NANYANG TECHNOLOGICAL UNIVERSITY
SINGAPORE

SC4016/CE4070/CZ4070

CYBER THREAT INTELLIGENCE

Group Project Report

Submitted by: Group 17

Date: 14 October 2024

Group Members:

Name	Matric No.
Ang Yi Xuan	U2022338K
Anika Tan Yan Yue	U2122089G
Bryan Lu We Zhern	U2120341F
Leo Zhi Kai	U2120050L
Neoh Kai Xiang	U2122233K
Niyatha Srinivasan	U2123423J
Sruthi Sathishkumar	U2223450D
Tan Hong Zhao	U2121275C

Table of Contents

Overview

This project focuses on ransomware attacks from four ransomware threat actors from January to September 2024. The four threat actors are BianLian, Cactus, Hunters International and Danon.

BianLian emerged in 2022 and has become one of the top three most active ransomware groups. They gain initial access through compromised Remote Desktop Protocol (RDP) credentials or via phishing. Their exploits involved stealing data and encrypting it for ransom. Over time, this shifted to only stealing and extorting data for ransom.

Cactus ransomware group first appeared in 2023. It typically gains access via vulnerable Virtual Private Networks (VPNs) and establishes command and control communication via SSH. It is like BianLian in the sense that Cactus is also a double-extortion ransomware which encrypts the data and exfiltrates it.

Hunters International started in late 2023 and was once speculated to be related to Hive, a ransomware group taken down by the FBI. It is a ransomware as a service (RaaS) that commonly uses vulnerabilities in public-facing applications and using stolen credentials for RDP services.

Danon is the youngest out of the four threat actors, starting out in April 2024. Unlike the other three groups, danon functions more as a data broker than a ransomware group. The group typically gains access via phishing emails to deploy their scripts.

The questions to be answered in this project are:

1. What is the percentage distribution of countries targeted globally? [2 marks]
2. Why are some countries more targeted than others? [2 marks]
3. Which ransomware group is the most active? What is so unique about their TTPs that makes them so "successful"? [6 marks]
4. Which industries are more prone to ransomware threats and why? [5 marks]
5. 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]
6. What are the 3 interesting insights the group observed? [9 marks]
7. What we learnt, what were our struggles in executing the project and how did we overcome them? [1 mark]

1. What is the % distribution in countries targeted globally?

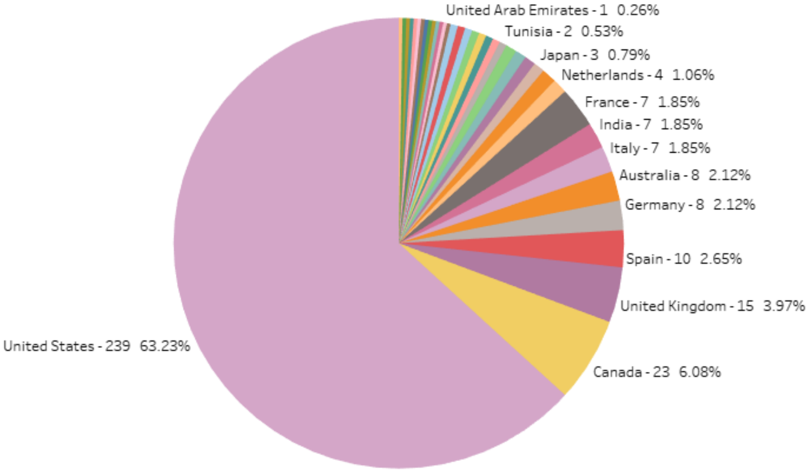


Figure 1. Pie Chart of Attack Count to Countries

Based on Figure 1, the four ransomware groups launched a total of 378 attacks. United States (US) topped the list at 239 attacks (63.23%). Canada followed at 23 attacks (6.08%). Europe and Australia combined saw 70 attacks (18.52%), especially against more developed European countries, with the United Kingdom (UK), Spain and Germany experiencing 15, 10 and 8 attacks respectively. Countries in Africa and Asia were less affected, totalling to only 31 attacks (8.20%). India led this group with 7 attacks, whilst most other countries experienced less than 3 attacks.

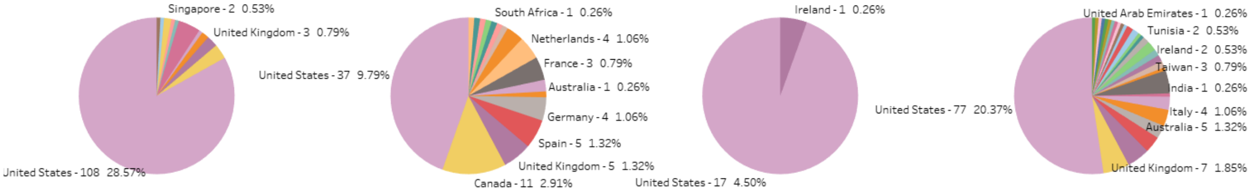


Figure 2. Pie Chart of Attack Count to Countries based on Ransomware groups (from left to right, Bianlian, Cactus, Danon, Hunters International)

Figure 2 provides a breakdown of the attack counts by individual ransomware groups targeting various countries. The distribution mirrors the overall trend we see in Figure 1, with the US experiencing the highest number of attacks, followed by other countries like Canada and the UK. This highlights that while some groups are active in more certain regions, the overall trend remains consistent.

