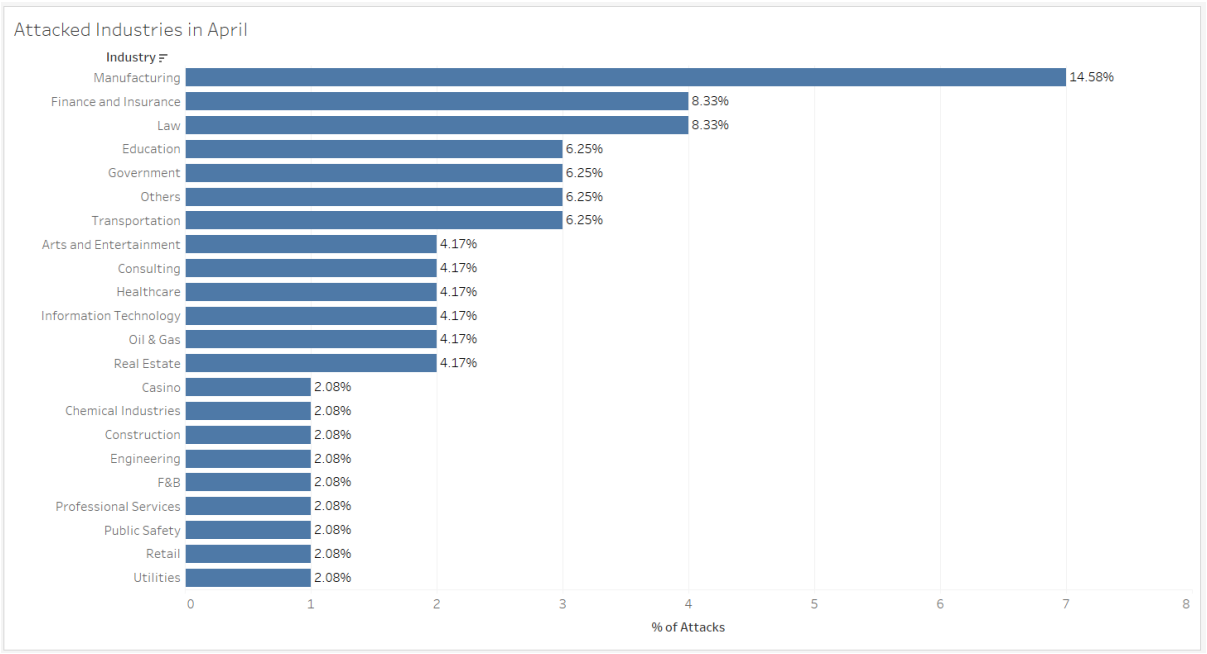
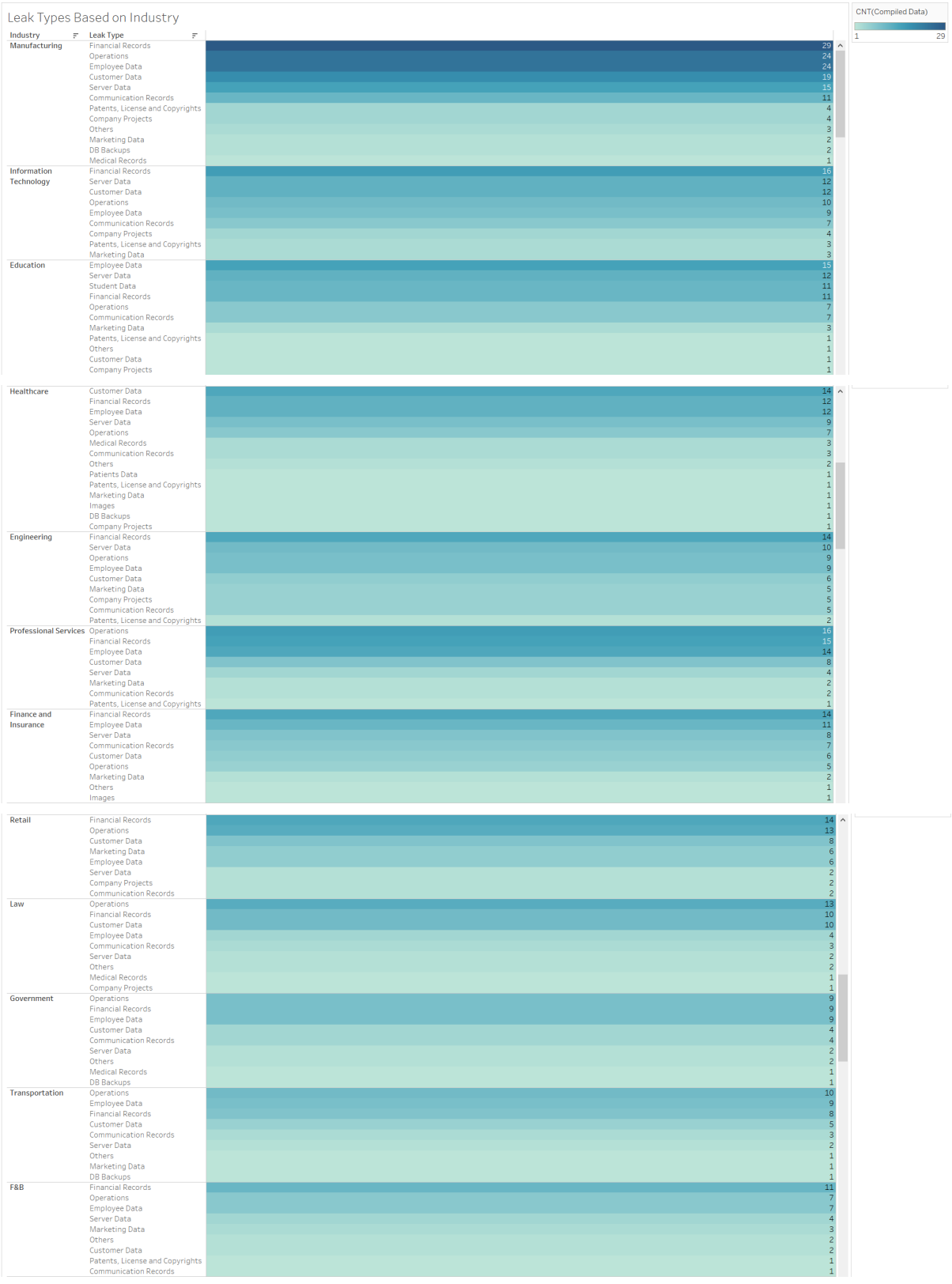
