CZ4070 Cyber Threat Intelligence Project 2: Analysis of different Ransomware sites

GROUP 7:

SANKAR SAMIKSHA (U2021021D)

RAVI SOUNDHARIYA (U2022267E)

SANSKIRTI VERMA (U2023954E)

POON YAN XIN MELISE (U2022504B)

LINCOLN LIM (U2120839J)

DANIEL TAY JIN HONG (U2121423C)

XING KUN (U2023452E)

MUHAMMAD HUDZAIFAH BIN MAHMOOD (U1940863E)

A project submitted to the School of Computer Science and Engineering as part of the CZ4070 Cyber Threat Intelligence Requirement

1 TABLE OF CONTENTS

2 Introduction

In this project, five ransomware shaming groups’ onion sites were scrapped – Lockbit, PlayNews(also known as Play or PlayCrypt), 8Base, Medusa and Lorenz. For this project, data type categories such as Personal Identifiable Information (PII), financial data and legal documents were constructed. Similarly, industry type categories were formed taking LinkedIn as a reference. Some industries were not available on LinkedIn, hence, were created from scratch. The data type and industry type categories are available in the Appendix.

3 Q1: What is the % distribution in Victim Industry and Geography? [2 marks]

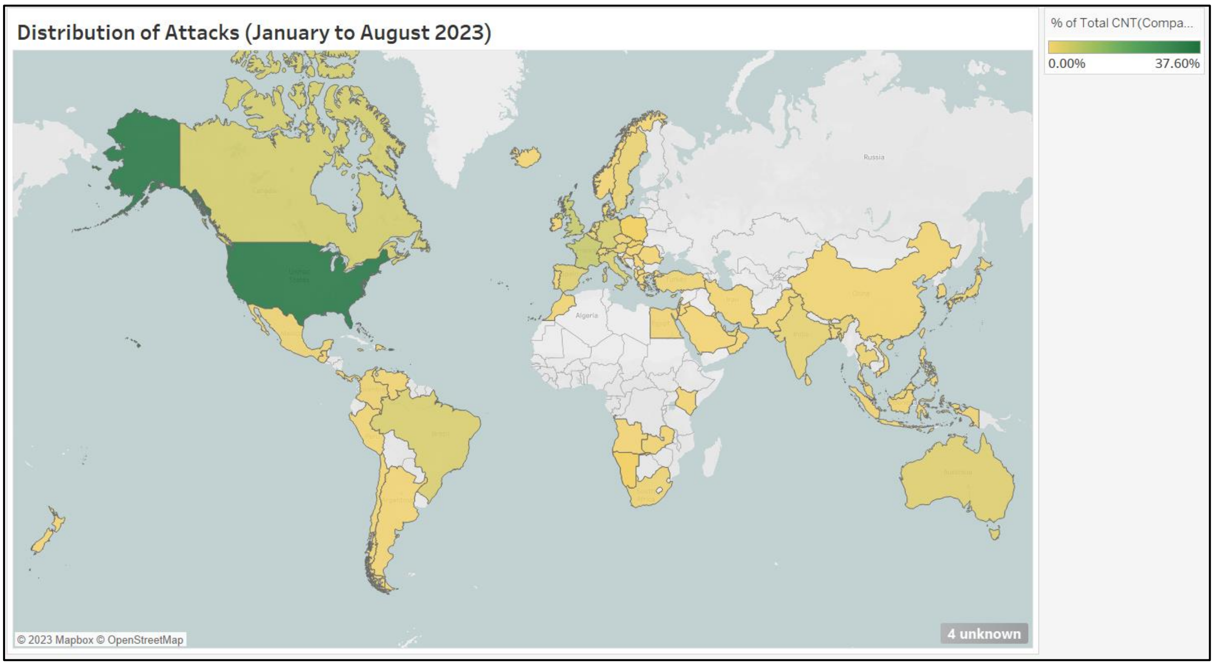

Distribution of Attacks (January to August 2023)
% of Total CNT(Compa...
0.00%
37.60%
Russia
Algeria
© 2023 Mapbox © OpenStreetMap
4 unknown

Figure 1: Distribution of Attacks

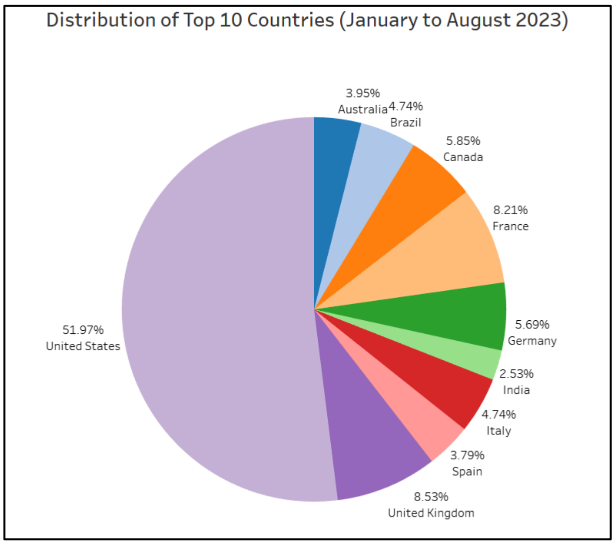


Figure 2: Percentage distribution of Top 10 Countries

The above figures shows the distribution of the attacks in each country. The attacks are from all five groups combined. United States has the highest number of attacks. It can be seen that these five groups combined, have attacked large portions of North America, South America, Europe and the APAC region. They have even attacked parts of South Africa and Middle East as well. Developed countries such as United States, United Kingdom, and France have higher proportion of attacks. Nations heavily reliant on technology and with extensive interconnectedness are more susceptible to cyber threats. The US, with its vital role in key manufacturing sectors and deep tech dependence, stands out as a prime target for cyber aggressors. Surprisingly, Russia has no reports of attacks. We hypothesise that the ransomwares we scrapped could be Russian aligned. This is supported by an article by Kaspersky that LockBit appears to deliberately refrain from targeting systems in Russia or any nations of the Commonwealth of Independent States. [1]This is likely to prevent legal actions in those regions. It is noteworthy that China did not make it into top 10 of countries attacked.

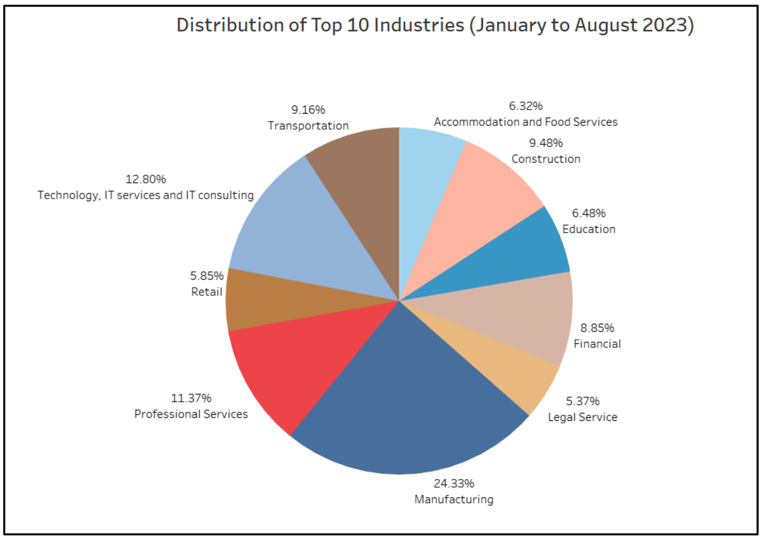


Figure 3: Percentage distribution of Industries (Top 10)

From the figure, Manufacturing industry takes up the largest proportion of the victim's industries, followed by Technology and Professional Services next.

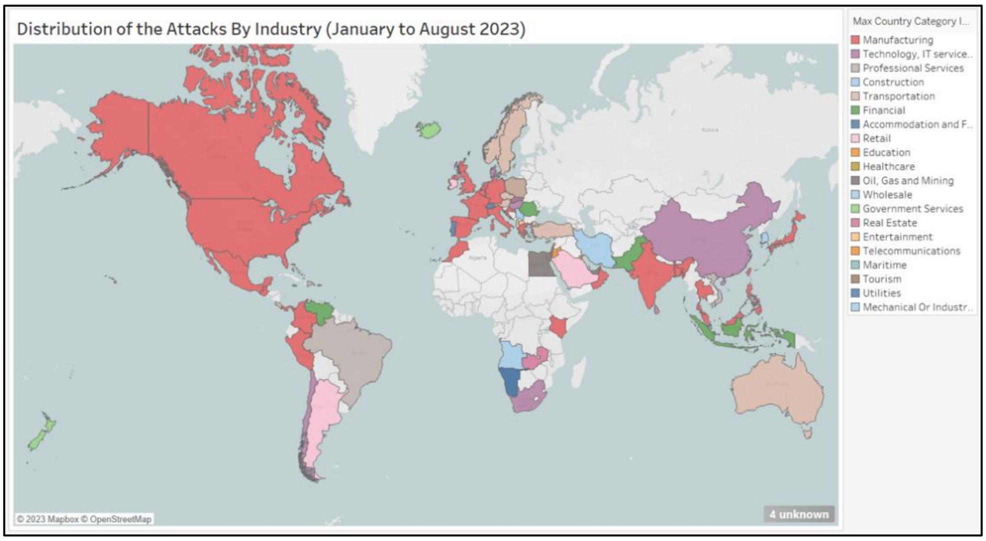


Figure 4: Industries that are attacked the most by country

The figure shows which industries are attacked in each country the most. For example, the manufacturing industry is targeted the most in India, Japan, South Korea, Germany, Italy, France, Spain, Mexico United Kingdom and United States. Many businesses in these nations operate within the manufacturing sector, so it's logical they experience a higher rate of attacks.