2. Why are some countries more targeted than others?

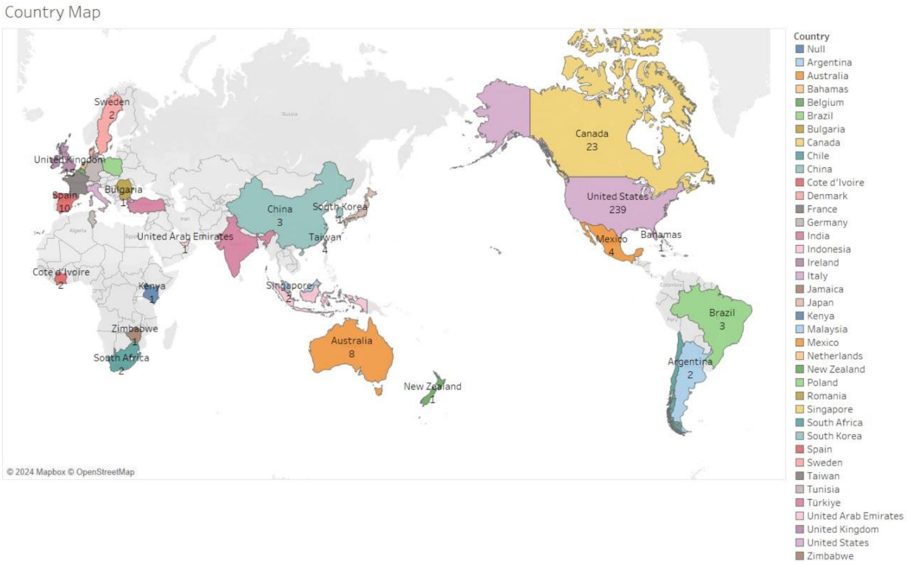


Figure 3. World Map of Attacks based on Countries

We did an Analysis of Competing Hypothesis (ACH), which can be found in the Appendix 2.1 Analysis of Competing Hypothesis.

Our analysis strongly suggests H3, that these ransomware groups are mostly after financial gains. All evidence indicates that these ransomware groups target developed countries, industries with valuable data, sensitive operations and high financial capabilities. (++ from E4 and + from E1, E2, and E3). This highlights their primary monetary goal over ideological motives.

H1 also receives some evidential support, as the high geographical distribution of attacks over developed / high-income countries is corroborated by E1 (++) but partially by E4 (+). This may suggest that ransomware groups favour wealthier nations where ransom demands are more likely to be paid.

H2, which hypothesises that ransomware groups target corporations handling valuable or sensitive data and operations, is also supported by E2 and E3 (++), although its overall alignment is less justified compared to H3.

Domain and email analysis of Hunter's International provides evidence of links with Russia and Nigeria. Furthermore, this group primarily uses Russian and English as medium of communications [3, 6]. This might suggest why English-speaking countries such as the US and Canada are targeted more. Additionally, factors such as a sense of patriotism, loyalty to local networks, or fear of attracting the attention of local law enforcement, could explain why Russia is not targeted as much in our research.

3. Which ransomware group is the most active? What is so unique about their Tactics, Techniques and Procedures (TTPs) that makes them so “successful”?

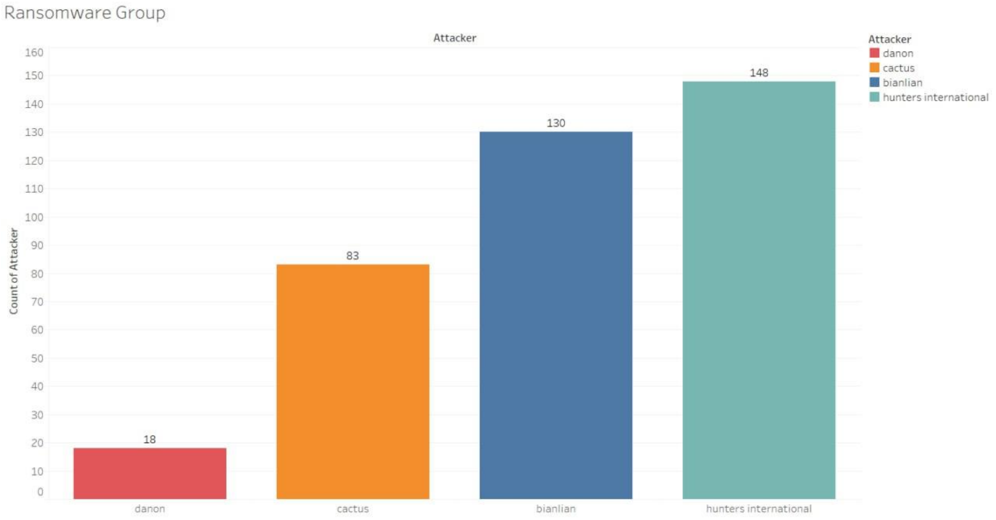


Figure 4. Bar Chart of Attackers and Total Number of Attacks

From our secondary research, we identified Ransomhub as the most active group over the last 90 days (August to October). For more information on Ransomhub TTPs, refer to Appendix 3.1.

Our primary research focused mainly on 4 ransomware groups: Hunters International, Bianlian, Cactus and danon over the 8-month period (from January to August). Hunter International had the most attack count during this period.

Hunter’s International operates as a Ransomware-as-a-Service (RaaS) model and is unique for prioritizing data exfiltration and has an easy-to-use user interface to make payment. Hunter's International targets Windows and Linux environments for data exfiltration [6].

The group formally began its activity on October 2023 [6], after the seize of infamous Ransomware group, HIVE. The match in 60% of their source code and the timing led to speculations of Hunter’s International being the “successors” of HIVE [2]. However, these speculations were promptly addressed by Hunter’s International on their official website. The group released that all of HIVE’s source code (written in C and golang) were bought by them. It also highlighted that encryption is not their primary goal. Hunter’s International also made considerable improvements and patches to the bought source code. The group rewrote the source code in Rust and changed the encryption process that they claimed it had several issues, “mistakes that caused unavailability for decryption” [2][3].

The infection chain usually begins with an initial access by supply chain attacks, social engineering using spearphishing email [T1566.001], compromised RDP service [T1133] and vulnerable public-facing application [T1190].

After gaining initial access, Hunters International executes various commands and edits register values to prevent backup and recovery. To evade detection, they also obtain ‘SE_DEBUG’ privilege and take a snapshot of all running process using ‘CreateToolhelp32Snapshot’ and searches for ‘winlogon.exe’ process [T1562]. If the malware sample is found, it opens the process and impersonates the token to escalate privileges and bypass access control [T1547].

