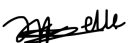






**NANYANG
TECHNOLOGICAL
UNIVERSITY**
SINGAPORE

Analysis of Different Ransomware Sites

CZ 4070 Cyber threat Intelligence
Group Project - Group 8

Sr No	Name	Matric Number	Sign
1	Joelle Chew Ningxi	U2223952D	
2	Darren Lee Jun Rui	U2122668B	Darren
3	Goyal Ananya Surendrakumar	U2023124B	
4	Harikrishnan Vinaya Souraba	U2023893J	Vinaya
5	Jerick Lim Kai Zheng	U2121327C	
6	Caren Tan Xin Yao	U2223431k	Caren
7	Joseph Teo	U2223041J	
8	Tan Jia Hao	U2022443F	

Evaluated by: Yihao Lim

Date Submitted: 14 October 2024

Table of Contents

Table of Contents	2
1. Introduction	3
2. What is the percentage distribution in countries targeted globally?	3
3. Why are some countries more targeted than others?	4
4. Which Ransomware group is the most active? What is so unique about their TTP that makes them so “successful”?	5
4.1 Most Active Ransomware Group	5
4.2 MITRE ATT&CK Framework	5
5. Which Industries Are More Prone To Ransomware Threats? Why?	7
6. 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.	8
7. Share three interesting insights you observed	9
7.1 RansomHub, the “New Kid on the Block”	9
7.2 Humans: the weakest link?	10
7.3 SMEs - the most sought after victim for ransomware groups	11
8. Share lessons learnt, what were your struggles in executing the project and how did you overcome them?	12
9. Conclusion	12
10. Contribution Table	13
11. References	14
11. Appendix	17

1. Introduction

This report analyses active ransomware groups, focusing on attack trends by location, industry, TTPs, and data exploitation. The four identified groups are Qilin, BianLian, RansomHub, and Play, with data collected from ransomware websites to meet intelligence needs.

Intelligence Requirement	Collection Requirement	Data source
Victim Name & Details	Company_Name	Ransomware site
	Website	Web scraping
Which Industries Are More Prone To Ransomware Threats? Why?	Industry	Web scraping
	Company size	Web scraping
What is the percentage distribution in countries targeted globally? Why are some countries targeted more than others?	HQ	Web scraping
	Country	Web scraping
Which Ransomware group is the most active? What is so unique about their TTP that makes them so "successful"? 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.	Date_Victimimized	Ransomware site
	NumViews (of threat)	Ransomware site
	RansomDataSize	Ransomware site
	RansomDataType	Ransomware site
	Ransomware_Grp	Ransomware site

2. What is the percentage distribution in countries targeted globally?

Figure 1 shows the distribution of attacks around the world that was initiated by the 4 ransomware groups stated above. The **United States** and **Canada** have the highest percentage distribution, with the US receiving 57.79% of attacks and Canada 5.72%. The chosen ransomware groups have also targeted other regions in South America, Asia-Pacific, and Europe. However, Russia and the majority of Africa have not been attacked by these groups.

Distribution of Attacks Globally

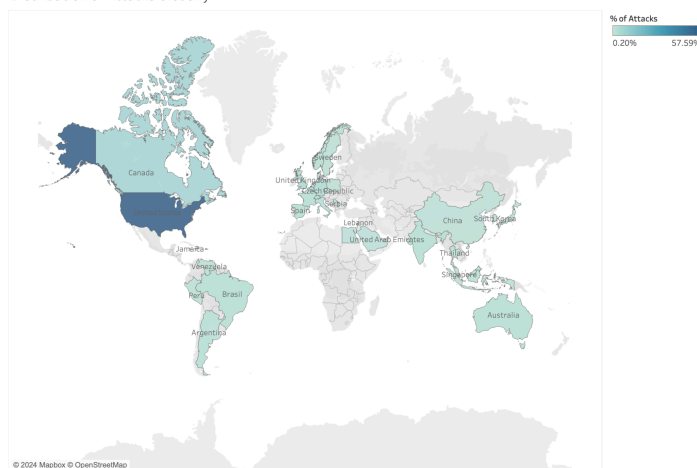


Figure 1: Map of the Distribution of Attacks

Distribution of Top 10 Countries

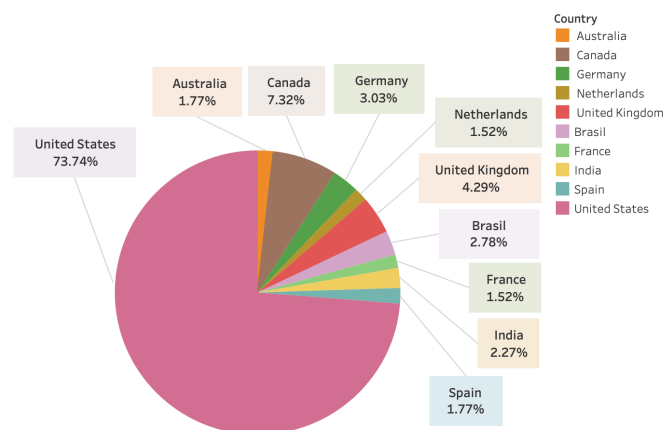


Figure 2: Percentage Distribution of Top 10 Countries

The pie chart above illustrates the top 10 countries that have been targeted. Based on this statistic, we can infer that the countries in North America, Europe, and Australia are the most susceptible to ransomware attacks. More specifically, the US, Canada, UK, and Germany have been most affected.