4 Q2: What Countries are most Targeted by Ransomware Actors? Why are some more targeted than others? [2 marks]

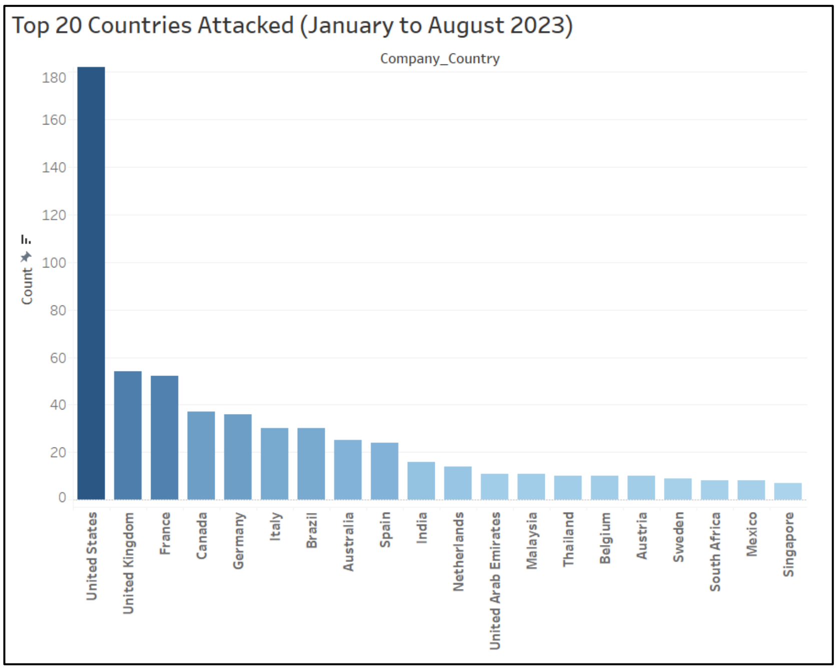


Figure 5: Top 20 most countries attacked

The graph above shows the top 20 countries most targeted by ransomware actors. The top is United States, followed by United Kingdom and France. Blackberry, a Canadian software company specializing in cybersecurity, stated that there is a "there is a positive correlation between an increased number of cyberattacks and countries that possess greater internet penetration, significant economies and larger populations" [2, 3].

United States does have the largest GDP [4]. This is probably why it is targeted the most.

Germany has fewer attacks than the United Kingdom (UK) even though Germany has a larger GDP and population than the UK [4, 5]. This is probably because UK has a larger internet penetration rate [6].

France has more attacks than Germany even though the latter has a larger GDP, a larger population, and a marginally larger internet penetration by 0.5% as of 2023 [4, 5, 6]. Hence, the reasons cited by Blackberry may not be the only causes for countries to be more targeted.

Firstly, countries could be targeted due to political reasons, financial reasons, specific motives of the threat groups etcetera. Secondly, the graph only shows the successful data leaks by only five ransomware groups. There are a lot more ransomware groups who would have attempted to attack a lot more countries and companies, and not all would have been successful.

5 Q3: Which Ransomware Group is the most active? What is so unique about their TTP that makes them so “successful”? [6 Marks]

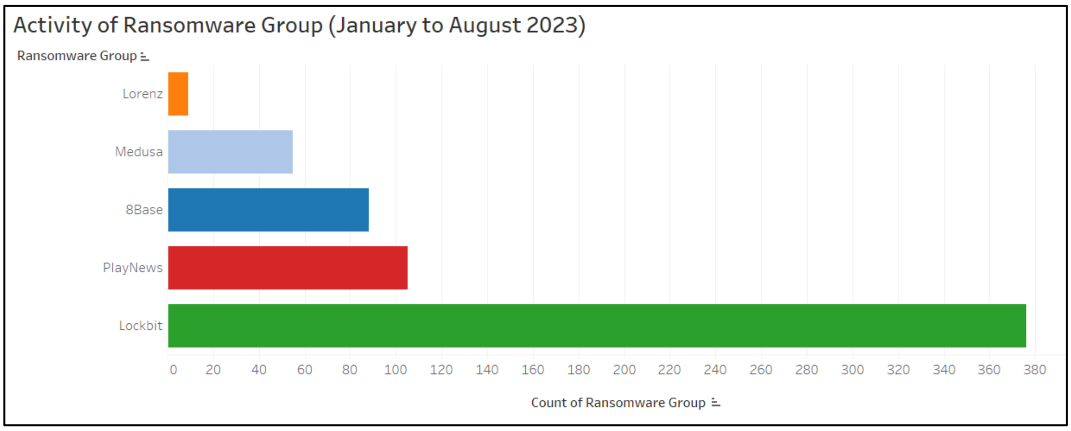


Figure 6: Activity of Each Ransomware Group in 2023

The most active ransomware group between January to August 2023 is Lockbit.

The Mitre ATT&CK framework was used to obtain the table below. However, not all techniques are listed as there are simply too many. Unfortunately, no information was available on 8base and Lorenz. A list of non-exhaustive tools used in each attack phase is documented as well.

	Lockbit (Examples only) [7] [8] [8] [9] [10] [11] [12]	Play [13] [14] [15] [16] [17]	Medusa [18]	Tools Used
Initial Access	T1189: Drive-by Compromise T1190: Exploit Public-Facing Application T1133: External Remote Services T1566: Phishing T1078: Valid Accounts	T1190: Exploit Public-Facing Application	T1133: External Remote Services T1566: Phishing	
Execution	T1059.003: Command and Scripting Interpreter: Windows Command Shell T1072: Software Deployment Tools T1569.002: System Services: Service Execution	T1106: Native API T1059: Command and Scripting Interpreter T1203: Exploitation for Client Execution	T1059.001: Command and Scripting Interpreter: PowerShell	Task Scheduler PowerShell Chocolatey PsExec
Persistence	T1547: Boot or Logon Autostart Execution T1078: Valid Accounts			Remote Desktop Protocol (RDP)
Privilege Escalation	T1548: Abuse Elevation Control Mechanism			User Account Control (UAC) bypass techniques Group Policy
Defence evasion	T1070.004: Indicator Removal: File Deletion T1027: Obfuscated Files or Information T1480.001: Execution Guardrails: Environmental Keying	T1027: Obfuscated Files or Information T1140: Deobfuscate/Decode Files or information T1055: Process Injection T1070:Indicator Removal	T1562.009: Impair Defenses: Safe Mode Boot	
Credential access	T1555.003: Credentials from Password Stores: Credentials from Web Browsers	T1552 : Unsecured Credentials		Mimikatz MiniDump
Discovery	T1046: Network Service Discovery	T1135 Network Share Discovery		Advanced IP Scanner NetScan

Lateral Movement	T1021.002: Remote Services: Server Message Block (SMB)/Admin Windows Shares	T1021 - Remote Services: SMB/Windows Admin Shares		Cobalt Strike
Collection	T1560.001: Archive Collected Data: Archive via Utility	T1056: Input Capture		7-zip Winrar MEGAsync FreeFileSync
Command and Control	T1095: Non-Application Layer Protocol T1572: Protocol Tunnelling T1071.001: Application Layer Protocol: Web Protocols T1219: Remote Access Software	T1090: Proxy T1071 : Application Layer Protocol		AnyDesk TeamViewer Plink Ligolo ThunderShell
Exfiltration	T1567: Exfiltration Over Web Service	T1030: Data Transfer Size Limits T1048 - Exfiltration Over Alternative Protocol		
Impact	T1486: Data Encrypted for Impact T1490: Inhibit System Recovery T1491.001: Defacement: Internal Defacement T1489: Service Stop	T1486: Data Encrypted for Impact T1490: Inhibit System Recovery T1489: Service Stop	T1486: Data Encrypted for Impact T1490: Inhibit System Recovery	

All ransomware groups rely heavily on encryption for their operations. They need to ensure that their chosen encryption method is resistant to brute-force attacks and difficult to break. This allows them to achieve T1486: Data Encrypted for Impact.

LockBit uses AES and ECC (Curve 25519) [19] encryption algorithms. LockBit’s binary is stored in the Main() function [20] as a base64 string encrypted using AES. Since the code itself is protected through encryption, it is able dodge malware detection and analysis. It can also elude signature-based detections as the encryption may vary depending on the cryptographic key used. This allows Lockbit to evade Endpoint Detection & Response (EDR) and Anti-Virus (AV) scans.

MedusaLocker uses both the AES and RSA algorithms [21]. AES256 is used to lock the victim’s files, creating a unique AES encryption key in the process. An embedded RSA key will proceed to encrypt said AES key, resulting in the ciphertext. Due to the adoption of a proper RSA algorithm, decryption of the AES key is practically impossible without the corresponding private key. As such, the private key must be obtained from the attackers to perform decryption.

Play is the first group to use an intermittent encryption technique [22]. Intermittent encryption is a technique that encrypts every other 0x100000 byte chunk in the file. The resultant file consists of null characters. This makes the encrypted and non-encrypted chunks visually identical. With this unique technique, Play can evade systems that use static analysis to detect ransomware infections.

In addition, it is realized that Lockbit uses a larger variety of techniques in comparison to the other groups. This could be why it is more successful than other groups. For example, during the initial access, Medusa only uses External Remote Services and Phishing, while Lockbit uses drive-by-compromise, exploiting public-facing applications and valid accounts as additional techniques as well.

Furthermore, Lockbit removes itself from the system through T1070.004, to prevent further detection. This could potentially allow it to stay longer within the victim’s systems [10].

Despite Lockbit having more techniques than the other groups, other factors could have helped it become the most successful. Firstly, Lockbit uses their malware as a Ransomware-as-a-Service (RaaS). Other attackers can choose to purchase this service and/or become an affiliate of the ransomware group. This provides more and more attackers the ability to readily launch attacks without the need to develop their own tools, simply by leveraging on other ransomware group’s expertise and notoriety. With more attackers using the RaaS, it is likely that more attacks occur and a larger proportion of them are successful.