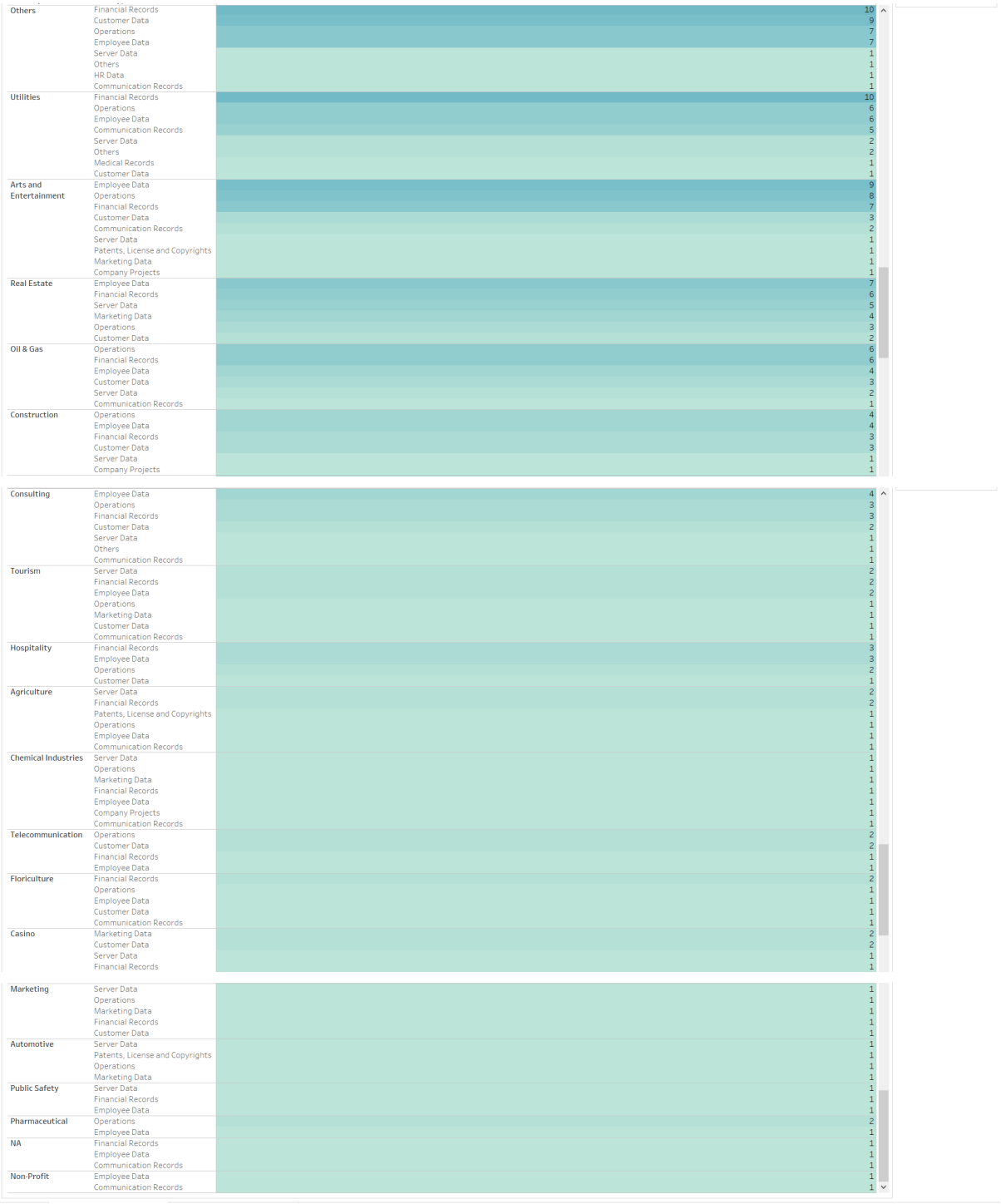