3. Why are some countries more targeted than others?

Attack Frequency of Top 10 Countries

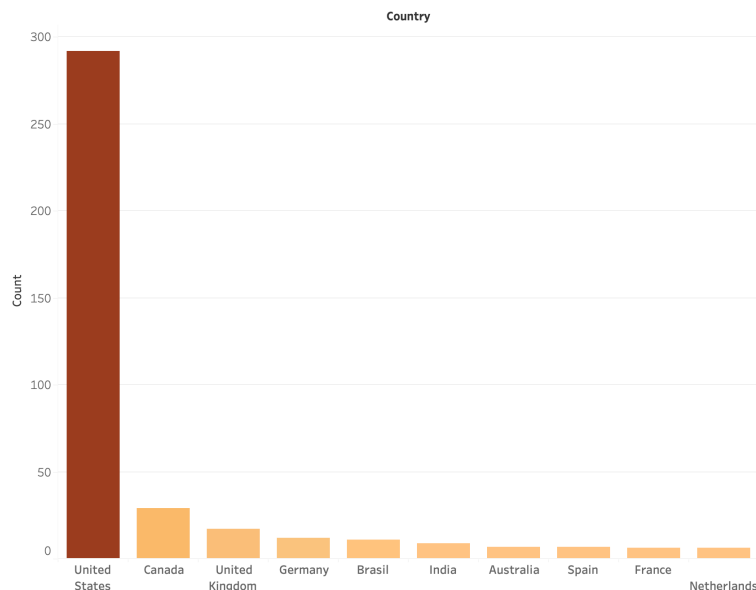


Figure 3: Number of Attacks for Top 10 Countries

The distribution of ransomware attacks across various nations can be seen in Figure 3, with the **United States (US)** experiencing the largest share of ransomware attacks. Certain commonalities amongst the targeted countries includes a country's wealth, the degree of digitalisation and visibility of successful attacks.

A country's **GDP** is a prime indicator for ransomware groups to target a region, as wealthy nations are more likely to pay off ransoms. Organisations like companies and government institutions' ability to

meet the demanded sums is possibly attributed to the increased subscription to cyber insurance. Along with the high level of economic development, these countries also experience and utilise a high **degree of digitalisation**. A significant portion of its economy engages in features such as widespread cloud adoption, connected devices and Internet of Things (IoT) systems that increases the exposure to cyberattacks [1].

In particular, the **visibility of widely publicised cases of successful attacks** have shown the success and profitability of these attacks, which have further encouraged cybercriminals' practices. These incidents highlight how lucrative ransomware can be, especially when criminals target critical infrastructure that requires services to be restored urgently. For instance, the Colonial Pipeline attack disrupted fuel supplies across the Eastern US, where a large ransom was eventually paid to restore operations, inevitably drawing attention to the effectiveness of such attacks [2]. Cases like this have shown that US companies are likely to concede to such attacks in order to avoid prolonged disruptions, thus becoming a prime target for cybercriminals. With the US media's extensive coverage of cyberattacks, it further encourages this trend by showcasing the vulnerabilities of US systems, inadvertently attracting more ransomware groups to attack US companies.

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

4.1 Most Active Ransomware Group

Play ransomware is the most active group, with 195 attacks from January to August 2024, double the totals of BianLian and RansomHub, and 60% higher than Qilin. Additionally, Play showed consistent activity, surpassing its average monthly attack count in 7 out of 8 months, outperforming all competitors. This makes Play the most active ransomware group.