We could consider the example of Medusa. It has much fewer techniques in their TTP as compared to Lockbit or Play. Yet, it was able to conduct more than 50 attacks from January to August 2023. This could be due to Medusa selling their MedusaLocker as a RaaS [22]. With higher adoption rate, more attacks will be accredited to Medusa.

However, being an RaaS or simply having more techniques may not help a ransomware group to become the most successful. The reasonings made in this report have been based off of the five ransomware groups that the team scrapped. In reality, there may be several factors other than TTP, that affect the success of a group. These factors could include the effectiveness of the tools and techniques, the skills of the actors, the susceptibility of the companies etc.

6 Q4: Which Industries Are More Prone To Ransomware Threats? Why?[5 Marks]

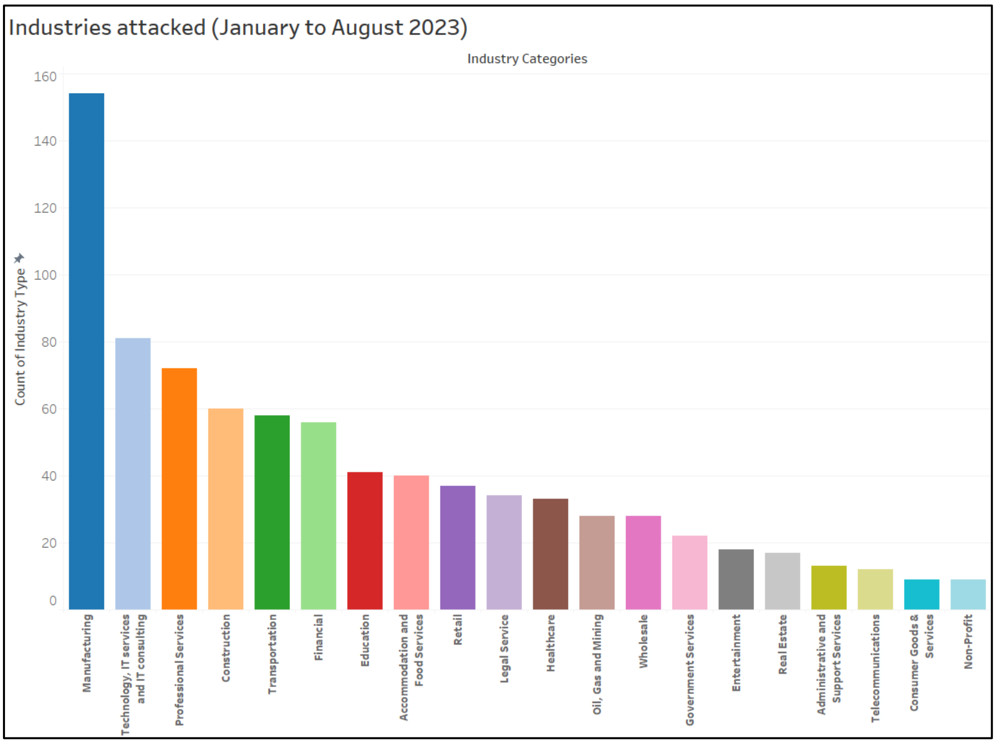


Figure 7: Top 20 Industries Attacked

Based on the graph shown above, the top five industries that are prone to ransomware threats are as follows:

<u>Manufacturing</u>

The manufacturing industry is one of the key industries in the secondary sector as it plays an important role in the supply chain and logistics management. Several other industries heavily rely on the manufacturing industry for raw materials, components, or finished products for their core businesses. Various B2B (Business-to-Business) companies within the secondary sector may also rely on the manufacturing industry for their core operations. In such a situation if organisations belonging to the manufacturing industry fall a victim to ransomware threats, all their plant operations and production lines will be disrupted. Recovery from the same will take a significant amount of time as the core work is being done physically at the plant location. Consequently, important deadlines and product deliveries must be pushed back as well [45].

Overall, targeting the manufacturing industry would mean targeting their suppliers and customers indirectly, thus sabotaging the global supply chain and economy. This would make the industry more likely to paying a ransom as they cannot afford any disruption in operations.

Technology, IT Services, and IT consulting

Organizations belonging to this industry are heavily dependent on their systems and data to provide services. These industries usually possess extremely crucial data such as customer information, intellectual property, and critical infrastructure. Another important reason could be that the companies in this industry typically have a complex and interconnected network. It would not be wrong to claim that the attack surface is directly proportional to the number of endpoint systems and the complexity of the network design, as it opens more potential vulnerabilities for the attackers to exploit.

Professional Services

This industry includes professional services firms, such as law firms, accounting firms, consultancy agencies, that handle extremely sensitive and valuable data of their clients. Client trust and confidentiality are the foundation of this industry, and once that is compromised with, it is very hard for the organisation to recover from the reputational damage caused. Furthermore, these companies rely on their IT systems and data to deliver services to their clients. Any disruption or loss of data can have a severe impact on their operations, thus making them more likely to pay a ransom to overcome downtime.

Construction

Firstly, the construction industry has valuable data and connectivity. Construction, categorized within the secondary sector, handles a significant amount of valuable data, such as architectural plans, blueprints, financial records, employee information, and project details. It supplies raw materials, components, and equipment to tertiary sectors such as healthcare, education, and financial services. Any disruption to the construction sector through ransomware can lead to disruptions in the supply chain, resulting in shortages and elevated costs for businesses operating in the tertiary sector [45, 46].

Additionally, threat actors know that the construction industry has a lack of regulations and lags in data security and privacy initiatives. This is mainly because this industry, to date, avoided heavy regulation in data security and privacy laws. The limited regulation and guidance in the construction industry may have contributed to less focus on cyber security than in other industries, allowing it to be more susceptible to threat actors.

Lastly, the lack of resources is also a reason why the construction industry is targeted. The supply chain of construction projects is mostly composed of small and medium-sized enterprises (SMEs), which generally do not devote sufficient resources to IT and security.

By looking closer at the data obtained, it is realized that some of these construction companies have big clients. For example, Play targeted the Jacobson Company in the U.S. This company may seem insignificant at first. However, on further investigation it is found that their clients include Morgan Stanley and Goldman Sachs. If Jacobson’s client data is stolen, attackers can get important client information which could help in launching more ransomware attacks against bigger companies who have much larger pockets.

Transport

Transport is a key sector of our economy. It includes aviation, maritime, railway, and road transport industries. This sector mainly is targeted is due to the ongoing digital transformation in the transport sector. The increased connectivity between IT and OT networks and the transportation sector has increased the urgency to pay ransom to avoid any critical business and social impact. Both cybercriminals and state sponsored threat actors are focused on targeting the transport industry [47].

Cybercriminals are the main actors responsible for attacks on the transport sector and all its sectors. The transportation sector is an enticing target for cybercriminals due to its potential for financial gain. Customer data is seen as a valuable commodity, and the sector holds proprietary information critical to the functioning of supply chains.

7 Q5: 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. [5 Marks]

Attackers often target the more valuable data of a company. As companies do not want this data to be leaked, they will be more willing to pay the ransom attacker's demand. It is important to note that although the primary goal of most ransomware attacks is to extort money from the victim, selling the stolen files is also one of the potential way for attackers to profit from their illicit activities.

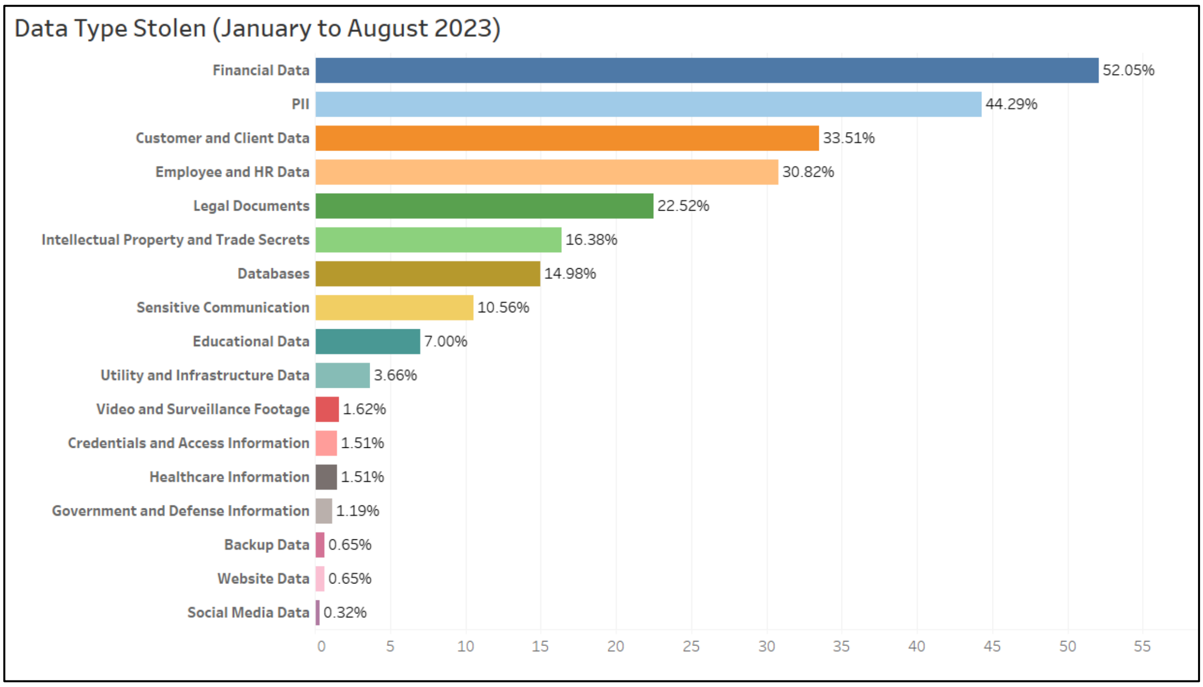


Figure 8: Data Types Stolen across all industries

Out of all the attacks, 52.05% of the victims have their financial data stolen and 44.29% of the victims have their personal identifiable information (PII) stolen. This result is closely followed by Customer and Client Data with 33.51% and Employee and HR data being 30.82%. Legal document is the 5th most common data stolen, at 22.52%.