Figure 28: Percentage of Attacks by Industries in April


Leak Types Based on Industry
CNT(Compiled Data)
1
29
Industry
Leak Type
Manufacturing
Financial Records 29
Operations 24
Employee Data 24
Customer Data 19
Server Data 15
Communication Records 11
Patents, License and Copyrights 4
Company Projects 4
Others 3
Marketing Data 2
DB Backups 2
Medical Records 1
Information Technology
Financial Records 16
Server Data 12
Customer Data 12
Operations 10
Employee Data 9
Communication Records 7
Company Projects 4
Patents, License and Copyrights 3
Marketing Data 3
Education
Employee Data 15
Server Data 12
Student Data 11
Financial Records 11
Operations 7
Communication Records 7
Marketing Data 3
Patents, License and Copyrights 1
Others 1
Customer Data 1
Company Projects 1
Healthcare
Customer Data 14
Financial Records 12
Employee Data 12
Server Data 9
Operations 7
Medical Records 3
Communication Records 3
Others 2
Patients Data 1
Patents, License and Copyrights 1
Marketing Data 1
Images 1
DB Backups 1
Company Projects 1
Engineering
Financial Records 14
Server Data 10
Operations 9
Employee Data 9
Customer Data 6
Marketing Data 5
Company Projects 5
Communication Records 5
Patents, License and Copyrights 2
Professional Services
Operations 16
Financial Records 15
Employee Data 14
Customer Data 8
Server Data 4
Marketing Data 2
Communication Records 2
Patents, License and Copyrights 1
Finance and Insurance
Financial Records 14
Employee Data 11
Server Data 8
Communication Records 7
Customer Data 6
Operations 5
Marketing Data 2
Others 1
Images 1
Retail
Financial Records 14
Operations 13
Customer Data 8
Marketing Data 6
Employee Data 6
Server Data 2
Company Projects 2
Communication Records 2
Law
Operations 13
Financial Records 10
Customer Data 10
Employee Data 4
Communication Records 3
Server Data 2
Others 2
Medical Records 1
Company Projects 1
Government
Operations 9
Financial Records 9
Employee Data 9
Customer Data 4
Communication Records 4
Server Data 2
Others 2
Medical Records 1
DB Backups 1
Transportation
Operations 10
Employee Data 9
Financial Records 8
Customer Data 5
Communication Records 3
Server Data 2
Others 1
Marketing Data 1
DB Backups 1
F&B
Financial Records 11
Operations 7
Employee Data 7
Server Data 4
Marketing Data 3
Others 2
Customer Data 2
Patents, License and Copyrights 1
Communication Records 1