To discover system files for encryption, ‘GetLogicalDrivesStringsW’ is used to obtain all available drives on the system [T1082]. If the result value is less than 2 (0 = DRIVE_UNKNOWN and 1 = DRIVE_NO_ROOT_DIR), the names will be skipped during encryption. AES cipher and RSA encryption algorithms are taken from Crates.io web service for creating and searching different packages for Rust. Once files are encrypted, a ransom note is displayed demanding payment in cryptocurrency. [7]

The HIVE encryption process included the creation of a *.key file in the root directory (C:\ or /root/). Required for decryption, this key file only exists on the machine where it was created and cannot be reproduced. A ransom note, HOW_TO_DECRYPT.txt was also dropped into each affected directory and states the *.key file cannot be modified, renamed, or deleted, otherwise the encrypted files cannot be recovered [T1486] [4].

In comparison, Hunter’s International encryption process was made different from that of Hive’s by implementing a simpler approach by including the encryption key in the encrypted files. It uses a combination of ChaCha20-Poly1305 to encrypt the files and RSA OAEP (method PKCS1 and SHA3-512 as the hash algorithm) to encrypt the keys. The data is decrypted using the RSA private key and is then utilized to generate the Chacha key. ChaCha20 is a symmetric encryption mechanism - the same key is used for both encryption and decryption [2].

Reasons for success:

i) Prioritizing **data exfiltration**: They understand the true value of the data and do not only use encrypted data as a leverage. The previous operation of HIVE not only limited the full exploitation of stolen data, focusing primarily on holding it for ransom, but also involved a unique and problematic decryption process. With Hunter’s International, they are interested in the decrypted data itself. Their newer model ensures that they either profit off ransom or they monetise the data itself.

ii) Professional, sophisticated UI to raise **reputation** among affiliates: A more sophisticated look associates itself with other larger groups like cl0p, Ransomhub and lockbit.

iii) The group is believed to have **affiliations** with other prominent ransomware groups, where they exchange tactics, tools, and sometimes even personnel. This allows the group to have more access to knowledge and manpower to increase their capability and capacity.

Refer to Appendix 3.2 for IoC (Hunter’s International), ATT&CK Technique (Hunter’s International and HIVE).

4. Which industries are more prone to ransomware threats and why?

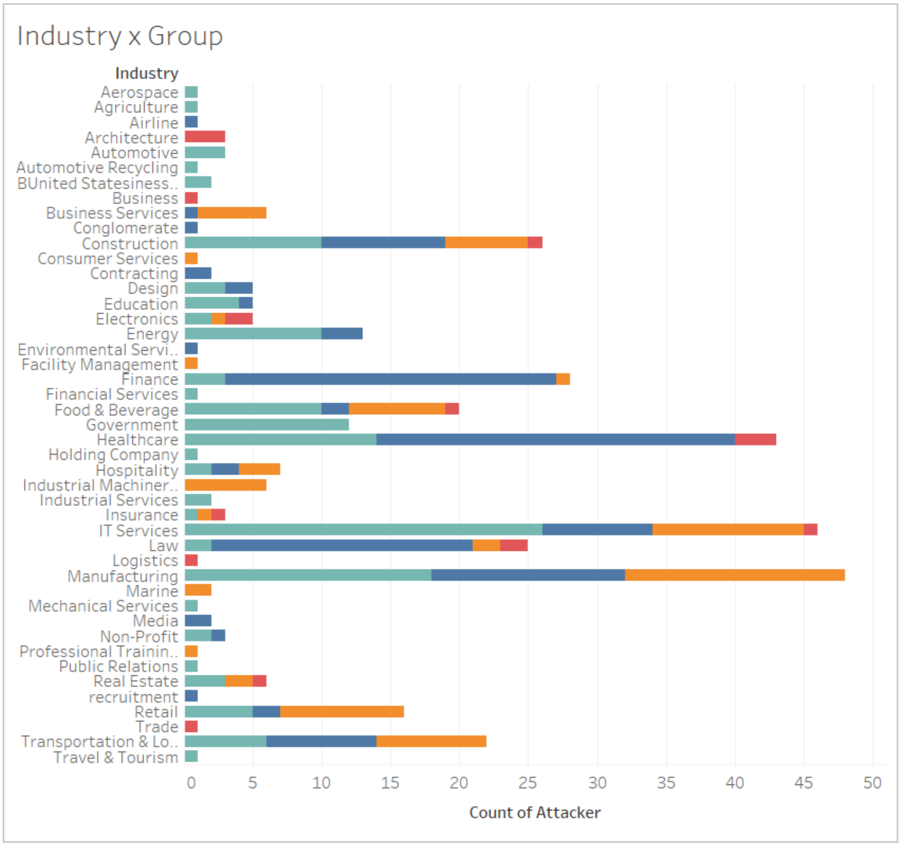


Figure 5. Distribution of Attacks By Industry with Count of Attackers Categorized By Groups

From our data, the industries targeted the most are Manufacturing, IT Services, and Healthcare. Most data stolen in each industry are employee and financial information. The value of these information is high for each industry, so they are not specific to the 3 industries identified.

4.1 Manufacturing

Most of the data stolen was company, email, and design information. These contain industry sensitive information such as intellectual property which is valuable for information brokering. A successful attack can affect production lines which causes a domino effect on sectors down the supply chain. Companies that cooperate widely can be exploited to infiltrate their partners through lateral movement. Manufacturing companies are also usually on older legacy systems, making them easier targets.