Threat actors target financial data the most, followed by personal identifiable information (PII).

Financial data are of highest value to a company and thus most often stolen. Firstly, there are laws that prevents unauthorized disclosure of financial data such as the Financial Services Modernization Act of 1999 in the United States. [23] Companies that leak sensitive financial data will lead to financial or even criminal penalty, causing companies to fall into a state of financial distress. Secondly, if financial data such as credit card information is stolen, cybercriminals can commit fraud or steal directly from the victim, resulting in huge financial loss of the victim. The company's standing in the industry might be compromised and in serious cases, result in the bankruptcy of a company. Therefore, financial data is deemed as the most valuable asset belonging to a company due to its direct implication to a company's financial health and stability.

In rare situations, attackers will be able to have access to a company's balance sheet through its financial data. They will then use the revenue streams and cash flow of the company to determine an appropriate ransom amount. This methodology was inferred from the Colonial Pipeline Ransomware Attack in 2021. [24]

PII is also protected by law such as Personal Data Protection Act (PDPA) in Singapore. [25] As companies are bounded by law to keep PII confidential, there will be legal implications if companies leak this information. Moreover, reputation is inherently important to a company and can impact its success and longevity. Hence, PII are a very valuable asset to a company for it to both maintain its legality and reputation.

The immediate economic implications that stolen financial data brings about greatly outweighs the indirect impacts brought about by stolen PII. For example, outflow of financials of a company can directly cause the company to suffer financial hardship and eventually result in bankruptcy. This is a more serious consequence than reputational loss brought about by PII. Therefore, financial data is the most valuable asset of most companies.

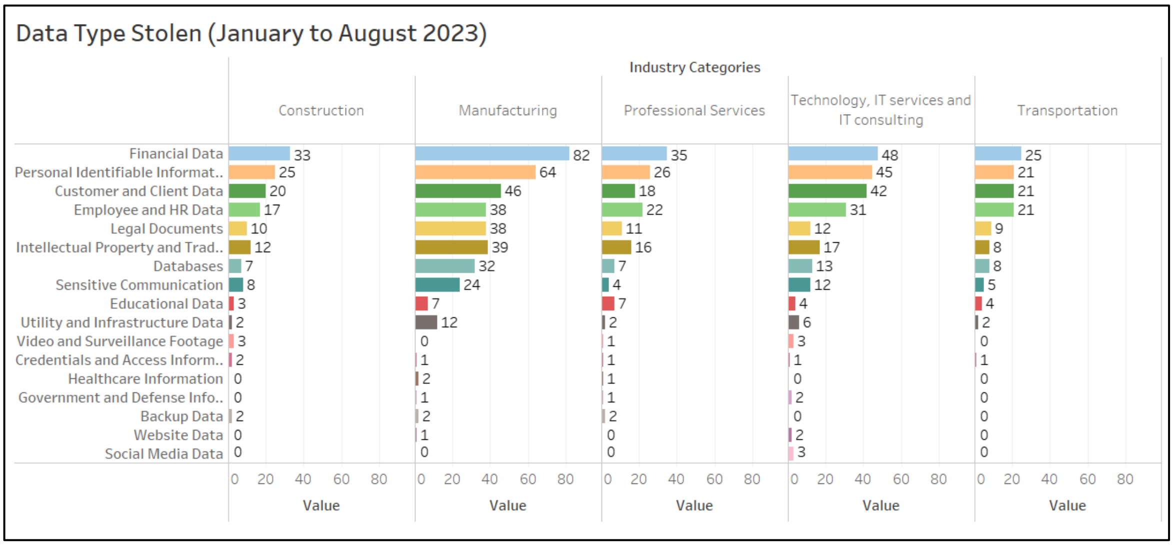


Figure 9: Data Types Stolen across Top 5 industries

In general, the data targeted in the top 5 industries follows a similar trend as above.

The manufacturing industry has a higher number of Utilities and Infrastructure data targeted as compared to educational data. Manufacturing involves the transformation of raw materials into final products using tools, human labour, machinery, and chemical processing [26] and educational data may encompass information related to the R&D activities of companies. Given the manufacturing industry's substantial dependence on its tools and machinery as compared to R&D efforts, encrypting them in a ransomware attack will cripple the operations of the company. Hence, this enables attackers to demand a higher ransom.

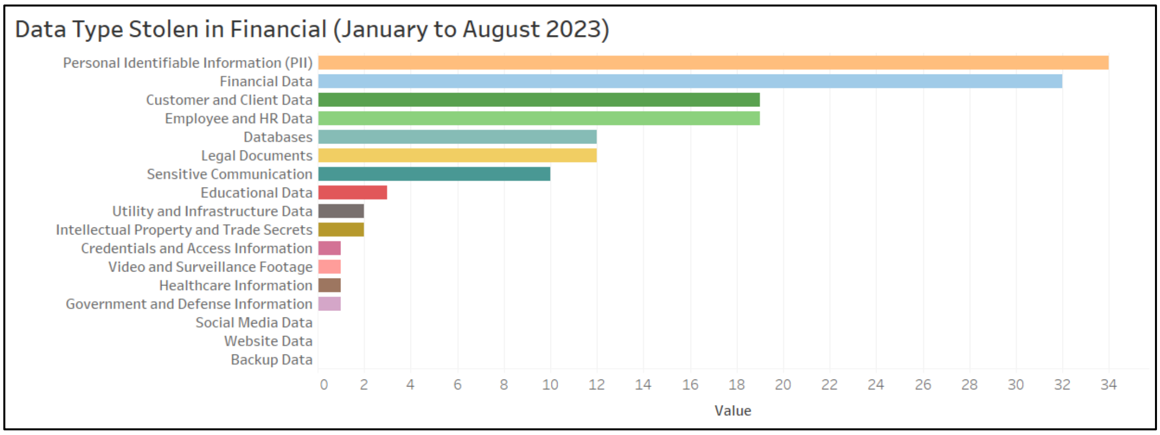


Figure 10: Data Types Stolen in Financial industry

In the Financial industry, Personal Identifiable Information (PII) is more commonly targeted by threat actors than financial data. In the financial industry, which is a service-oriented industry, customers expect their data to be protected. These industries often serve high-net worth or high-profile people. If the PII of these customers are leaked, it will greatly erode the trust of customers and damage the reputation of financial institutions. In comparison, while financial data like credit card numbers can lead to immediate financial losses when leaked, its impact is often shorter-term as compared to PII leaks. Financial institutions can often reverse fraudulent transactions and issue new cards or account numbers.

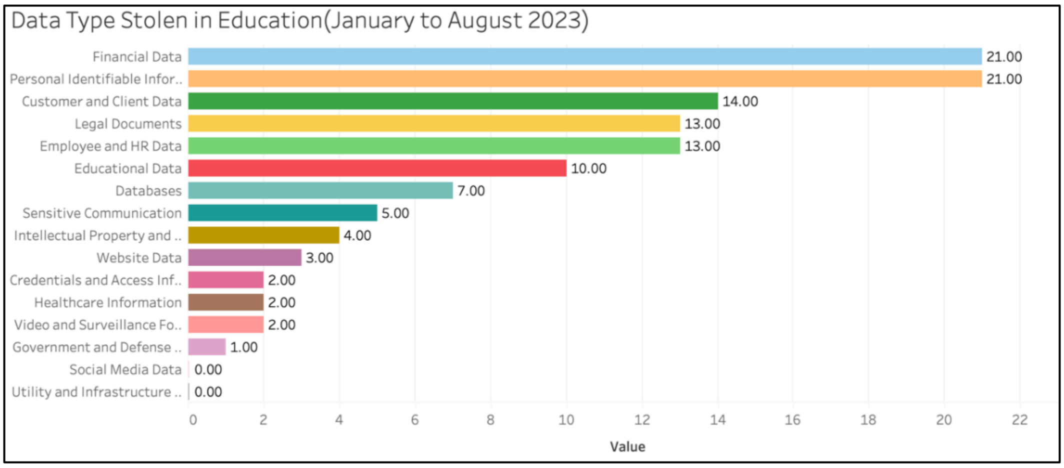


Figure 11: Data Types Stolen in Education industry

In the education industry, Personal Identifiable Information (PII) and financial data is more commonly targeted by threat actors than educational data. Educational institutions are subjected to various data protection regulations such as the Family Educational Rights and Privacy Act (FERPA) which is a federal law in United States that “prohibits educational institutions from disclosing “personally identifiable information in education records” without the written consent of an eligible student”. [27] Failure to comply with these regulations can result in legal actions, hefty fines and lawsuits to the institution, putting the institution’s financial stability at risk.

While educational data is also important, the legal obligations to protect PII and financial data are often more explicit and heavily regulated in the education industry.