No. of Attacks by Ransomware groups

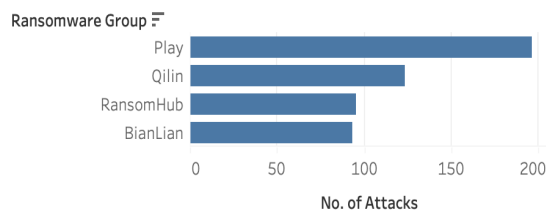


Figure 4: Number of Attacks per Ransomware Group

Number of Attacks of Groups by Month

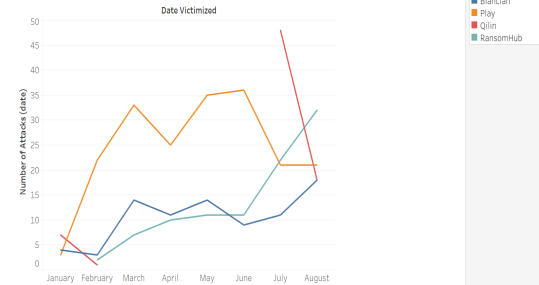


Figure 5: Ransomware Group Incident Count per Month

4.2 MITRE ATT&CK Framework

	Play [3][4][5][6]	Qilin [7][8][9][10][11]	BianLian [12][13][14][15][16]	RansomHub [17]
Initial Access	T1078: Valid Accounts T1190: Exploit Public-Facing Application	T1078 - Valid Accounts T1566 - Phishing	T1566: Phishing T1133 - External Remote Services	T1566: Phishing T1190 - Exploit Public-Facing Applications
Execution	T1059 - Command and Scripting Interpreter T1129: Shared Modules	T1059: Command and Scripting Interpreter	T1059: Command and Scripting Interpreter T1053 - Scheduled Task/Job	T1059: Command and Scripting Interpreter T1047 - Windows Management Instrumentation
Persistence	T1574: Hijack Execution Flow	T1053: Scheduled Task/Job	T1098 - Account Manipulation	T1136 - Create Account
Privilege Escalation	T1055: Process Injection T1574 - Hijack Execution Flow: DLL Side-Loading	T1078: Valid Accounts	T1068: Exploitation for privilege escalation	T1098 - Account Manipulation
Defense evasion	T1562 - Impair Defences T1070 - Indicator Removal	T1070: Indicator Removal T1562 - Impair Defences T1027 - Obfuscated Files or Information	T1562: Impair Defences	T1036 - Masquerading T1070: Indicator Removal T1562 - Impair Defences
Credential access	T1003 - OS Credential Dumping T1056: Input Capture	T1003 - OS Credential Dumping	T1003: OS Credential Dumping	T1003: OS Credential Dumping T1110 - Brute Force
Discovery	T1046 - Network Service Discovery T1057: Process Discovery T1082: System Information Discovery T1083: File and Directory Discovery T1120: Peripheral Device Discovery T1497: Virtualization/Sandbox Evasion T1518: Software Discovery	T1135- Network Share Discovery	T1046: Network Service Discovery T1033 - System Owner / User Discovery T1069 - Permission Groups Discovery	T1046: Network Service Discovery T1018 - Remote System Discovery
Lateral Movement	T1091: Replication Through Removable Media T1570: Lateral Tool Transfer	T1021: Remote Services T1091- Replication through removable media	T1021: Remote Services	T1210 - Exploitation of remote services
Collection	T1005: Data from Local System T1056: Input Capture	T1074: Data Staged	T1115: Clipboard Data	T1213: Data from Information Repositories
Command and Control	T1568.002: Dynamic Resolution: Domain Generation Algorithms T1105: Ingress Tool Transfer	T1071 - Application Layer Protocol T1001 - Data Obfuscation	T1071: Application Layer Protocol	T1219 - Remote Access Software
Exfiltration	T1041 - Exfiltration Over C2 Channel	T1011 - Exfiltration over other network medium	T1041: Exfiltration Over Command and Control Channel T1537 - Transfer Data to cloud account T1567 - Exfiltration Over Web Service	T1048 - Exfiltration Over Alternative Protocol T1537 - Transfer Data To Cloud Account
Impact	T1486 - Data Encrypted for Impact T1489: Service Stop T1491.001: Defacement: Internal Defacement	T1486: Data encrypted for impact T1485 - Data Destruction T1561 - Disk Wipe T1490 - Inhibit System Recovery	T1486: Data Encrypted for Impact	T1486: Data Encrypted for Impact T1490 - Inhibit System Recovery
Tools Used	Mimikatz, Process Hacker, Plink, AdFind, GMER, IOBit, PsExec, PowerTool, PowerShell, bloodhound	PsExec, VMware vCenter, Powershell	Rclone, PsExec, RDP, Command Shell, other native window tools	BitSAdmin, Cobalt Strike, Mimikatz, PSExec, PowerShell, RClone, Silver, SMBExec, WinSCP, CrackMapExec, Kerberoast, AngryIPScanner

Figure 6: MITRE ATT&CK Framework across ransomware websites (Full table in Appendix)

The distinctiveness of the PLAY's TTP (Tactics, Techniques, and Procedures) can be seen in the following components from the MITRE ATT&CK framework, which likely contributed to their successful attacks.

Initial Access - We will assess from the initial access component because most attacks will be limited by the robustness of the entry techniques. Play was observed to opt out of using *phishing* as their primary technique due to the unreliability of social engineering techniques, which can be observed in the infrequencies of attacks and sudden spike in attack incidents near August for Ransomhub in Fig. 5. Instead, using a mix of a *more reliable public-facing method* coupled with a *steady stream of valid accounts* fortifies Play's entrypoint's success.

Execution - In this phase we can see that Play employs Shared Modules (T1129) to perform execution unlike the other three ransomware groups. This could have a significant boost in the probability of Play's successful attacks because shared modules enable the attackers to attack by embedding malicious code in them, effectively disguising it as legitimate software. So this makes attribution more cumbersome as traditional defences focus on standalone executable files. Moreover, by using shared modules for execution Play can also bypass detection by security solutions designed to monitor and control script execution or scheduled tasks. In contrast, the other three groups rely more on detectable methods like scripting and task scheduling.

Persistence - In this phase Play employs Hijack Execution Flow (T1574) to persist in the victim's system. This technique allows play to introduce malware into the system by hijacking the legitimate system processes, which allows them to embed themselves into the system architecture without raising suspicion. For instance: Play can manipulate how the operating system locates programs to be executed[18]. So this technique ensures that malware only activates only when a certain process starts, making it difficult to detect. Thus Play's approach is harder to detect, contributing to greater success in persistence. In contrast, Qilin employs visible Scheduled Tasks(T1053), Bianlian uses Account Manipulation (T1092), and RansomHub creates new accounts, which are easier to detect through user monitoring.

Command and Control - In this phase Play employs a powerful technique of Dynamic Resolution (T1568) by using dynamic domain generation algorithm. This allows Play to dynamically establish connections to command and control infrastructure to evade common detection[19], as if one domain is taken down, another can quickly be utilised. This ensures persistent access to compromised systems and makes it hard for the security teams to track all the potential domains. Moreover, by mimicking legitimate URL patterns, DGA generated domains can blend in with normal traffic, further complicating the detection. On the other hand, the lack in the usage of DGA by other ransomware groups means that if a C2 endpoint is discovered, the attacker's ability to communicate can be severely compromised.

As observed from the above comparison, Play's attacks have shown proficiency through exploiting vulnerabilities across diverse sectors, whilst ensuring a comprehensive attack cycle. Their focus on rapid exploitation and broad but reliable targeting techniques, made them highly successful in terms of the scale of operations.