4.2 IT Services

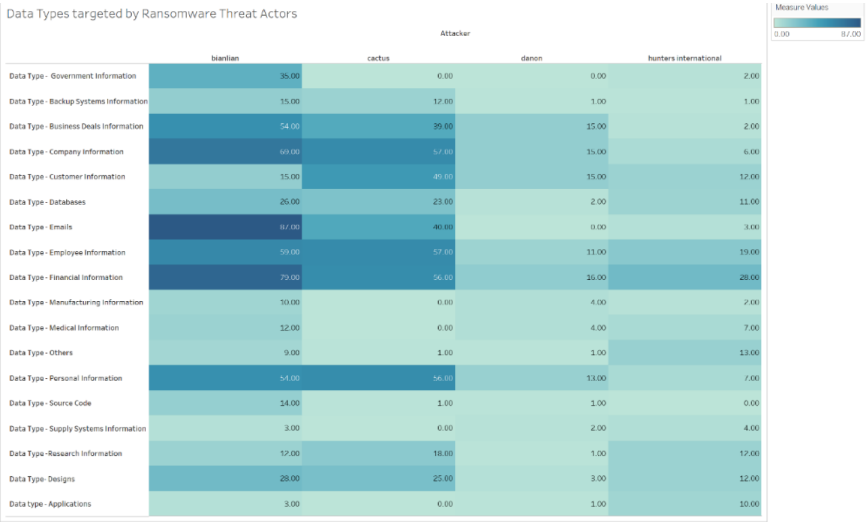
Most of the relevant data stolen was company and customer information. These can contain information like company security policy and customer credit card information. Knowing the security policy makes it easier for attackers, which is valuable alongside credit card information. Another relevant data is source code, which allows exploitation of code vulnerability.

4.3 Healthcare

Most of the data stolen was employee and patient personal information, financial information, and medical records This industry is especially vulnerable to ransomware because it handles valuable sensitive information, and any downtime can endanger lives, prompting quick ransom payments. Additionally, the sector often relies on outdated, less secure systems, making them a frequent target. Regulations like GDPR and HIPAA impose significant penalties for failing to protect personally identifiable information (PII), making organizations prime targets due to the potential reputational and financial fallout of a data breach.

5. What kind of data do actors usually target? What are the kinds of data targeted in each industry? Show a breakdown comparing types of data stolen.

The Data Types ransomware threat actors focus on are typically weighed by factors such as ease of access, sensitivity of data and priority given to data. Our analysis of the threat actor has let us arrive at the heatmap shown below.



Data Types targeted by Ransomware Threat Actors

	Attacker			
	bianlian	cactus	danon	hunters international
Data Type - Government Information	35.00	0.00	0.00	2.00
Data Type - Backup Systems Information	15.00	12.00	1.00	1.00
Data Type - Business Deals Information	54.00	39.00	15.00	2.00
Data Type - Company Information	69.00	57.00	15.00	6.00
Data Type - Customer Information	15.00	49.00	15.00	12.00
Data Type - Databases	26.00	23.00	2.00	11.00
Data Type - Emails	87.00	40.00	0.00	3.00
Data Type - Employee Information	59.00	57.00	11.00	19.00
Data Type - Financial Information	79.00	56.00	16.00	28.00
Data Type - Manufacturing Information	10.00	0.00	4.00	2.00
Data Type - Medical Information	12.00	0.00	4.00	7.00
Data Type - Others	9.00	1.00	1.00	13.00
Data Type - Personal Information	54.00	56.00	13.00	7.00
Data Type - Source Code	14.00	1.00	1.00	0.00
Data Type - Supply Systems Information	3.00	0.00	2.00	4.00
Data Type -Research Information	12.00	18.00	1.00	12.00
Data Type- Designs	28.00	25.00	3.00	12.00
Data type - Applications	3.00	0.00	1.00	10.00

Figure 6. Heatmap of Different Data Types and Attackers

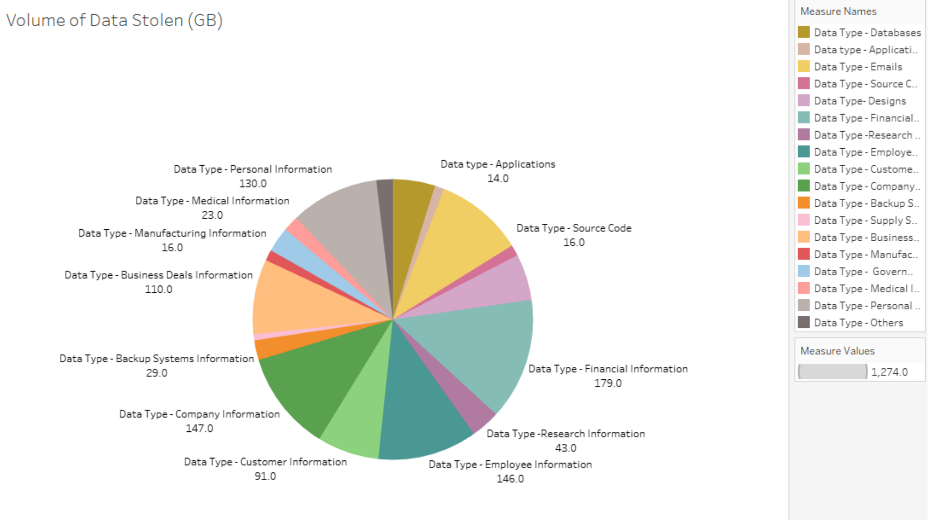
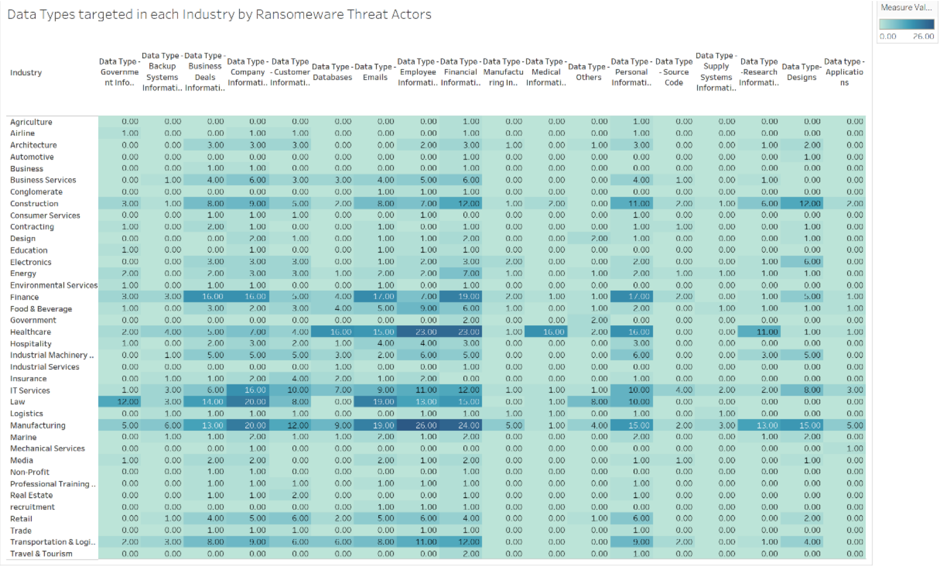