8 Q6: SHARE 3 INTERESTING INSIGHTS YOU OBSERVED [9 MARKS]

8.1 PLAY RANSOMWARE: INDISCRIMINATE OR STATE-SPONSORED?

The reason why Play is in focus in this section is due to the types of information stolen and the impact of the attacks. Additionally, there is a speculation that Play may be linked to the Quantum Ransomware group and/or the Hive Ransomware Group. Quantum is an offshoot from Conti, a Russian-based ransomware group [28, 29]. Hive is suspected to be a Russian-based ransomware-group [30] and was disrupted by the FBI. [13, 14, 31, 32]

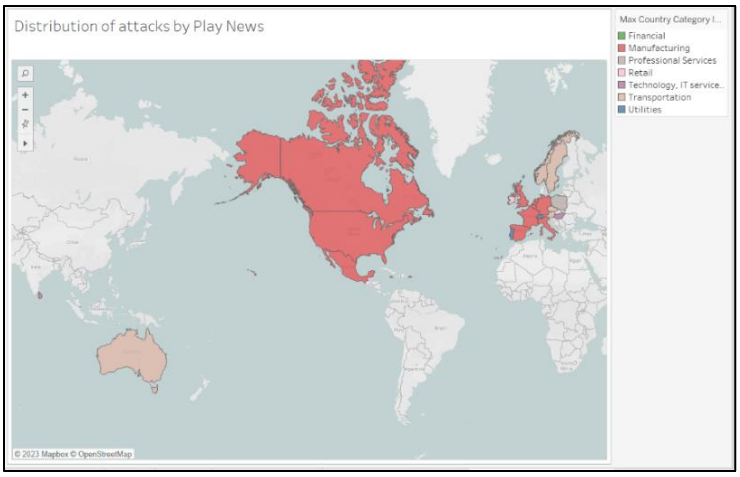


Figure 12: Distribution of attacks by Play News

During the analysis, it was realized that Play concentrated their attacks to United States, Europe, and Australia and in a various number of industries. This indicates that Play might prefer attacking Western Countries. Additionally, their ability to attack various industries suggests that they are probably versatile and efficient in the TTP that they use. Their skill sets may also be more diverse.

In fact, even though Play is not an RaaS like Medusa or Lockbit, it still managed to rank 2nd in terms of number of attacks and has the same variety in the industries attacked like Lockbit.

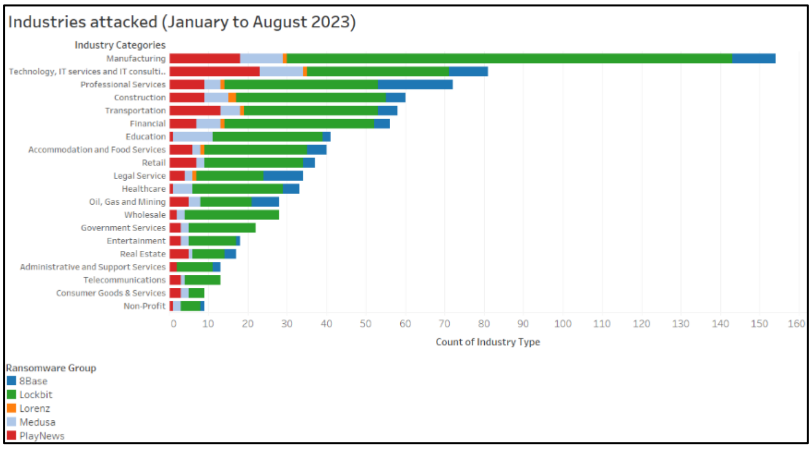
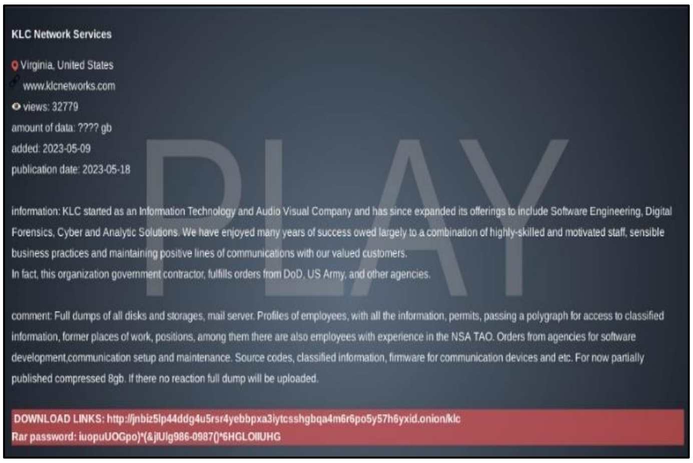


Figure 13: Industries attacked (January to August 2023)

The graph on the left shows Play in red and Lockbit in green.



KLC Network Services

Virginia, United States
www.klcnetworks.com
views: 32779
amount of data: ???? gb
added: 2023-05-09
publication date: 2023-05-18

information: KLC started as an Information Technology and Audio Visual Company and has since expanded its offerings to include Software Engineering, Digital Forensics, Cyber and Analytic Solutions. We have enjoyed many years of success owed largely to a combination of highly-skilled and motivated staff, sensible business practices and maintaining positive lines of communications with our valued customers.
In fact, this organization government contractor, fulfills orders from DoD, US Army, and other agencies.

comment: Full dumps of all disks and storages, mail server. Profiles of employees, with all the information, permits, passing a polygraph for access to classified information, former places of work, positions, among them there are also employees with experience in the NSA TAO. Orders from agencies for software development,communication setup and maintenance. Source codes, classified information, firmware for communication devices and etc. For now partially published compressed 8gb. If there no reaction full dump will be uploaded.

DOWNLOAD LINKS: http://jnbiz5lp44ddg4u5rsr4yebbpxa3iytcsshgbqa4m6r6po5y57h6yxid.onion/klc
Rar password: iuopuUOGpo)*(&jlUlg986-0987()*6HGLOllUHG

Figure 14: KLC Network Services

Looking closer, it is realized that Play managed to attack KLC Network Services and leaked polygraph information that gave access to classified information. KLC is a government contractor and fulfils orders from the Department of Defence (DoD) and the US Army [33].

Given this information, it is likely that the impact of leaking such polygraphs could have severe detrimental effects on the national security of the US.

Looking at primary sources may not give insights into the TTPs used. Hence, further research was done looking into secondary sources. It was found out that Play uses custom made data-gathering tools called Grixba [33, 34, 35]. This evidence suggests that Play consists of is highly skilled hackers to be able to develop proprietary tools.

Moreover, Play managed to steal government information in Switzerland from a consumer services company Xplain. They also targeted a Czech Republican company called Omnipol, a technology company for defence, security, and aeronautical systems and stole secret information although did not specify what it is. Yet, on the complete opposite spectrum, they targeted Pizza73 and stole pizza recipes! The screenshots of these companies from Play's onion site are available in the appendix.

An ACH analysis can be done to analyse the above information:

Hypothesis / Evidence	Play is an indiscriminate ransomware group with no potential links to other groups or countries	Play is linked to Hive and/or Quantum and potentially linked to Russia.
Attacks are concentrated in the western countries (primary source).	-	+
Attacks have leaked confidential and important government information from KLC, Xplain, Omnipol etc. (primary source)	-	+
Attacks have happened on industries that are not related to any government at all such as Pizza73. (primary source)	++	-
Potential Links to Quantum Ransomware group found after they revealed the same watermark dropped by botnets used by Quantum and Conti [14]. (Secondary Source)	-	+

Play uses similar TTP like Hive albeit not entirely the same. (Secondary Source) [14, 32]	-	+
Hive has been known to attack regions like Latin America, Europe and some parts of Asia. (Secondary source). [14] Play has attacked countries in America and Europe (Note: it is only between January to August 2023). (primary source)	-	+

8.2 WHY ARE THE OTHER TWO POWERHOUSES (CHINA & RUSSIA) NOT TARGETED AS MUCH?

Introduction

Ransomware attacks have been on the rise globally, but interestingly, Russia and China have witnessed fewer attacks than might be expected given their technological advancements. This section explores the possible reasons behind this trend.

Ransomware Language Exclusion Mechanisms

Activity Timeline of LockBit

Tracing the evolution of ransomwares provides context to its targeting pattern. ABCD ransomware, the predecessor to LockBit was first observed in September 2019. By January 2020, ransomware under LockBit name made its appearance in Russian-language-based cybercrime forums, indicating its potential origin and the inclination to avoid Russian systems. [11]

LockBit 3.0's Language Check Mechanism

LockBit 3.0, integrates a unique mechanism that checks the system's language before executing its malicious intent. If it identifies languages from a predefined exclusion list, it ceases its operations and leave the system untouched. The exclusion list is extensive and includes languages predominantly spoken in Russia and several Commonwealth of Independent States (CIS). [36] Russia and Tatar are two primary examples. The full list can be found in the appendix.

Geopolitical Considerations

Avoiding Domestic Prosecution

It's probable that ransomware groups avoid targeting their own territories to escape legal repercussions. [1] LockBit's apparent exclusion of Russian and CIS system could support this. Launching cyberattacks within one's own country can attract immediate attention from domestic law enforcement. Prosecution is often swifter and more certain when the crime affects national interests or citizens directly. For example, in many countries, cybercrimes against their own citizens are pursued more aggressively than crimes against foreign nationals.

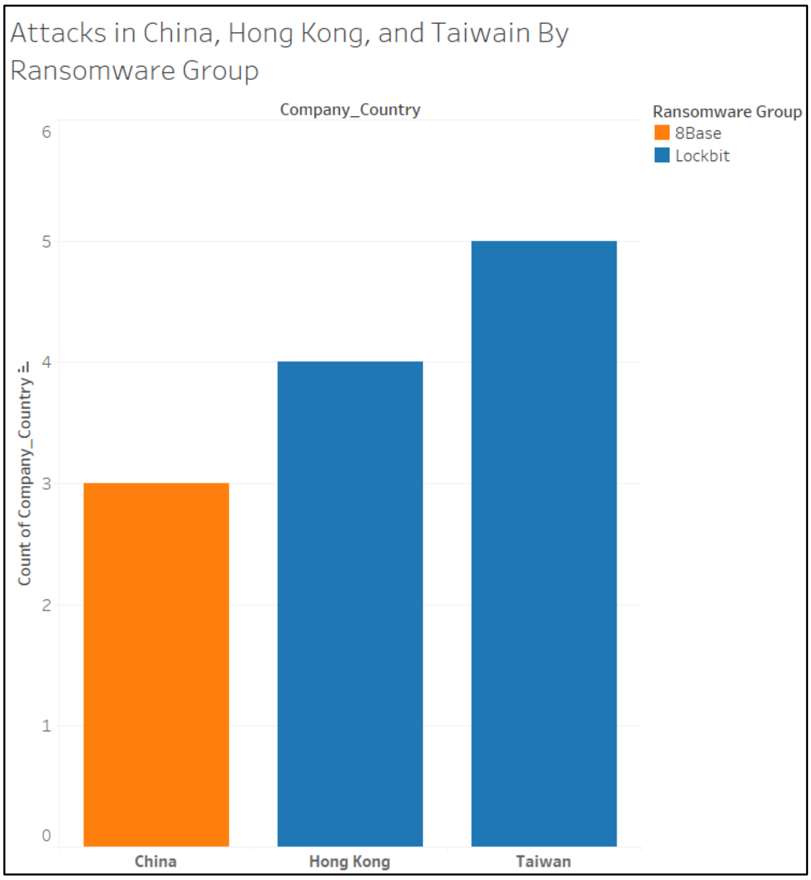


Figure 15: Attacks in China, Hong Kong and Taiwan by Ransomware

China's Situation

While Mainland China has witnessed minimal attacks, its special administrative regions like Hong Kong and Taiwan have been targeted. LockBit recorded attacks in these areas, perhaps exploiting the historical and political intricacies these regions share with Mainland China. Only 8Base, carried out a few attacks within China.