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

No. Of Attacks By Industry

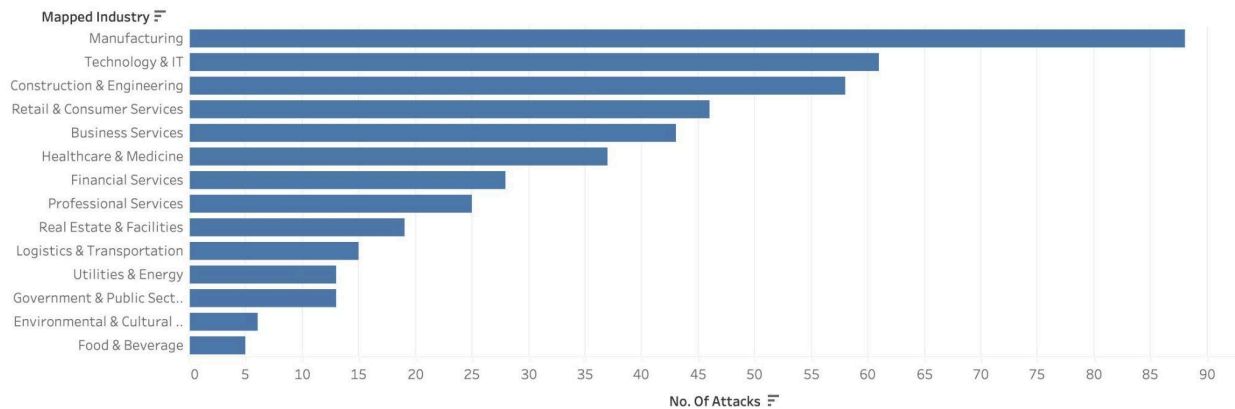


Figure 7: Distribution of ransomware attacks by industry

The top industries include manufacturing, technology & IT, and construction & engineering.

Data sensitivity: Industries like **retail & consumer services** and **business services** often manage large volumes of private and sensitive materials such as health records, financial transactions, bank account numbers, and legal documents [20]. Ransomware threats affect clients when the release of these data records escalates in the form of identity theft, financial losses and emotional distress. For companies, the exposure of sensitive data poses a serious disruption to their daily business continuity, tarnishing brand reputation, class-action lawsuits for failing to protect these data records, and a loss of customer trust [21]. Ransomware groups are aware of how sensitive these records are to both parties, and exploit this knowledge to target industries that store large quantities of such data types, leveraging higher ransoms.

Dependence on operational continuity: Industries that rely greatly on operational continuity are more prone to ransomware attacks due to the urgent nature of their daily processes. Industries such as **manufacturing, technology & IT** experience significant financial losses and a cascading disruption to the supply chain even when the interruption is brief [22]. Ransomware groups capitalise on this urgency to quickly restore operations and avoid further losses, hence by targeting companies in this sector, they are more likely to receive payment.

Weak cybersecurity infrastructure: Industries with a foundational level of cybersecurity infrastructure are particularly vulnerable to ransomware attacks as their defences are insufficient to fend off sophisticated cyber threats [23]. Small and medium-sized enterprises in sectors like **construction & engineering** do not have sufficient resources to invest into more robust cybersecurity measures like encryption, intrusion detection systems, nor do they possess a proper cybersecurity team to protect their stored data. The lack of backup systems or incident response plans also leads to a slow recovery from ransomware attacks, exacerbating their financial losses [24]. Even with the absence of sensitive data that usually correlates to higher ransom payments, attackers still capitalise on them due to the relative ease to overwhelm their cyber defences.

6. 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.

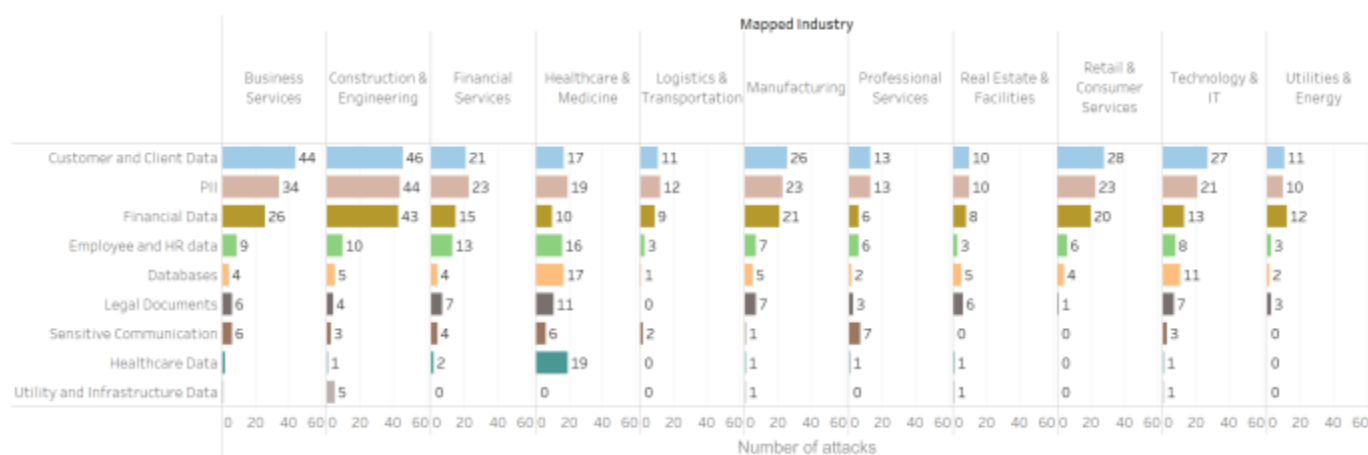


Figure 8: Data Type Stolen and number of attacks across Different Industries

Across the board, ransomware actors have been observed to target Customer & Client Data the most, followed by Personal Identifiable Information (PII) and then Financial Data. But there are slight differences in the order of popularity within each particular industry.

Business Services, Construction & Engineering, Manufacturing, Retail & Consumer Services, Technology & IT - The kinds of data stolen are **Customer & Client Data, PII, Financial Data, Employee & HR Data, Legal Documents** - in decreasing popularity (with slight variance). The top 4 kinds of data stolen are readily available within the above industries, because their projects involve financial transactions, exchange of PII for their employees' work stint, as well as information about their clients through contracts. Targeting these data types is also the most impactful for attacks, because it works as a two-pronged approach by the ransomware group to further pressure the victim company to take action. The first aspect is from the internal pressure of having the victim company's internal data such as its financial situation and employees' private information to be leaked, which are generally sensitive in nature and should not be publicly available. The second aspect is the external pressure exerted by the clients for the victim company to take action as they are indirectly implicated by extension.