Others	Financial Records	10
	Customer Data	9
	Operations	7
	Employee Data	7
	Server Data	1
	Others	1
	HR Data	1
	Communication Records	1
Utilities	Financial Records	10
	Operations	6
	Employee Data	6
	Communication Records	5
	Server Data	2
	Others	2
	Medical Records	1
	Customer Data	1
Arts and Entertainment	Employee Data	9
	Operations	8
	Financial Records	7
	Customer Data	3
	Communication Records	2
	Server Data	1
	Patents, License and Copyrights	1
	Marketing Data	1
	Company Projects	1
Real Estate	Employee Data	7
	Financial Records	6
	Server Data	5
	Marketing Data	4
	Operations	3
	Customer Data	2
Oil & Gas	Operations	6
	Financial Records	6
	Employee Data	4
	Customer Data	3
	Server Data	2
	Communication Records	1
Construction	Operations	4
	Employee Data	4
	Financial Records	3
	Customer Data	3
	Server Data	1
	Company Projects	1
Consulting	Employee Data	4
	Operations	3
	Financial Records	3
	Customer Data	2
	Server Data	1
	Others	1
	Communication Records	1
Tourism	Server Data	2
	Financial Records	2
	Employee Data	2
	Operations	1
	Marketing Data	1
	Customer Data	1
	Communication Records	1
Hospitality	Financial Records	3
	Employee Data	3
	Operations	2
	Customer Data	1
Agriculture	Server Data	2
	Financial Records	2
	Patents, License and Copyrights	1
	Operations	1
	Employee Data	1
	Communication Records	1
Chemical Industries	Server Data	1
	Operations	1
	Marketing Data	1
	Financial Records	1
	Employee Data	1
	Company Projects	1
	Communication Records	1
Telecommunication	Operations	2
	Customer Data	2
	Financial Records	1
	Employee Data	1
Floriculture	Financial Records	2
	Operations	1
	Employee Data	1
	Customer Data	1
	Communication Records	1
Casino	Marketing Data	2
	Customer Data	2
	Server Data	1
	Financial Records	1
Marketing	Server Data	1
	Operations	1
	Marketing Data	1
	Financial Records	1
	Customer Data	1
Automotive	Server Data	1
	Patents, License and Copyrights	1
	Operations	1
	Marketing Data	1
Public Safety	Server Data	1
	Financial Records	1
	Employee Data	1
Pharmaceutical	Operations	2
	Employee Data	1
NA	Financial Records	1
	Employee Data	1
	Communication Records	1
Non-Profit	Employee Data	1
	Communication Records	1