Figure 7. Pie Chart of Composition of Different Data Types

From the graphs, we can deduce that the top five data types that ransomware threat actors target are Financial Information, Company Information, Employee Information, Emails, Personal Information.

1. Financial Information: All threat actors targeted financial information, and this category is the top data type stolen by each group. A leak in financial data can lead to financial fraud, loss of reputation and legal issues between the company and other affected parties.
2. Company Information: Exposing company information can lead to trade secrets and intellectual property being revealed. It can also expose other sensitive data like the company's customers and contractors. All groups targeted this type of information as well.
3. Employee Information: This could be used for impersonation attacks where an adversary poses as an employee to gain access into the company's system. All groups targeted this type of information as well.
4. Emails: Exposing emails increases the attack surface available to adversaries. These emails could be a potential target for phishing attacks, especially if the emails are already compromised.
5. Personal Information: Ransomware groups recognise that this type of information is one of the most sensitive data available and can be used for identity theft. All groups targeted this type of information as well.

To look further into the distribution of data types that ransomware actors set sights on, we now illustrate the data types most sought after by threat actors in each industry.



Data Types targeted in each Industry by Ransomeware Threat Actors

Industry	Data Type - Governme nt Info..	Data Type - Backup Systems Informati..	Data Type - Business Deals Informati..	Data Type - Company Informati..	Data Type - Customer Informati..	Data Type - Databases	Data Type - Emails	Data Type - Employee Informati..	Data Type - Financial Informati..	Data Type - Manufactu ring In..	Data Type - Medical Informati..	Data Type - Others	Data Type - Personal Informati..	Data Type - Source Code	Data Type - Supply Systems Informati..	Data Type -Research Informati..	Data Type- Designs	Data type - Applicatio ns
Agriculture	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00
Airline	1.00	0.00	0.00	1.00	1.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00
Architecture	0.00	0.00	3.00	3.00	3.00	0.00	0.00	2.00	3.00	1.00	0.00	1.00	3.00	0.00	0.00	1.00	2.00	0.00
Automotive	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00
Business	0.00	0.00	1.00	1.00	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Business Services	0.00	1.00	4.00	6.00	3.00	3.00	4.00	5.00	6.00	0.00	0.00	0.00	4.00	1.00	0.00	1.00	0.00	0.00
Conglomerate	0.00	0.00	0.00	0.00	0.00	0.00	1.00	1.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Construction	3.00	1.00	8.00	9.00	5.00	2.00	8.00	7.00	12.00	1.00	2.00	0.00	11.00	2.00	1.00	6.00	12.00	2.00
Consumer Services	0.00	0.00	1.00	1.00	1.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00
Contracting	1.00	0.00	2.00	1.00	0.00	0.00	1.00	0.00	1.00	0.00	0.00	0.00	1.00	1.00	0.00	0.00	1.00	0.00
Design	0.00	0.00	0.00	2.00	1.00	0.00	1.00	1.00	2.00	0.00	0.00	2.00	1.00	0.00	0.00	0.00	1.00	0.00
Education	1.00	0.00	0.00	1.00	0.00	0.00	1.00	1.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Electronics	0.00	0.00	3.00	3.00	3.00	0.00	1.00	2.00	3.00	2.00	0.00	0.00	2.00	0.00	0.00	1.00	6.00	0.00
Energy	2.00	0.00	2.00	3.00	3.00	1.00	2.00	2.00	7.00	1.00	0.00	1.00	2.00	1.00	1.00	1.00	1.00	0.00
Environmental Services	1.00	0.00	1.00	1.00	0.00	0.00	1.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Finance	3.00	3.00	16.00	16.00	5.00	4.00	17.00	7.00	19.00	2.00	1.00	1.00	17.00	2.00	0.00	1.00	5.00	1.00
Food & Beverage	1.00	0.00	3.00	2.00	3.00	4.00	5.00	9.00	6.00	1.00	0.00	1.00	2.00	0.00	1.00	1.00	1.00	1.00
Government	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	2.00	0.00	0.00	2.00	0.00	0.00	0.00	0.00	0.00	0.00
Healthcare	2.00	4.00	5.00	7.00	4.00	16.00	15.00	23.00	23.00	1.00	16.00	2.00	16.00	0.00	0.00	11.00	1.00	1.00
Hospitality	1.00	0.00	2.00	3.00	2.00	1.00	4.00	4.00	3.00	0.00	0.00	0.00	3.00	0.00	0.00	0.00	0.00	0.00
Industrial Machinery ..	0.00	1.00	5.00	5.00	5.00	3.00	2.00	6.00	5.00	0.00	0.00	0.00	6.00	0.00	0.00	3.00	5.00	0.00
Industrial Services	0.00	0.00	0.00	0.00	0.00	1.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Insurance	0.00	1.00	1.00	2.00	4.00	2.00	1.00	2.00	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00
IT Services	1.00	3.00	6.00	16.00	10.00	7.00	9.00	11.00	12.00	1.00	1.00	1.00	10.00	4.00	2.00	2.00	8.00	3.00
Law	12.00	3.00	14.00	20.00	8.00	0.00	19.00	13.00	15.00	0.00	1.00	8.00	10.00	0.00	0.00	0.00	0.00	0.00
Logistics	0.00	1.00	1.00	1.00	1.00	0.00	0.00	1.00	1.00	1.00	1.00	0.00	1.00	0.00	1.00	0.00	0.00	0.00
Manufacturing	5.00	6.00	13.00	20.00	12.00	9.00	19.00	26.00	24.00	5.00	1.00	4.00	15.00	2.00	3.00	13.00	15.00	5.00
Marine	0.00	1.00	1.00	2.00	1.00	1.00	2.00	1.00	2.00	0.00	0.00	0.00	2.00	0.00	0.00	1.00	2.00	0.00
Mechanical Services	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00
Media	1.00	0.00	2.00	2.00	0.00	0.00	2.00	1.00	2.00	0.00	0.00	0.00	1.00	1.00	0.00	0.00	1.00	0.00
Non-Profit	0.00	0.00	1.00	1.00	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Professional Training ..	0.00	0.00	1.00	1.00	1.00	0.00	1.00	1.00	1.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00
Real Estate	0.00	0.00	1.00	1.00	2.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00
recruitment	0.00	0.00	0.00	0.00	0.00	0.00	1.00	1.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Retail	0.00	1.00	4.00	5.00	6.00	2.00	5.00	6.00	4.00	0.00	0.00	1.00	6.00	0.00	0.00	0.00	2.00	0.00
Trade	0.00	0.00	1.00	1.00	1.00	0.00	0.00	1.00	1.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00
Transportation & Logi..	2.00	3.00	8.00	9.00	6.00	6.00	8.00	11.00	12.00	0.00	0.00	0.00	9.00	2.00	0.00	1.00	4.00	0.00
Travel & Tourism	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	2.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00