China’s Firewall

China’s formidable digital barrier, the Great Firewall, could play a role in curbing ransomware incidents. Some of the known techniques deployed are destination IP address blocking, URL filtering, DNS poisoning, TCP reset attacks, Deep packet inspection, Fake SSL root certificates, Active probing and many more. [37]
DNS poisoning allows China to use the internet service providers (ISPs) to aid in its censorship efforts by having them block or redirect DNS queries.

Active Probing is used to tackle anti-censorship services such as VPNs and Tor. Chinese authorities use active probing to trace connections back to blocklisted IP addresses.

All public Tor nodes are blocked in China with the anonymity network being partially accessible in China using bridges and pluggable transports. The other means will be to use Shadowsocks, it creates a SOCK55 proxy connection to a server one rents outside of China.

To make matters worse, ransomware groups demand for payment in cryptocurrency which is banned in China.

With such tight egress traffic scrutiny and the inability to access cryptocurrency, ransomware attackers will find it hard to extort victims for ransoms. Hence, staying away is easier than attacking.

Conclusion

Russia and China's low ransomware attack frequency can be attributed to the built-in language checks in ransomwares like LockBit 3.0, the geopolitical strategies of ransomware groups and China’s Great Firewall. While the language checks serve as a technical barrier, the geopolitical considerations offer a layer of protection against potential legal consequences in their home territories.

8.3 ANALYSING RANSOMWARE GROUP ACTIVITY: REAL-WORLD PATTERNS AND TRENDS

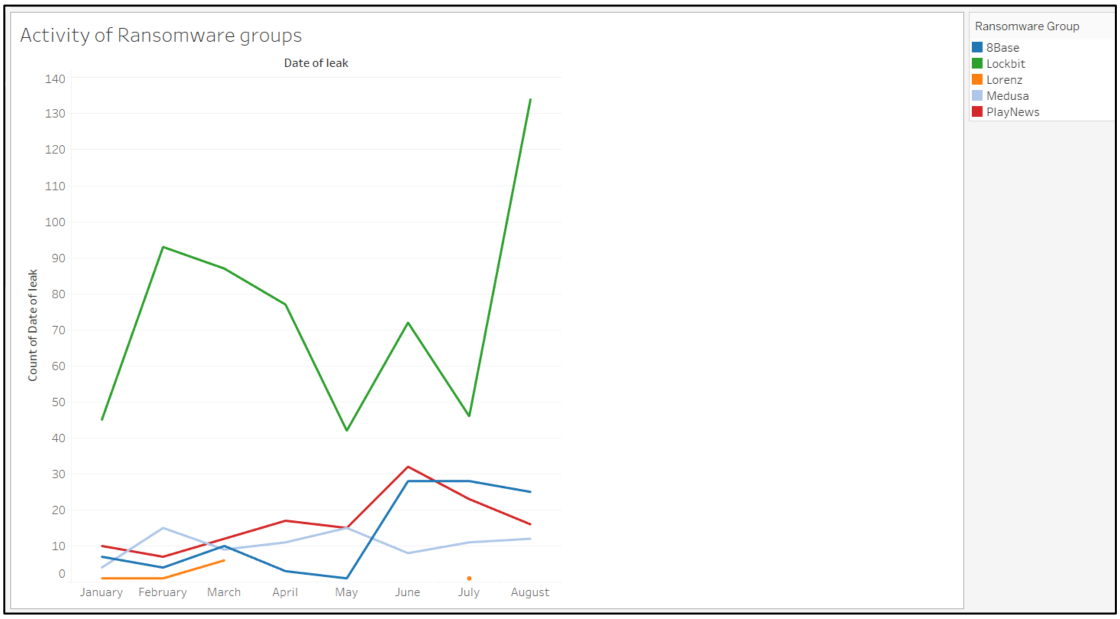


Figure 16: Activity of Ransomware Groups

From the dates of data leaks that we exfiltrated from the ransomware shaming groups, we can see some patterns and possibly attribute them to significant world news.

From late February to May of 2023, there are generally lesser cases compared to the latter half of the year. Particularly, activity of Lockbit and 8Base has dropped significantly throughout the period. The team thinks that this is due to the impacts of the Russian invasion of Ukraine on 24 February 2023. There are two main impacts that could have caused the dip in ransomware group activity.

According to the head of Russia's ministry of digital affairs, around 100,000 IT specialists have left Russia in 2022 [38]. It is not far-fetched to imagine a higher number in 2023 as many more would have been worried about the business outlook especially in the IT security service focused state. Termed as a “tech brain drain”, the team suspect members of Russia and the Commonwealth of Independent States (CIS) within these ransomware shaming groups to be affected negatively by this, causing disruption in their daily lives and careers [39]. Russia's military mobilization of its citizens could have contributed to further displacement too. This has possibly decentralized the organized ransomware group landscape that had existed, causing an overall decrease in ransomware activity.

Due to the close economic relationship between Russia and the CIS, where Ukraine is a part of before the war, geopolitical tensions from the war have damaged the "brotherhood" between Russian threat actors located in states of the CIS. It is noted that Lockbit has affiliations with Russia and 8Base is suspected to be founded in Moldova, which has left the CIS on 13 May 2023 [40]. There could have been internal instability within the ransomware groups, causing fallouts and thus, less focus on ransomware attacks.

As time went on, the ransomware groups could have regrouped and started more attacks. From the chart, activity started to ramp up from May to August. The success of these attacks could have been attributed to the MOVEit campaign led by Cl0p, which took advantage of the zero-day vulnerability, CVE-2023-34362 and CVE-2023-35036, to deal the most ransomware attacks from June to July, overtaking Lockbit [41]. Nearly 1,000 organizations and 60 million individuals are reportedly impacted by the MOVEit campaign. It is possible the other ransomware groups used this vulnerability to attack other companies too, leading to the huge spike in attacks. Some notable companies that used the MOVEit file transfer software include US Department of Energy, Shell, Ernst & Young, and many more.

9 Q7: Share lessons learnt, what were your struggles in executing the project and how did you overcome them? [1 Mark]

The first struggle we faced is that data stolen by the ransomware groups are large in amount and diversity. To answer some of the above questions, the team had to understand the data we were working with. While some of the ransomware groups do give useful descriptions as to what kind of data is stolen, most are given vague statements or no description at all. Hence, the team needed to deep dive into data directories where various types of data could exist, such as database files .db or excel sheets .xlsx. To make things worse, due to the reach of these ransomware groups, there is often a language barrier when facing files in another language. Accuracy in classification of data types is bound to be affected by human error and biasness.

To overcome this to the best of our ability, the team looked at news reports or articles of the data leak along with data overviews from the ransomware groups to lessen the amount of data exploring yet still get an accurate representation of the data stolen. We also formed our own data taxonomy by standardizing the data types early and their corresponding characteristics — a fixed set of questions to ask when faced with a piece of data before classifying it. For example, the team will ask the following questions when faced with potential financial data:

- Are there credit card numbers of the company/client/customer?
- Are there bank account information of the company/client/customer?
- Are there bank transactions/transfers?

For documents that are in a foreign language, the team used the tool Google Translate on our phones to scan documents and get the translation easily, making classification of data possible even across languages.

From this struggle, the team learnt the difficulty of big data handling and the importance of establishing a robust data classification system that allows for easy identification and categorization. This not only streamlined our data handling and retrieval but also saved time resolving any confusions within the team. Even so, when faced with terabytes of data to classify, the team lamented with regret that we can only do so to a reasonable degree.

Another struggle the team faced is the volatility of the dark web. As the data obtained would be of a higher quality if popular ransomware shaming groups were to be analysed, the team initially found ALPHV to be one of the suitable candidates as it had a lot of company data stolen within the year that could value add to the overall data scraped. However, halfway through the process of scraping the ALPHV site, it went offline and never went back online on the same onion address till the submission of this report.

To overcome this unprecedented situation, the team had to resort to less popular ransomware shaming groups to make up for the loss of ALPHV. The team scraped beyond the recommended number of ransomware shaming groups to reach an amount of data satisfying statistical significance. Scraping additional ransomware shaming sites actually increased the diversity of our data, increasing the representative sample of the companies that fell victim to ransomware. Reversing this incident into an opportunity, the team is able to come up with more meaningful results.

From this struggle, the team learnt the unreliability of the dark web and the ability to adapt to changing conditions, especially when concerning onion sites. Ransomware shaming sites often operate in a grey area of legality and ethics, and with their lack of consistency, they often go offline without notice and might change their site address. For the sake of educational and research value of this project, the team learnt to deal with the risks when interacting with such sites by making compromises.

10 REFERENCES

[1] “Kaspersky,” 1 January 2023. [Online]. Available: https://www.kaspersky.com/resource-center/threats/lockbit-ransomware.