Figure 29: Leaked Data Types Based on Industry

Total Leaked Size by Industry

Industry	Organisation	
Healthcare	St Rose Hospital	17,000
	ZEUS Scientific	540
	Avante Health Solutions	90
	Medlab Pathology	86
	Total	**17,716**
Manufacturing	Radical Sportscars	1,000
	ChemiFlex	1,000
	Henry	830
	N****	560
	Drive Products	500
	Crupi Group	450
	Hi Tech HoneyComb	350
	Berlina Tbk	223
	American International Industries	167
	SEMITEC Corporation	150
	Broshuis | Driving innovation	117
	Orotex	70
	Power Plant Services LLC	50
	Wolfe Industrial	45
	Badger Truck Refrigeration, Inc	36
	Tex-Isle Supply	32
	AHT Wisconsin Windows	11
	Shaw & Slavsky	6
	Total	**5,597**
Information Technology	BEESENSE	1,300
	Hci Systems Inc	800
	Myofficeplace Inc	506
	Modular Mining Systems	500
	Ability Commerce	200
	Aria systems	100
	ZXP Technologies	82
	Total	**3,488**
Engineering	BRYCON Construction	900
	Delon Hampton & Associates, Chartered	817
	IM Group	521
	HRL Technology Group	400
	MITCON Consultancy & Engineering Services	110
	Altec Engineering LLC	80
	Total	**2,828**
Government	Instituto Agrario Dominicano	1,100
	Florida Department of Veterans' Affairs	1,100
	Elgin County	50
	Tehama County Social Services	32
	Total	**2,282**
F&B	Broadleaf	795
	Golden Coin Bake Shop & Restaurant	476
	Bonn Nutrients Pvt	400
	Maple Lodge Farms	300
	Total	**1,971**
Finance and Insurance	RG Alliance Group	1,200
	Lightbank	590
	M. Green and Company LLP	41
	Acquarius Trust Group	10
	Total	**1,841**
Education	Myton School	567
	Emilio Sanchez American School	235
	Camden City School District	200
	CIMT College	196
	Altoona Area School District	150
	VANOSS Public School	80
	Lewis & Clark College	26
	Total	**1,454**
Transportation	Pilenpak	1,000
	Liftow LTD	255
	JetStar	43
	Jazeera Airways	1
	Total	**1,299**
Others	Confcommercio - Alessandria - Home	700
	Shred Station	47
	Service Employees' International Union	43
	YMCA	28
	Total	**818**
Real Estate	Realstar Holdings Partnership	378
	Australian Real Estate Group Pty Ltd	200
	Valley Rentals	120
	Block Buildings LLC	58
	Total	**756**
Law	Lawadami	500
	Moskowitz, Mandell & Salim, P.A.	89
	Total	**589**
Construction	Hufcor	550
	Total	**550**
Casino	Eureka Casino Resort	480
	Total	**480**
Utilities	Midland Cogeneration Venture, Michigan	150
	Midland Cogeneration Venture	150
	MCV Holding Company LLC	150
	Total	**450**
Professional	Freyr Solutions	400

Total Leaked Size by Industry

Industry	Organisation	
F&B	Broadleaf	795
	Golden Coin Bake Shop & Restaurant	476
	Bonn Nutrients Pvt	400
	Maple Lodge Farms	300
	Total	**1,971**
Finance and Insurance	RG Alliance Group	1,200
	Lightbank	590
	M. Green and Company LLP	41
	Acquarius Trust Group	10
	Total	**1,841**
Education	Myton School	567
	Emilio Sanchez American School	235
	Camden City School District	200
	CIMT College	196
	Altoona Area School District	150
	VANOSS Public School	80
	Lewis & Clark College	26
	Total	**1,454**
Transportation	Pilenpak	1,000
	Liftow LTD	255
	JetStar	43
	Jazeera Airways	1
	Total	**1,299**
Others	Confcommercio - Alessandria - Home	700
	Shred Station	47
	Service Employees' International Union	43
	YMCA	28
	Total	**818**
Real Estate	Realstar Holdings Partnership	378
	Australian Real Estate Group Pty Ltd	200
	Valley Rentals	120
	Block Buildings LLC	58
	Total	**756**
Law	Lawadami	500
	Moskowitz, Mandell & Salim, P.A.	89
	Total	**589**
Construction	Hufcor	550
	Total	**550**
Casino	Eureka Casino Resort	480
	Total	**480**
Utilities	Midland Cogeneration Venture, Michigan	150
	Midland Cogeneration Venture	150
	MCV Holding Company LLC	150
	Total	**450**
Professional Services	Freyr Solutions	400
	Samrin Services Pvt Ltd	40
	Total	**440**
Retail	NewYorker	340
	Total	**340**
Arts and Entertainment	Moscone Center	250
	Total	**250**
Agriculture	Danielski Farms Inc	200
	Total	**200**
Chemical Industries	CROWN TECHNOLOGY Ltd	150
	Total	**150**
Consulting	InfoTek Consulting Services	11
	Total	**11**

Figure 30: Leaked Data Size by Industry

References

Abrams, L.A. [@LawrenceAbrams]. (2022, April 28). Typically, you can detect a rebrand via code overlaps or chatty ops/affiliates. [Tweet; thread]. Twitter. https://twitter.com/LawrenceAbrams/status/1519495698680623104

Abrams, L. (2022, February 5). BlackCat (ALPHV) ransomware linked to BlackMatter, DarkSide gangs. Bleeping Computer. Retrieved March 19, 2023, from https://www.bleepingcomputer.com/news/security/blackcat-alphv-ransomware-linked-to-blackmatter-darkside-gangs/