Figure 8. Heatmap of Different Industries and Data Types

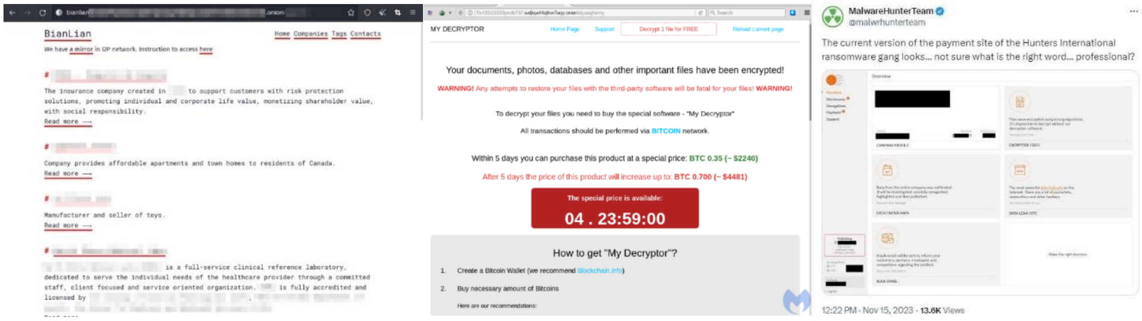
The graph above reveals that threat actors target specific data types depending on the industry. While financial information is consistently sought across companies from all industries, several other types of data targeted vary significantly by sector, with different industries facing unique risks based on their specific vulnerabilities. We will now compare the different data types aimed at by threat actors across industries that have been most prone to ransomware threats:

- Healthcare: The healthcare industry experiences an influx of attacks targeting personal information of their patients and employees, and their databases. The type of data stolen from the healthcare industry is typically sensitive and therefore extremely valuable for threat actors to exploit. Moreover, medical information is required to be readily available, which threat actors leverage on when withholding the information until a ransom is paid.

- Manufacturing, Construction, and Logistics: Companies in the manufacturing, construction, and logistics industries suffer heavy data leaks of employee and company information, business deals, and individual research and designs. Information in these industries is heavily guarded and secretive as it is not to be revealed to competitors. Hence, they hold high value which may attract threat actors.
- Finance, Law, IT: In addition, companies in the finance, law and IT industries lose personal and company information and business deals, and the companies in the law industry are additionally targeted for government information as well. Information in these industries is sought after due to their sensitivity and importance to critical infrastructure and services. Hence, threat actors may target this information for financial gain as well.

6. What are the 3 interesting insights the group observed?

6.1 Design of Payment Site of Ransomware Groups



BianLian

Home Companies Tags Contacts

We have a mirror in I2P network. Instruction to access here

[redacted]

The insurance company created in [redacted] to support customers with risk protection solutions, promoting individual and corporate life value, monetizing shareholder value, with social responsibility.
Read more →

[redacted]

Company provides affordable apartments and town homes to residents of Canada.
Read more →

[redacted]

Manufacturer and seller of toys.
Read more →

[redacted]

[redacted] is a full-service clinical reference laboratory, dedicated to serve the individual needs of the healthcare provider through a committed staff, client focused and service oriented organization. [redacted] is fully accredited and licensed by [redacted]

MY DECRYPTOR

Home Page Support Decrypt 1 file for FREE Reload current page

Your documents, photos, databases and other important files have been encrypted!

WARNING! Any attempts to restore your files with the third-party software will be fatal for your files! WARNING!

To decrypt your files you need to buy the special software - "My Decryptor"

All transactions should be performed via BITCOIN network.

Within 5 days you can purchase this product at a special price: BTC 0.35 (~ $2240)

After 5 days the price of this product will increase up to: BTC 0.700 (~ $4481)

The special price is available:
04 . 23:59:00

How to get "My Decryptor"?

1. Create a Bitcoin Wallet (we recommend Blockchain.info)
2. Buy necessary amount of Bitcoins

Here are our recommendations:

MalwareHunterTeam
@malwrhunterteam

The current version of the payment site of the Hunters International ransomware gang looks... not sure what is the right word... professional?