[2] B. Sussman and C. Mok, “BlackBerry Blog,” 02 September 2023. [Online]. Available: https://blogs.blackberry.com/en/2023/02/top-10-countries-most-targeted-by-cyberattacks-2023-report.

[3] Blackberry, “Blackberry,” 2022. [Online]. Available: https://www.blackberry.com/content/dam/bbcomv4/global/pdf/0408-Threat-ReportV17.pdf. [Accessed 20 October 2023].

[4] worldometers, “GDP by Country,” worldometers, 2023. [Online]. Available: https://www.worldometers.info/gdp/gdp-by-country/. [Accessed 10 October 2023].

[5] worldometers, “Countries in the world by population (2023),” 2023. [Online]. Available: https://www.worldometers.info/world-population/population-by-country/. [Accessed 20 October 2023].

[6] statista, “Countries with the highest internet penetration rate as of July 2023,” 2023. [Online]. Available: https://www.statista.com/statistics/227082/countries-with-the-highest-internet-penetration-rate/. [Accessed 20 October 2023].

[7] Amer Elsad; JR Gumarin ;Abigail Barr, “LockBit 2.0: How This RaaS Operates and How to Protect Against It,” unit42 Palo Atlo, 9 June 2022. [Online]. Available: https://unit42.paloaltonetworks.com/lockbit-2-ransomware/#lockbit-3. [Accessed 22 October 2023].

[8] Flashpoint, “LockBit Ransomware: Inside the World’s Most Active Ransomware Group,” 20 July 2023. [Online]. Available: https://flashpoint.io/blog/lockbit/. [Accessed 22 October 2023].

[9] Joint Cybersecurity Advisory, “Understanding Ransomware Threat Actors: LockBit PDF,” Joint Cybersecurity Advisory, 14 June 2023. [Online]. Available: https://www.cisa.gov/sites/default/files/2023-06/aa23-165a_understanding_TA_LockBit_0.pdf. [Accessed 22 October 2023].

[10] Seguranca Informatica, “Malware analysis: Details on LockBit ransomware,” 5 October 2021. [Online]. Available: https://seguranca-informatica.pt/malware-analysis-details-on-lockbit-ransomware/#.YwKahHbMIQ8.

[11] “#StopRansomware: LockBit 3.0,” 16 March 2023. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a. [Accessed 22 October 2023].

[12] CISA, “Understanding Ransomware Threat Actors: LockBit CISA report,” 14 June 2023. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a. [Accessed 22 October 2023].

[13] Avertium, “AN IN-DEPTH LOOK AT PLAY RANSOMWARE,” Avertium, 4 January 2023. [Online]. Available: https://explore.avertium.com/resource/an-in-depth-look-at-play-ransomware. [Accessed 22 October 2023].

[14] D. O. Ladores, L. Silva, S. Burden, J. Agcaoili, I. N. Chavez, I. Kenefick, I. N. Gonzalez and P. Pajares, “Play Ransomware's Attack Playbook Similar to that of Hive, Nokoyawa,” trendmicro, 06 September 2022. [Online]. Available: https://www.trendmicro.com/en_us/research/22/i/play-ransomware-s-attack-playbook-unmasks-it-as-another-hive-aff.html. [Accessed 22 October 2023].

[15] Trend Micro, “Ransomware Spotlight Play,” Trend Micro, 21 July 2023. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-play. [Accessed 22 October 2023].

[16] H. Montini, L. Ponpeu and B. Glushko, “How to Recover From Play Ransomware Attack,” salvagedata, 11 May 2023. [Online]. Available: https://www.salvagedata.com/play-ransomware/. [Accessed 22 October 2023].

[17] S. Imano and J. Slaughter, “Ransomware Roundup – Play,” FORTIGUARD LABS THREAT RESEARCH, 22 December 2022. [Online]. Available: https://www.fortinet.com/blog/threat-research/ransomware-roundup-play-ransomware. [Accessed 22 October 2023].

[18] CISA, "#StopRansomware: MedusaLocker," CISA, 11 August 2022. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-181a. [Accessed 22 October 2023].

[19] "VMWare," 28 October 2022. [Online]. Available: https://blogs.vmware.com/security/2022/10/esxi-targeting-ransomware-tactics-and-techniques-part-2.html.

[20] "Seguranca Informatica," 2023. [Online]. Available: https://seguranca-informatica.pt/malware-analysis-details-on-lockbit-ransomware/#.YwKahHbMIQ8.

[21] "Seqrite," 16 October 2023. [Online]. Available: https://www.seqrite.com/blog/medusalocker-ransomware-an-in-depth-technical-analysis-and-prevention-strategies/.

[22] SOCRadar, "Dark Web Profile: Medusa Ransomware (MedusaLocker)," SOCRadar, 5 September 2023. [Online]. Available: https://socradar.io/dark-web-profile-medusa-ransomware-medusalocker/. [Accessed 22 October 2023].

[23] "Federak Reserve History," 22 November 2013. [Online]. Available: https://www.federalreservehistory.org/essays/gramm-leach-bliley-act.

[24] S. M. Kerner, "TechTarget," 26 April 2022. [Online]. Available: https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know.

[25] "Personal Data Protection Commission Singapore," 1 February 2021. [Online]. Available: https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act.

[26] W. Kenton, "Manufacturing: Definition, Types, Exampleds, and Use as Indicator," Investopedia, 16 September 2022. [Online]. Available: https://www.investopedia.com/terms/m/manufacturing.asp#:~:text=The%20term%20manufacturing%20refers%20to,of%20the%20raw%20materials%20used.. [Accessed 16 October 2023].

[27] "U.S. Department of Education," 25 August 2021. [Online]. Available: https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html.

[28] Avertium, "AN IN-DEPTH LOOK AT QUANTUM RANSOMWARE," Avertium, 16 August 2022. [Online]. Available: https://explore.avertium.com/resource/an-in-depth-look-at-quantum-ransomware. [Accessed 22 October 2023].

[29] M. BURGESS, "Leaked Ransomware Docs Show Conti Helping Putin From the Shadows," Wired, 10 May 2022. [Online]. Available: https://www.wired.com/story/conti-ransomware-russia/. [Accessed 22 October 2023].

[30] U.S Department of the Treasury, "Treasury Sanctions Russian Ransomware Actor Complicit in Attacks on Police and U.S. Critical Infrastructure," U.S Department of the Treasury, 16 May 2023. [Online]. Available: https://home.treasury.gov/news/press-releases/jy1486. [Accessed 22 October 2023].

[31] threatshub, "Play Ransomware's Attack Playbook Similar to that of Hive, Nokoyawa," threatshub, 06 September 2022. [Online]. Available: https://www.threatshub.org/blog/play-ransomwares-attack-playbook-similar-to-that-of-hive-nokoyawa/. [Accessed 22 October 2023].

[32] CISA, "#StopRansomware: Hive Ransomware," Cybersecurity & Infrastructure Security Agency, 25 November 2022. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-321a. [Accessed 22 October 2023].

[33] A. Khaitan, "Play Ransomware Gang Behind KLC Network Services Cyber Attack," The Cyber Express, 9 May 2023. [Online]. Available: https://thecyberexpress.com/klc-network-services-cyber-attack/. [Accessed 22 October 2023].

[34] B. Toulas, "Play ransomware gang uses custom Shadow Volume Copy data-theft tool," Bleeping Computer, 19 April 2023. [Online]. Available: https://www.bleepingcomputer.com/news/security/play-ransomware-gang-uses-custom-shadow-volume-copy-data-theft-tool/. [Accessed 22 October 2023].

[35] Symantec by Broadcom, "Play Ransomware Group Using New Custom Data-Gathering Tools," Symantec by Broadcom, 19 April 2023. [Online]. Available: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/play-ransomware-volume-shadow-copy. [Accessed 22 October 2023].

[36] "Trend Micro," 25 July 2022. [Online]. Available: https://www.trendmicro.com/en_us/research/22/g/lockbit-ransomware-group-augments-its-latest-variant--lockbit-3-.html.

[37] ProtonVPN, 3 February 2023. [Online]. Available: https://protonvpn.com/blog/great-firewall-china/.

[38] A. &. D. P. Marrow, “Exclusive: Fear of tech 'brain drain' prevents Russia from seizing yandex for now, sources say,” Reuters, 10 August 2023. [Online]. Available: https://www.reuters.com/technology/fear-tech-brain-drain-prevents-russia-seizing-yandex-now-sources-2023-08-10/. [Accessed 22 October 2023].

[39] “Russia's war against Ukraine disrupts the Cybercriminal Ecosystem,” Recorded Future, [Online]. Available: https://www.recordedfuture.com/russias-war-against-ukraine-disrupts-cybercriminal-ecosystem. [Accessed 22 October 2023].

[40] R. September, “Krebs on Security,” 18 September 2023. [Online]. Available: https://krebsonsecurity.com/2023/09/whos-behind-the-8base-ransomware-website/. [Accessed 22 October 2023].

[41] T. I. Team, “Malwarebytes,” [Online]. Available: https://www.malwarebytes.com/blog/threat-intelligence/2023/07/ransomware-review-july-2023. [Accessed 22 October 2023].

[42] Cybersecurity & Infrastructure Security Agency, “#StopRansomware: Hive Ransomware,” Cybersecurity & Infrastructure Security Agency, 25 November 2022. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-321a. [Accessed 22 October 2022].

[43] [Online]. Available: https://www.trendmicro.com/en_us/research/22/g/lockbit-ransomware-group-augments-its-latest-variant--lockbit-3-.html.

[44] [Online]. Available: https://www.trendmicro.com/en_us/research/22/g/lockbit-ransomware-group-augments-its-latest-variant--lockbit-3-.html.

[45] S. Chhetri and S. Faezi, “Manufacturing Supply Chain and product lifecycle security in the era of industry 4.0, vol 2, issue 1,” *Journal of Hardware and Systems Security,* pp. 51-68, 2017.