Avertium. (2022, August 16). An In-Depth Look at Quantum Ransomware. Retrieved March 19, 2023, from https://explore.avertium.com/resource/an-in-depth-look-at-quantum-ransomware

Avertium (2022, May 10). The Top 5 Cyber Threats Within the Manufacturing Industry. Retrieved March 19, 2023, from https://www.avertium.com/resources/threat-reports/top-5-threats-within-manufacturing

Anvilogic. (2022, July 6). *Quantizing Quantum Ransomware*. https://www.anvilogic.com/learn/quantizing-quantum-ransomware

Bangcawayan, J. (2021, September 21). Cybersecurity Challenges Faced by Engineering Companies. SSL.com. Retrieved March 19, 2023, from https://www.ssl.com/blogs/cybersecurity-engineering-companies/

BianLian: New Ransomware variant on the rise. (2022, August 18). Cyble Blog. Retrieved March 18, 2023, from https://blog.cyble.com/2022/08/18/bianlian-new-ransomware-variant-on-the-rise/

Biggest Manufacturing Industry Cyber Attacks. (n.d.). Arctic Wolf. Retrieved March 19, 2023, from https://arcticwolf.com/resources/blog/top-8-manufacturing-industry-cyberattacks/

Breaking Down the BlackCat Ransomware Operation. (2022, July 7). CIS. https://www.cisecurity.org/insights/blog/breaking-down-the-blackcat-ransomware-operation

Constantin, L. (2021, May 13). DarkSide ransomware explained: How it works and who is behind it. CSO Online. https://www.csoonline.com/article/3618688/darkside-ransomware-explained-how-it-works-and-who-is-behind-it.html

Culafi, A. (2022, January 18). Ransomware actors increasingly demand payment in Monero. TechTarget. Retrieved March 19, 2023, from https://www.techtarget.com/searchsecurity/news/252512142/Ransomware-actors-increasingly-demand-payment-in-Monero

Cyber-attacks on manufacturing: A clear and present danger. (n.d.). Cyber Startup Observatory. Retrieved March 19, 2023, from https://cyberstartupobservatory.com/cyber-attacks-on-manufacturing-a-clear-and-present-danger/

Cybereason vs. Quantum Locker Ransomware. (2022, May 9). Cybereason. Retrieved March 18, 2023, from https://www.cybereason.com/blog/cybereason-vs.-quantum-locker-ransomware

Data Breaches 101: How They Happen, What Gets Stolen, and Where It All Goes - Security News. (2018, August 10). Trend Micro. Retrieved March 19, 2023, from https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/data-breach-101

Duncan, B. (2021, April 1). Hancitor's Use of Cobalt Strike and a Noisy Network Ping Tool. Palo Alto Unit 42. Retrieved March 18, 2023, from https://unit42.paloaltonetworks.com/hancitor-infections-cobalt-strike/

DXC Technology. (n.d.). New BianLian ransomware group picks up its pace. https://dxc.com/us/en/insights/perspectives/report/dxc-security-threat-intelligence-report/october-2022/new-bianlian-ransomware-group-picks-up-its-pace

5 Industries Most at Risk of Data Breaches. (2022, May 5). Ekran System. Retrieved March 19, 2023, from https://www.ekransystem.com/en/blog/5-industries-most-risk-of-data-breaches

Galiette, A., Bunce, D., Santos, D., & Westfall, S. (2022, August 9). Novel News on Cuba Ransomware: Greetings From Tropical Scorpius. Unit 42. https://unit42.paloaltonetworks.com/cuba-ransomware-tropical-scorpius/

Hancitor (Malware Family). (n.d.). Malpedia. Retrieved March 18, 2023, from https://malpedia.caad.fkie.fraunhofer.de/details/win.hancitor

Holyome, K. (2023, January 4). Manufacturing and Cyberattacks: New Research Reveals Work Stoppages. BlackBerry Blog. Retrieved March 19, 2023, from https://blogs.blackberry.com/en/2023/01/manufacturing-and-cyberattacks-new-research

IBM Security X-Force Threat Intelligence Index 2023. (2023, February 24). IBM. Retrieved March 19, 2023, from https://www.ibm.com/downloads/cas/DB4GL8YM