Overview

[redacted]

COMPANY PROFILE

ENCRYPTED FILES

EXFILTRATED DATA

DATA LEAK SITE

BULK EMAIL

12:22 PM · Nov 15, 2023 · 13.6K Views

Figure 9. Typical Ransomware Sites (Left and Middle) versus Hunters International (Right)

Referring to Figure 9, compared to other ransomware payment sites, Hunters International's design appears to prioritize an easy experience for victims, resembling a user-friendly e-commerce platform. This approach minimizes psychological and technical barriers, making it easier for victims to complete the ransom transaction. This plays into psychological manipulation of the victims and reduces their emotional resistance to paying the ransom by subtly shifting victims' mindsets to viewing the ransom payment as a transactional necessity rather than an extortion. Additionally, the attention to detail in the design style may be a strategic choice aimed at impressing potential affiliates and conveying an image of sophistication that establishes their brand image, and signal that they are serious in their operations and any attempt by the victims to thwart their actions will be futile.

6.2 Increased Ransomware Threat Groups' Activity in April 2024

Threat actor groups frequently exploit time periods of high-pressure and activity to execute their attacks seamlessly and conceal their actions. One such common period favoured by ransomware actors is particularly the dates leading up to key tax filling season in the target countries. From our analysis in Figure 1, we note that the US had been the most heavily targeted and had been susceptible to the highest number of ransomware attacks by the four threat groups, accounting for 63.23% of the total attacks analysed. It is also prudent to note that the tax deadline in US falls on April 15, during which companies and individuals may be caught up in communications pertaining to tax relations, which enlarges their attack surface and introduces more vulnerabilities for threat actors to exploit.

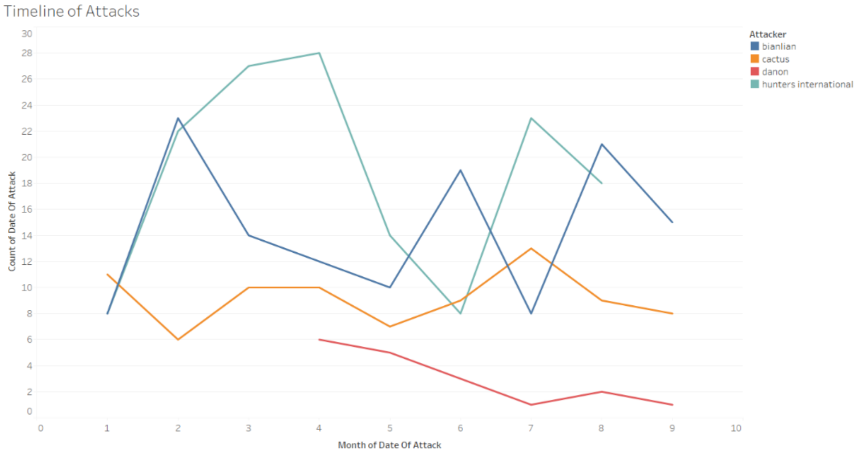


Figure 11. Timeline of Attacks (By Month) for Each Group

From Figure 11, it can be observed that three out of the four threat groups had experienced a significant surge of activity in April, with Hunters International reaching its peak number of attacks during this period. This heightened activity could have a possible attribution to an increase in phishing emails impersonating tax authorities or councils, which are already known to be the 8th most common type of phishing email attacks [8]. The urgency and confusion faced by the public offers threat actors the perfect opportunity to establish a foothold in critical infrastructure of targeted organisations and conduct a successful attack, where they extract their intended data.

6.3 Target Selection Strategies: Divergent Approaches in Ransomware Attacks

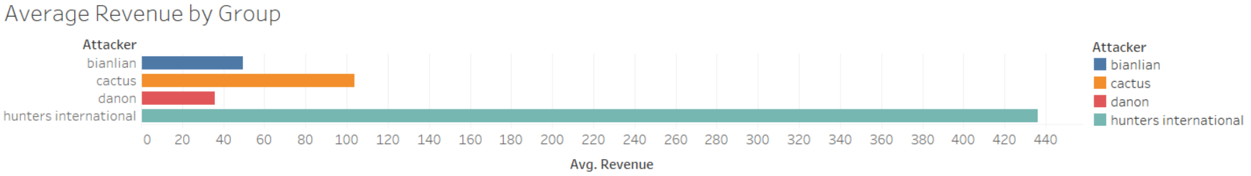


Figure 12. Average Revenue of Victims Targeted for Each Group

Assuming revenue is the primary indicator of a company's market position and size, Figure 12 shows that majority of the ransomware groups analysed had a higher attack count for small and medium-sized companies, with Hunters International being the only exception, targeting higher profile and wealthier companies instead.

There has been a rising trend where ransomware groups have been gravitating towards attacking smaller businesses. LockBit, known to historically dominate the cybercrime world, was reported to have attacked the greatest number of small businesses in the Sophos Incident Response, 2023 report [9]. This can be attributed to the negligence of the security standing of small businesses, who may invest more resources in establishing their business in their respective industries and increasing their revenue instead. The vulnerable standpoint of these organisations may also prompt a victim company to be more likely to pay the ransom, as the loss they experience during an attack is more impactful. Small organisations also pose as a gateway to a larger enterprise, which is a route of less resistance for ransomware groups to undertake compared to attacking larger enterprises head on and overcoming their high-end, complex security services [10].

Hunters International, on the other hand, adopts a high-risk, high-reward hunting strategy and consistently targets larger companies instead. Interestingly, this RaaS group is relatively new, having garnered public attention only in October 2023, and has already been described as a "rapidly rising group" [11]. The deviation from the prevailing trend where even prominent ransomware groups targets small businesses suggests a strategic approach: by breaching the seemingly unbreakable security systems of large businesses, Hunters International may be aiming to increase its popularity and bolster its reputation. Moreover, successfully compromising high-profile targets also enhances the ransomware group's perceived skill level, instilling greater fear and respect among future potential victims. As a result, companies may take the group more seriously in subsequent attacks, reflecting the group's growing influence and capability.