Financial Services, Healthcare & Medicine, Logistics & Transportation - A similar case for the rankings of data types can be seen here, but there are larger counts of **PII**. This is inherent to the industry as they have to deal with large quantities of personal information, so such data will be more readily available for stealing. These kinds of data are classified as Red under the Traffic Light Protocol; that signifies the most confidential information that can be stolen, and are highly valued in the dark web for example, which is why attackers target these types of information that have the highest returns in terms of value. With the exception of Logistics & Transportation, there are also larger quantities of **Employee & HR Data** for stealing as their trade involves manpower as the crux of their offered services, so their employee data will be

more abundant in the victim's systems. On top of that, the wellbeing of their employees would be the company's top priority; so as to offer a safe environment for them to offer their expertise. Therefore, ransomware actors will target such information, to cripple the faith that employees have of their company and disrupt the operations of the victim companies through an indirect form of psychological attack. This then increases the urgency of the victim companies to respond to the requests of the ransomware actors, which ultimately hastens the process of the victims succumbing to the actor's threats.

Professional Services, Real Estate & Facilities - They have an equal number of **Customer & Client Data and PII**, which can be attributed to these two industries relying upon the presentation of PII together with any new business transaction involved. For instance, law companies - which fall under the Professional Services requires official identification documents upon transaction, which may not be the case for the above section, that appears to operate under the same business model but have unofficial channels for procurement of Financial Services or Healthcare & Medicine (Eg: Illegal money-lending, TCM). A possible justification for the equal values would be that these information are stored together on the same database, and can be easily fetched as a whole. There would also not be any need to make complex storage architectures as the industry's main focus is not on the digital forefront.

Utilities & Energy - The values of **Financial Data** are the highest, which is dissimilar from the general trend of PII, Customer & Client Data to be the most popular data type stolen and interestingly noted to be of the same value. The industry solely focuses on the provision of living necessities and seldom requires repeated customer interaction or personal details, which will explain why the numbers are significantly lower for the other data types.

7. Share three interesting insights you observed

7.1 RansomHub, the "New Kid on the Block"

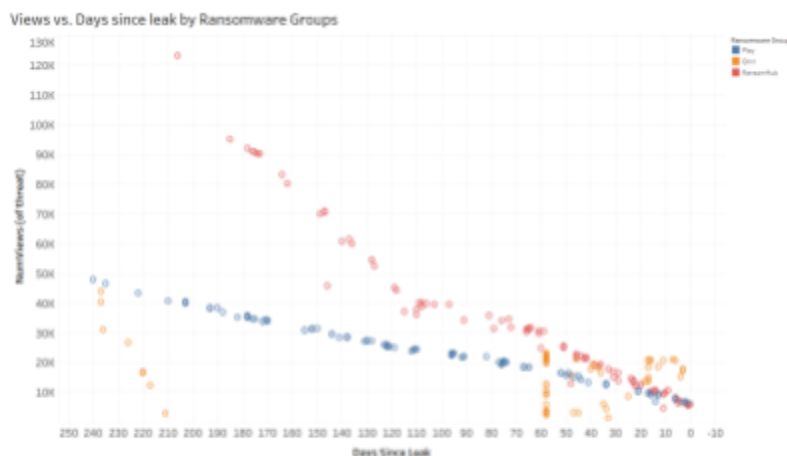


Figure 9: Number of views received and the Days since the leak was publicised

During our analysis of view counts for various ransomware incidents, we discovered an incident with over 122k views - a clear outlier. This unexpected spike in views prompted further investigation, leading us to RansomHub's first known attack. As a new player in the ransomware scene, RansomHub quickly gained significant attention, partly due to its affiliation with

Knight(Cyclops 2.0)[25] - known for their "novel form of malicious software that not only

encrypts a network's data but also exfiltrates it, essentially merging the functions of data theft and ransomware"[26].

The high number of views for RansomHub's debut attack likely reflects the interest within the cybersecurity community to understand this new threat. The connection to Knight meant that RansomHub was not just another emerging group - it had potential backing from a more experienced player, increasing its perceived risk. Researchers and defenders would have been particularly keen to monitor RansomHub's actions closely, especially given the growing frequency of ransomware attacks and rapid rise of new groups in the landscape.

RansomHub's tactics - such as targeted phishing ([T1566: Phishing](#)), credential harvesting ([T1003: OS Credential Dumping](#)), and sophisticated data exfiltration techniques ([T1041: Exfiltration Over C2 Channel](#)) - only strengthened interest, as researchers aimed to stay ahead of this new threat.

7.2 Humans: the weakest link?

In analysing the Tactics, Techniques, and Procedures of Play, Qilin, BianLian, and RansomHub, it becomes evident that humans remain one of the most significant points of failure in network security. While these ransomware groups leverage sophisticated attack techniques, their initial entry points are frequently focused on human-centric vulnerabilities, such as phishing, weak credential management, and exploiting remote access.

Three of the four ransomware groups - Qilin, BianLian, and RansomHub still rely heavily on phishing ([T1566: Phishing](#)) for initial access. This technique exploits users' trust and lack of awareness, often tricking them into clicking on malicious links or downloading harmful attachments. The simplicity and success of phishing highlight how social engineering still remains a key method for attackers to gain unauthorised access. However, Play has taken a different approach, evolving away from phishing. This shift shows Play's adaptability in refining their tactics and maintaining control.