[46] B. García de Soto, Ž. Turk, A. Maciel and M. S. Sonkor, “Understanding the significance of cybersecurity in the construction industry: Survey findings,” *Journal of Construction Engineering and Management,* vol. 148, no. 9, 2022.

[47] “ENISA Transport Threat Landscape: Transport Sector,” 2023.

11 Appendix

11.1 Appendix A: Data type Categories

1. Personal Identifiable Information (PII)
2. Financial Data
3. Healthcare Information
4. Employee and HR Data
5. Intellectual Property and Trade Secrets
6. Customer and Client Data
7. Legal Documents
8. Government and Defence Information
9. Educational Data
10. Credentials and Access Information
11. Databases
12. Website Data
13. Backup Data
14. Video and Surveillance Footage
15. Social Media Data
16. Utility and Infrastructure Data
17. Sensitive Communication

11.2 Appendix B: Industry Types Categories

1. Manufacturing
2. Accommodation and Food Services
3. Professional Services
4. Government Services
5. Administrative and Support Services
6. Agriculture
7. Retail
8. Financial
9. Automotive
10. Research
11. Technology, IT services and IT consulting
12. Construction
13. Business Supplies & Equipment
14. Real Estate
15. Consumer Goods & Services
16. Dentistry
17. Education
18. Utilities
19. Entertainment
20. Equipment Rental Services
21. Farming
22. Furniture
23. Healthcare
24. Industrial Automation
25. Job Recruitment
26. Landscaping Services
27. Legal Services
28. Libraries
29. Management Company
30. Maritime
31. Mechanical or Industrial Engineering
32. Medical Device
33. Oil, Gas and Mining
34. Newspaper Publishing
35. Non-Profit
36. Public Administration
37. Telecommunications
38. Tourism
39. Travel
40. Wholesale

11.3 Appendix C: Onion Sites

Lockbit:

```
http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion/
```

8Base:

```
http://basemmnnqwxevlymli5bs36o5ynti55xojzvn246spahniugwkff2pad.onion/
```

Medusa:

```
http://medusaxko7jxtrojdkxo66j7ck4q5tgktf7uqsqyfry4ebnxlcbkccyd.onion/
```

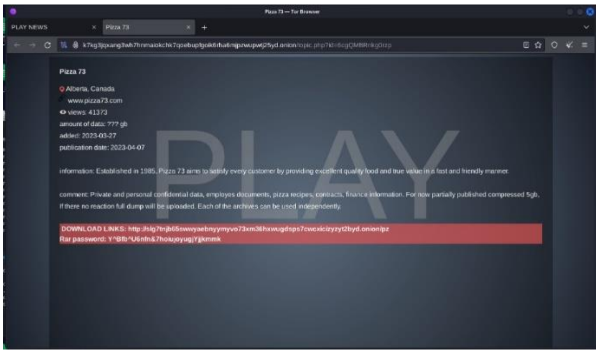
PLAY:

```
http://k7kg3jqxang3wh7hnmaiokchk7qoebupfgoik6rha6mjpzwupwtj25yd.onion/
```

Lorenz:

```
http://lorenzmlwpzgxq736jzseuterytjueszsvznuibanxomlpkyxk6ksoyd.onion/
```

11.4 Appendix d: PLAY


Pizza 73 — Tor Browser
PLAY NEWS
Pizza 73
k7kg3jqxang3wh7hnmaiokchk7qoebupfgoik6rha6mjpzwupwtj25yd.onion/topic.php?id=6cgQMBRnkg0rzp
PLAY

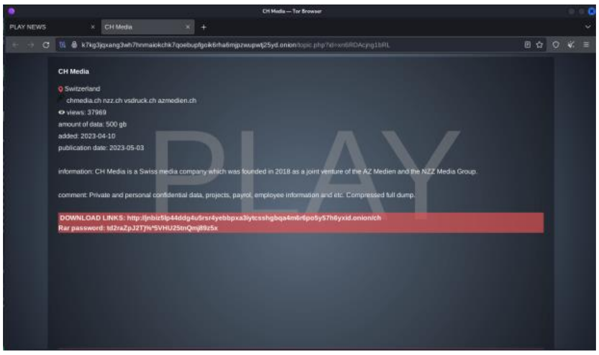
Pizza 73

Alberta, Canada
www.pizza73.com
views: 41373
amount of data: ??? gb
added: 2023-03-27
publication date: 2023-04-07

information: Established in 1985, Pizza 73 aims to satisfy every customer by providing excellent quality food and true value in a fast and friendly manner.

comment: Private and personal confidential data, employes documents, pizza recipes, contracts, finance information. For now partially published compressed 5gb, if there no reaction full dump will be uploaded. Each of the archives can be used independently.

DOWNLOAD LINKS: http://slg7tnjb65swwyaebnyymyvo73xm36hxwugdsps7cwcxicizyzyt2byd.onion/pz
Rar password: Y^Bfb^U6nfn&7hoiujoyugjYjjkmmk


CH Media — Tor Browser
PLAY NEWS
CH Media
k7kg3jqxang3wh7hnmaiokchk7qoebupfgoik6rha6mjpzwupwtj25yd.onion/topic.php?id=xn6RDAcjng1bRL
PLAY

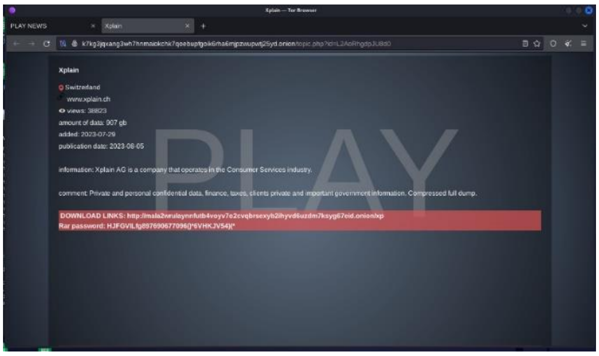
CH Media

Switzerland
chmedia.ch nzz.ch vsdruck.ch azmedien.ch
views: 37969
amount of data: 500 gb
added: 2023-04-10
publication date: 2023-05-03

information: CH Media is a Swiss media company which was founded in 2018 as a joint venture of the AZ Medien and the NZZ Media Group.

comment: Private and personal confidential data, projects, payrol, employee information and etc. Compressed full dump.

DOWNLOAD LINKS: http://jnbiz5lp44ddg4u5rsr4yebbpxa3iytcsshgbqa4m6r6po5y57h6yxid.onion/ch
Rar password: td2raZpJ2Tj%*5VHU25tnQmj89z5x


Xplain — Tor Browser
PLAY NEWS
Xplain
k7kg3jqxang3wh7hnmaiokchk7qoebupfgoik6rha6mjpzwupwtj25yd.onion/topic.php?id=L2AoRhgdpJU8d0
PLAY

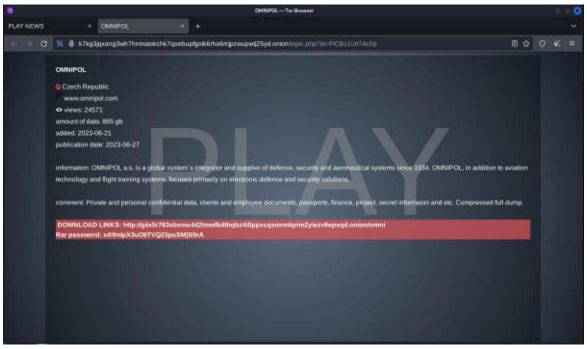
Xplain

Switzerland
www.xplain.ch
views: 38823
amount of data: 907 gb
added: 2023-07-29
publication date: 2023-06-05

information: Xplain AG is a company that operates in the Consumer Services industry.

comment: Private and personal confidential data, finance, taxes, clients private and important government information. Compressed full dump.

DOWNLOAD LINKS: http://mala2wrulaynnfutb4voyv7o2cvqbrsexyb2ihyvd6uzdm7ksyg67eid.onion/xp
Rar password: HJFGVILfg897690677096()*6VHKJV54)(*


OMNIPOL — Tor Browser
PLAY NEWS
OMNIPOL
k7kg3jqxang3wh7hnmaiokchk7qoebupfgoik6rha6mjpzwupwtj25yd.onion/topic.php?id=PtC8u1Ut7Ac0p
PLAY

OMNIPOL

Czech Republic
www.omnipol.com
views: 24571
amount of data: 885 gb
added: 2023-06-21
publication date: 2023-06-27

information: OMNIPOL a.s. is a global system's integrator and supplier of defence, security and aeronautical systems since 1934. OMNIPOL, in addition to aviation technology and flight training systems, focuses primarily on electronic defence and security solutions.

comment: Private and personal confidential data, clients and employee documents, passports, finance, project, secret informaion and etc. Compressed full dump.

DOWNLOAD LINKS: http://giix5r763sbxmu442tmwfb4thqbz4i5ppxcqsmnnlqnm2yiezv6epxqd.onion/omni
Rar password: s4!fmlpX3uOlTVQ23puSMjS5rA

Pizza73(Top Right), CH Media(Top Left), Xplain(Bottom Right), Omnipol(Bottom Left)

11.5 Appendix F: List of language exclusion

1. Arabic (Syria)
2. Armenian (Armenia)
3. Azerbaijani (Cyrillic Azerbaijan)
4. Azerbaijani (Latin Azerbaijan)
5. Belarusian (Belarus)
6. Georgian (Georgia)
7. Kazakh (Kazakhstan)
8. Kyrgyz (Kyrgyzstan)
9. Romanian (Moldova)
10. Russian (Moldova)
11. Russian (Russia)
12. Tajik (Cyrillic Tajikistan)
13. Turkmen (Turkmenistan)
14. Tatar (Russia)
15. Ukranian (Ukraine)
16. Uzbek (Cyrillic Uzbekistan)
17. Uzbek (Latin Uzbekistan)