Intelligence, M. D. T. (2022, August 17). *The many lives of BlackCat ransomware*. Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/2022/06/13/the-many-lives-of-blackcat-ransomware/

Lakshmanan, R. (2022, March 18). Experts Find Some Affiliates of BlackMatter Now Spreading BlackCat Ransomware. The Hacker News. Retrieved March 18, 2023, from https://thehackernews.com/2022/03/experts-find-some-affiliates-of.html

Langager, C. (2021, August 30). When Is Earnings Season? Investopedia. Retrieved March 19, 2023, from https://www.investopedia.com/ask/answers/08/earnings-season.asp

Manufacturing sector is the most popular target of cyber attacks. (2022, March 21). Cybersec Europe. Retrieved March 19, 2023, from https://www.cyberseceurope.com/blog/artikel/manufacturing-sector-is-the-most-popular-target-of-cyber-attacks/

MalwareHunterTeam [@malwrhunterteam] (2022, August 12). *AA BianLian x64 ransomware sample: eaf5e26c5e73f3db82cd07ea45e4d244ccb3ec3397ab5263a1a74add7bbcb6e2 So it is another Go ransomware. 😅 "jack/Projects/project1/crypt28"* [Tweet]. Twitter. https://twitter.com/malwrhunterteam/status/1557789273595731969

Noberus Ransomware: Darkside and BlackMatter Successor Continues to Evolve its Tactics. (2022, September 22). Symantec Enterprise Blogs. Retrieved March 18, 2023, from https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/noberus-blackcat-ransomware-ttps

Palazolo, G. (2022, November 8). *BlackCat Ransomware: Tactics and Techniques From a Targeted Attack*. Netskope. https://www.netskope.com/blog/blackcat-ransomware-tactics-and-techniques-from-a-targeted-attack

Peters, G. (n.d.). Use of Cryptocurrency in Ransomware Attacks, Available Data, and National Security Concerns. Senate Committee on Homeland Security and Governmental Affairs. Retrieved March 19, 2023, from https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/HSGAC%20Majority%20Cryptocurrency%20Ransomware%20Report_Executive%20Summary.pdf

Ransomware Spotlight: BlackCat - Security News. (2022, October 27). Trend Micro. Retrieved March 18, 2023, from https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackcat

Ransomware Spotlight: Cuba - Security News. (2022, December 7). Trend Micro. Retrieved March 19, 2023, from https://www.trendmicro.com/vinfo/ph/security/news/ransomware-spotlight/ransomware-spotlight-cuba

Sason, D. (2022, August 19). BlackMatter Ransomware: In-Depth Analysis & Recommendations | Varonis. https://www.varonis.com/blog/blackmatter-ransomware

Smilyanets, D. (2022, February 3). An ALPHV (BlackCat) representative discusses the group's plans for a ransomware 'meta-universe'. The Record by Recorded Future. Retrieved March 19, 2023, from https://therecord.media/an-alphv-blackcat-representative-discusses-the-groups-plans-for-a-ransomware-meta-universe

#StopRansomware: Cuba Ransomware. (2023, January 5). CISA. Retrieved March 18, 2023, from https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-335a

The BlackBerry Research & Intelligence Team. (2022, October 10). BianLian Ransomware Encrypts Files in the Blink of an Eye. https://blogs.blackberry.com/en/2022/10/bianlian-ransomware-encrypts-files-in-the-blink-of-an-eye

The Types Of Business Data That Hackers Look For. (n.d.). ERGOS.com. Retrieved March 19, 2023, from https://ergos.com/microsoft/the-types-of-business-data-that-hackers-look-for/

Tompkins, A. (2023, January 24). *What to know about BlackCat, the new ransomware group hitting hospitals, clinics, pharma – Poynter*. Poynter. Retrieved March 19, 2023, from https://www.poynter.org/reporting-editing/2023/what-is-blackcat-royal-malware-ransomware/

What Is Cuba Ransomware? (n.d.). BlackBerry. Retrieved March 18, 2023, from https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/cuba

Wikipedia contributors. (2023, March 2). DarkSide (hacker group). Wikipedia. https://en.wikipedia.org/wiki/DarkSide_(hacker_group)