All four ransomware groups also use a combination of dual use tools - legitimate tools such as [PsExec](#) and [Powershell](#). These tools allow the attackers to execute their malicious actions while blending in with normal system operations. Although dual-use tools are essential for day-to-day system administration, human error in configuring, managing, and securing them remains a major factor in why they are successfully exploited by ransomware groups.

Without proper policy enforcement, user training, and monitoring systems, organisations leave themselves vulnerable to attacks that could otherwise be mitigated. Addressing these human-centric weaknesses is key to defending against the misuse of legitimate tools by ransomware actors.

7.3 SMEs - the most sought after victim for ransomware groups

Number of Attacks by Company Size

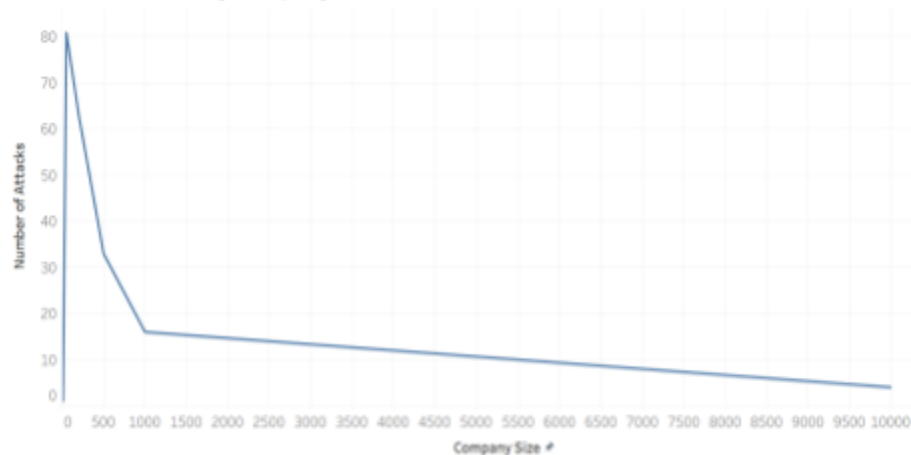


Figure 10: Attacks Compared to Company Size

From Figure 10, the number of ransomware attacks peaked when the company size is around 50 employees which typically falls under the category of small business or small and medium-sized enterprise (SME). SMEs are attacked the most frequently compared to micro-enterprises or

large corporations due to several reasons.

Firstly, although micro-enterprises may be easier to compromise because of their limited resources and weaker defences, they are less attractive to attackers because of their **inability to pay significant ransoms**. It may actually be more favourable for the micro-enterprises to just close down their business than pay the exorbitant fees to restore operations. Additionally, micro-enterprises typically possess smaller amounts of sensitive data that the ransomware group can steal. Hence, offering little reward for the attacker's effort, making them less appealing as targets.

Secondly, SMEs often play a crucial role within supply chains for larger organisations. These SMEs usually have weaker security compared to the larger companies that they work with and they could **serve as an indirect entry point** into bigger and more valuable targets [27]. Attackers see SMEs as a gateway into bigger companies that store more valuable data, making SMEs an attractive intermediary target in ransomware campaigns.

Lastly, big corporations generally possess more advanced cybersecurity defences and are more likely to implement frequent data backups. Their preparedness enables them to quickly recover from attacks and reduces their likelihood of paying ransoms. Knowing this, cybercriminals may avoid targeting large enterprises as the **probability of receiving payment is lower**. Furthermore, attacking large companies will typically make headlines when they are attacked, **capturing the attention of the media and law enforcement**. This will potentially increase the risk for the attackers as more resources are dedicated to finding and retaliating against them [28].

Thus, SMEs represent the “sweet spot” for ransomware groups. They **offer a balance between vulnerability and profitability**, where attackers can exert relatively little effort while still gaining

substantial financial rewards. In other words, SMEs are big enough to provide lucrative payouts but small enough to have security weaknesses that attackers can easily exploit.

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

From this report, we learnt more about the TTPs and motivations of ransomware groups towards different companies and industries. Most of our struggles occur during the scraping of the ransomware sites. These involve configuring VMWare and TOR browser for scraping onion sites, having to scrape Lockbit's data type which cannot be done directly. Halfway through scraping Lockbit, its sites were taken down by NCA, so we opted to use another site which was live and had data types that were easier to scrape in general. Moreover, we particularly wanted meta data on the data stolen, we wanted to gain insights on the data type and nature of data most sought after by ransomware groups. Since most of the scraped lockbit data was in image format with very limited image descriptors, we decided to pivot to Play instead. Mostly, when we faced issues, we would search for videos or guides for how to configure VMWare for example and would only pivot when the time sink is overly excessive.

9. Conclusion

In conclusion, this report highlights the threats posed by various ransomware groups, with particular focus on Play , which emerged as the most active ransomware shaming website from the sample, with a strong and unique TTP owing to its success. Through examination of attack patterns, methods and target sectors, ransomware actors mostly take advantage of human weaknesses, antiquated security measures and the growing digitization of industries. Our primary and secondary research concludes the US to be the most attacked country from January to August 2024, owing to factors such as high level of wealth and digitalisation. In terms of industries affected, ransomware groups express greater interest in companies handling sensitive data like retail & consumer services and business services, or companies dependent on operational continuity in manufacturing, technology & IT. By focusing on these points of reference, we can build a better understanding of the importance of robust cybersecurity measures and timely responses to evolving tactics of ransomware groups.