7. What we learnt, what were our struggles in executing the project and how did we overcome them?

Distributed Denial of Service (DDoS) protection was put in place using CAPTCHA on the Dedicated Leak Sites (DLS) to prevent scraping. Additionally, certain groups with high attack counts did not provide the necessary information we needed for this project. Thus, we decided to choose threat actors that did not have CAPTCHA implemented on their DLS and that had the necessary information.

Additionally, different DLS had different layouts. This made it impossible to use the same scraping script for all the DLSs. Therefore, each DLS had their separate individual scraping script. To ensure consistency in the columns of the final CSV file, the group agreed on the information to be retrieved from the DLSs.

Another challenge was that data values across threat actors can vary. For example, United States in one DLS may be "United States" while another may be "US". To address this, we standardised values in our data cleaning.

It is also important to note that at this current time of the report, Cactus has more leaks than bianlian whereas bianlian had more records at the time we were scrapping data. Thus, analysis and conclusions may change with new information.

8. References

1) https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a
2) https://www.bitdefender.com/en-us/blog/businessinsights/hive-ransomwares-offspring-hunters-international-takes-the-stage/
3) https://blog.barracuda.com/2024/07/29/hunters-international--your-data-is-the-prey

4) https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-321a
5) https://www.cisa.gov/stopransomware
6) https://netenrich.com/blog/hunters-international-group-dls-identity-exposure

7) https://www.acronis.com/en-sg/cyber-protection-center/posts/hunters-international-new-ransomware-based-on-hive-source-code/
8) https://blog.usecure.io/the-most-common-examples-of-a-phishing-email
9) https://news.sophos.com/en-us/2024/03/12/2024-sophos-threat-report/
10) https://carlscomputercare.com/smaller-businesses-ransomware/
11) https://adarma.com/blog/hunters-ransomware-group/#:~:text=Now%20established%20as%20a%20major,their%20approach%20apart%20from%20Hive's

9. Appendix

2.1 Analysis of Competing Hypothesis

TABLE I
HYPOTHESIS

Label	Question	Hypothesis
H1	Do ransomware groups favour targeting developed / high-income countries?	Developed / High-income countries are being targeted more compared to the rest of the world.
H2	Are ransomware groups targeting corporations with valuable / sensitive data / operations?	Ransomware groups are targeting corporations with valuable / sensitive data / operations.
H3	Are ransomware groups aiming for financial gains, or are they acting has hacktivists or nation state actors?	Ransomware groups are aiming for financial gains, and not for hacktivism or as nation state actors.

TABLE II
EVIDENCE

Label	Factor	Brief Explanation
E1	Target Victim (Geography)	Statistics shown that more than 85% attacks happen on developed / high-income countries.
E2	Industry Sector (Data)	Attackers are inclined to target certain industries that handles valuable or sensitive information, which the attackers could use as leverage against information owners. These sectors include Healthcare, Design and Law.
E3	Industry Sector (Service)	Ransomware groups target corporations that offer crucial service to a wide range of customers, having service downtime could potentially impact company's operations. These sectors include Healthcare, IT services and Finance.
E4	Target Victim (Financial)	Ransomware groups target corporations that has a higher financial capability to pay of the ransom.

TABLE III
ASSESSMENT

Evidence / Hypotheses	H1	H2	H3

E1	++	N	++
E2	N	++	+
E3	N	++	+
E4	+	N	++

++: Very consistent, +: Consistent, N: Neutral / Non-applicable, -: Inconsistent, --: Very inconsistent

3.1 Information on RansomHub

RansomHub is the most active group with more than 200 attacks in the last 90 days. RansomHub is a ransomware-as-a-service variant—formerly known as Cyclops and Knight—that has established itself as an efficient and successful service model (recently attracting high-profile affiliates from other prominent variants such as LockBit and ALPHV). The affiliates leverage a double-extortion model by encrypting systems and exfiltrating data to extort victims. It should be noted that data exfiltration methods are dependent on the affiliate conducting the network compromise. The ransom note dropped during encryption does not generally include an initial ransom demand or payment instructions. Instead, the note provides victims with a client ID and instructs them to contact the ransomware group via a unique .onion URL (reachable through the Tor browser). The ransom note typically gives victims between three and 90 days to pay the ransom (depending on the affiliate) before the ransomware group publishes their data on the RansomHub Tor data leak site.

3.2 IoC for Hunter's International

Type	**IoC**	**Description**
SHA256	94b6cf6c30f525614672a94b8b9788b46cbe061f89ccbb994507406404e027af	Ransomware sample
SHA256	c4d39db132b92514085fe269db90511484b7abe4620286f6b0a30aa475f64c3e	Ransomware sample

MITRE ATT&CK Technique

Data Encrypted for Impact	T1486	Threat actors deploy a ransom note HOW_TO_DECRYPT.txt into each affected directory which states the *.key file cannot be modified, renamed, or deleted, otherwise the encrypted files cannot be recovered.
Phishing	T1566.001	Threat actors gain access to victim networks by distributing phishing emails with malicious attachments.
External Remote Services	T1133	Threat actors gain access to victim networks by using single factor logins via RDP, VPN, and other remote network connection protocols.
Exploit Public-Facing Application	T1190	Threat actors gain access to victim network by exploiting the following Microsoft Exchange vulnerabilities: CVE-2021-34473, CVE-2021-34523, CVE-2021-31207, CVE-2021-42321.
Impair Defenses	T1562	Threat actors disable security software and monitoring tools, modify firewall rules to allow for undetected data exfiltration

		and tamper with logging mechanisms, allowing them to operate undetected within the network for extended periods.
Boot or Logon AutoStart Execution	T1547	Threat actors maintain persistence by modifying Windows Registry run keys and startup folders to include ransomware software.
System Information Discovery	T1082	Threat actors gather detailed information about the compromised systems and network architecture and locate critical data for exfiltration.