10. Contribution Table

No.	Name	Contribution
1	Joelle Chew Ningxi	<ul style="list-style-type: none">• Web scraping• Questions 1 & 2 + Tableau
2	Darren Lee Jun Rui	<ul style="list-style-type: none">• Ransomware scraping• Question 4 + Tableau
3	Goyal Ananya Surendrakumar	<ul style="list-style-type: none">• Web scraping• Question 4 (TTP) + Tableau• Introduction
4	Harikrishnan Vinaya Souraba	<ul style="list-style-type: none">• Web scraping• Question 4 (TTP) + Tableau
5	Jerick Lim Kai Zheng	<ul style="list-style-type: none">• Ransomware scraping• Question 5 + Tableau
6	Caren Tan Xin Yao	<ul style="list-style-type: none">• Ransomware scraping• Question 6 + Tableau
7	Joseph Teo	<ul style="list-style-type: none">• Ransomware scraping• Question 6 + Tableau• Lessons learnt + Conclusion
8	Tan Jia Hao	<ul style="list-style-type: none">• Overall report polishing

11. References

- [1] Highfill, T., & Surfield, C. (2022, November). *New-and-revised-statistics-of-the-US-digital-economy-2005-2021*. Bureau of Economic Analysis.
<https://www.bea.gov/system/files/2022-11/new-and-revised-statistics-of-the-us-digital-economy-2005-2021.pdf>
- [2] Wood, K. (2023, March 7). *Cybersecurity Policy Responses to the Colonial Pipeline Ransomware Attack*. The Georgetown Environmental Law Review.
<https://www.law.georgetown.edu/environmental-law-review/blog/cybersecurity-policy-responses-to-the-colonial-pipeline-ransomware-attack/#:~:text=A%20hacker%20group%20known%20as,diesel%20fuel%2C%20and%20jet%20fuel.>
- [3] “Weekly Intelligence Report - 26 July 2024 - CYFIRMA,” CYFIRMA, Sep. 27, 2024.
<https://www.cyfirma.com/news/weekly-intelligence-report-26-july-2024/> (accessed Oct. 13, 2024)
- [4] “#StopRansomware: Play Ransomware | CISA,” www.cisa.gov, Dec. 18, 2023.
<https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a>
- [5] “How Trend Micro Managed Detection and Response Pressed Pause on a Play Ransomware Attack,” *Trend Micro*, Aug. 22, 2024.
https://www.trendmicro.com/en_us/research/24/h/pressing-pause-on-play-ransomware.html (accessed Oct. 13, 2024).
- [6] L. Fróes, “REPLAY: Revisiting Play Ransomware Anti-Analysis Techniques,” *Netskope*, Aug. 08, 2024.
<https://www.netskope.com/blog/replay-revisiting-play-ransomware-anti-analysis-techniques> (accessed Oct. 13, 2024).
- [7] A. Sentenac, “A Busy Agenda: Darktrace’s Detection of Qilin Ransomware-as-a-Service Operator,” *Darktrace.com*, Jul. 04, 2024.
<https://darktrace.com/blog/a-busy-agenda-darktraces-detection-of-qilin-ransomware-as-a-service-operator> (accessed Oct. 13, 2024).
- [8] “Qilin Ransomware,” *Blackpoint Cyber*, Sep. 09, 2024.
<https://blackpointcyber.com/resources/threat-profile/qilin-ransomware/> (accessed Oct. 13, 2024)
- [9] “Unveiling Qilin/Agenda Ransomware - A Deep Dive into Modern Cyber Threats,” *SEC Consult*, Jun. 28, 2024.
<https://sec-consult.com/blog/detail/unveiling-qilin-agenda-ransomware-a-deep-dive-into-modern-cyber-threats/> (accessed Oct. 13, 2024).

- [10] "Dark Web Profile: Qilin (Agenda) Ransomware," SOCRadar® Cyber Intelligence Inc., Jun. 06, 2024. <https://socradar.io/dark-web-profile-qilin-agenda-ransomware/>
- [11] A. Mascellino, "Qilin Ransomware's Sophisticated Tactics Unveiled By Experts," *Infosecurity Magazine*, Jul. 17, 2024. <https://www.infosecurity-magazine.com/news/qilin-ransomwares-tactics-unveiled/> (accessed Oct. 13, 2024).
- [12] P. Kimayong, "BianLian Ransomware Group: 2024 Activity Analysis | Official Juniper Networks Blogs," *Official Juniper Networks Blogs*, Jul. 11, 2024. <https://blogs.juniper.net/en-us/security/bianlian-ransomware-group-2024-activity-analysis> (accessed Oct. 13, 2024).
- [13] C. Barry, "BianLian: The face-changing ransomware menace," *Barracuda Blog*, Aug. 09, 2024. <https://blog.barracuda.com/2024/08/09/bianlian--the-face-changing-ransomware-menace>
- [14] D. Frank, "Threat Assessment: BianLian," *Unit 42*, Jan. 23, 2024. <https://unit42.paloaltonetworks.com/bianlian-ransomware-group-threat-assessment/> (accessed Oct. 13, 2024).
- [15] CISA, "#StopRansomware: BianLian Ransomware Group | CISA," *www.cisa.gov*, May 16, 2023. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-136a>
- [16] Y. Ernalbant, "Threat Actor Profile: BianLian, The Shape-Shifting Ransomware Group," *SOCRadar® Cyber Intelligence Inc.*, Jul. 13, 2023. <https://socradar.io/threat-actor-profile-bianlian-the-shape-shifting-ransomware-group/>
- [17] "#StopRansomware: RansomHub Ransomware | CISA," *Cybersecurity and Infrastructure Security Agency CISA*, Aug. 29, 2024. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a>
- [18] "Hijack Execution Flow, Technique T1574 - Enterprise | MITRE ATT&CK®," *attack.mitre.org*. <https://attack.mitre.org/techniques/T1574/>
- [19] "Dynamic Resolution, Technique T1568 - Enterprise | MITRE ATT&CK®," *attack.mitre.org*. <https://attack.mitre.org/techniques/T1568/>
- [20] U.S. Department of Health & Human Services. (n.d.). Breach portal: Notice to the secretary of HHS breach of unsecured protected health information. Retrieved from https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
- [21] Corbet, S., & Goodell, J. W. (2022). The reputational contagion effects of ransomware attacks. *Finance Research Letters*, 47(Part B), 102715.

- [22] Cybereason. (2023). The state of ransomware in the manufacturing sector. Retrieved from <https://www.cybereason.com/blog/the-state-of-ransomware-in-the-manufacturing-sector>
- [23] Byrne, M. D. (2021). Cybersecurity and the new age of ransomware attacks. *Journal of PeriAnesthesia Nursing*, 36(5), 594-596. <https://doi.org/10.1016/j.jopan.2021.07.004>
- [24] Gasparini, C. A. (2021). Protecting intellectual property in the digital age. *The Journal of Intellectual Property Law*, 19(2), 78-95. <https://www.proquest.com/openview/f6201613928365d1bed639047821e5c0/1?pq-origsite=gscholar&cbl=1976358>
- [25] #stopransomware: Ransomhub ransomware: CISA. Cybersecurity and Infrastructure Security Agency CISA. (2024, September 5). <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a>
- [26] Talukdar, S. (2024, February 3). Understanding knight ransomware: Advisory, analysis: CloudSEK. <https://www.cloudsek.com/blog/understanding-knight-ransomware-advisory-analysis>
- [27] World Economic Forum, Accenture, Jurgens, J., & Dal Cin, P. (2024). Global Cybersecurity Outlook 2024. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf
- [28] Drapkin, A., & Drapkin, A. (2022, February 7). 82% of ransomware attacks target small businesses, report reveals. Tech.co. <https://tech.co/news/82-of-ransomware-attacks-target-small-businesses-report-reveals>

11. Appendix

MITRE ATT&CK Framework (Highlighted points are unique to Play)

	Play [3][4][5][6]	Qilin [7][8][9][10][11]	Bianlian [12][13][14][15][16]	RansomHub [17]
Initial Access	T1078.001 - Valid Accounts T1190: Exploit Public-Facing Application	T1078 - Valid Accounts T1566 - Phishing	T1566: Phishing T1133 - External Remote Services	T1566: Phishing T1190 - Exploit Public-Facing Applications
Execution	T1059 - Command and Scripting Interpreter T1129: Shared Modules	T1059- Command and Scripting Interpreter	T1059- Command and Scripting Interpreter T1053 - Scheduled Task/Job	T1059: Command and Scripting Interpreter T1047 - Windows Management Instrumentation
Persistence	T1574: Hijack Execution Flow	T1053- Scheduled Task/Job	T1098 - Account Manipulation	T1136 - Create Account
Privilege Escalation	T1055- Process Injection T1574 - Hijack Execution Flow: DLL Side- Loading	T1078- Valid Accounts	T1068: Exploitation for privilege escalation	T1098 - Account Manipulation
Defense evasion	T1562 - Impair Defences T1070 - Indicator Removal	T1070- Indicator Removal T1562 - Impair Defences T1027 - Obfuscated Files or Information	T1562: Impair Defences	T1036 - Masquerading T1070- Indicator Removal T1562 - Impair Defences
Credential access	T1003 - OS Credential Dumping T1056: Input Capture	T1003 - OS Credential Dumping	T1003: OS Credential Dumping	T1003: OS Credential Dumping T1110 - Brute Force
Discovery	T1046 - Network Service Discovery T1057- Process Discovery T1082- System Information Discovery T1083- File and Directory Discovery T1120- Peripheral Device Discovery T1497- Virtualization/Sandbox Evasion T1518- Software Discovery	T1135- Network Share Discovery	T1046: Network Service Discovery T1033 - System Owner / User Discovery T1069 - Permission Groups Discovery	T1046: Network Service Discovery T1018 - Remote System Discovery
Lateral Movement	T1091: Replication Through Removable Media T1570: Lateral Tool Transfer	T1021- Remote Services T1091- Replication through removable media	T1021: Remote Services	T1210 - Exploitation of remote services
Collection	T1005: Data from Local System T1056: Input Capture	T1074: Data Staged	T1115: Clipboard Data	T1213: Data from Information Repositories
Command and Control	T1568.002: Dynamic Resolution: Domain Generation Algorithms T1105: Ingress Tool Transfer	T1071 - Application Layer Protocol T1001 - Data Obfuscation	T1071: Application Layer Protocol	T1219 - Remote Access Software

Exfiltration	T1041 - Exfiltration Over C2 Channel	T1011 - Exfiltration over other network medium	T1041: Exfiltration Over Command and Control Channel T1537 - Transfer Data to cloud account T1567 - Exfiltration Over Web Service	T1048 - Exfiltration Over Alternative Protocol T1537 - Transfer Data To Cloud Account:
Impact	T1486 - Data Encrypted for Impact T1489: Service Stop T1491.001: Defacement: Internal Defacement	T1486- Data encrypted for impact T1485 - Data Destruction T1561 - Disk Wipe T1490 - Inhibit System Recovery	T1486: Data Encrypted for Impact	T1486: Data Encrypted for Impact T1490 - Inhibit System Recovery
Tools Used	Mimikatz, Process Hacker, Plink, AdFind, GMER, IOBit, PsExec, PowerTool, PowerShell, bloodhound	PsExec, VMware vCenter, Powershell	Rclone, PsExec, RDP, Command Shell, other native window tools	BITSAAdmin, Cobalt Strike, Mimikatz, PSEXec, PowerShell, RClone, Silver, SMBExec, WinSCP, CrackMapExec, Kerberoast, AngryIPScanner