NANYANG
TECHNOLOGICAL
UNIVERSITY
SINGAPORE

CZ4070 - Cyber Threat Intelligence

Project 1 Report

30th September 2022

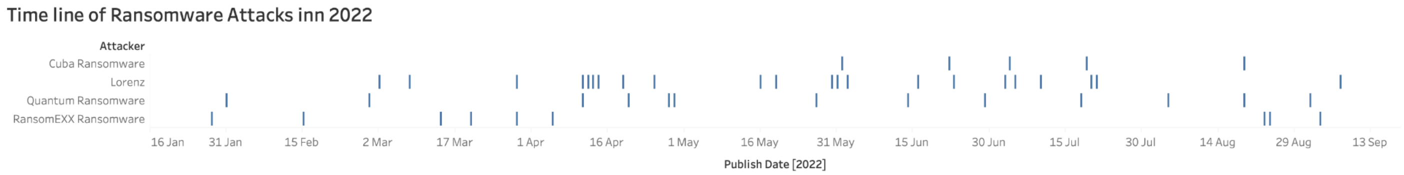
Group 1 :

Group Members	Matriculation Number
Astha Garg	U1923971H
Agnesh Ramesh	U1921141K
Bachhas Nikita	U1921630F
Unnikrishnan Malavika	U1923322E
Lee Lucius	U1922868B
Kondreddy Saitejareddy	U1923841F

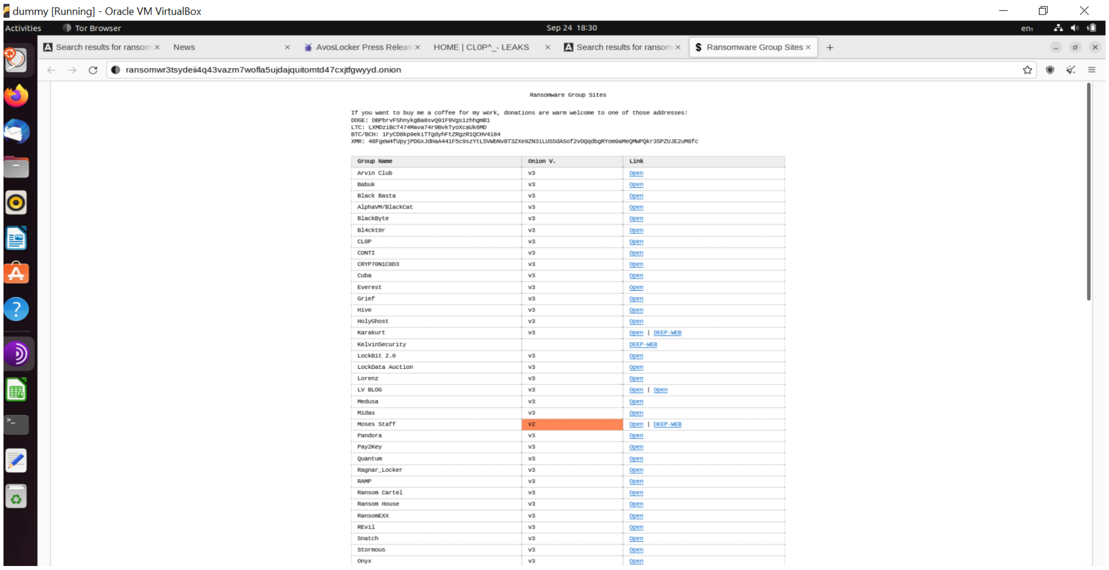
Overview

The following data has been scrapped from various websites across the dark web using the Tor browser. For this report, we will be focusing on four different ransomware groups: Quantum, RansomEXX, Cuba and Lorenz.

The figure below shows the timeline for the attacks that have occurred over the span of 9 months from January to September 2022.



An interesting insight is that an increase in ransomware activity could be seen between the months of April and May and June - August.


dummy [Running] - Oracle VM VirtualBox
Activities
Tor Browser
Sep 24 18:30
en
Search results for ransom
News
AvosLocker Press Releas
HOME | CL0P^_- LEAKS
Search results for ransom
Ransomware Group Sites
ransomwr3tsydeii4q43vazm7wofla5ujdajquitomtd47cxjtfgwyyd.onion

Ransomware Group Sites

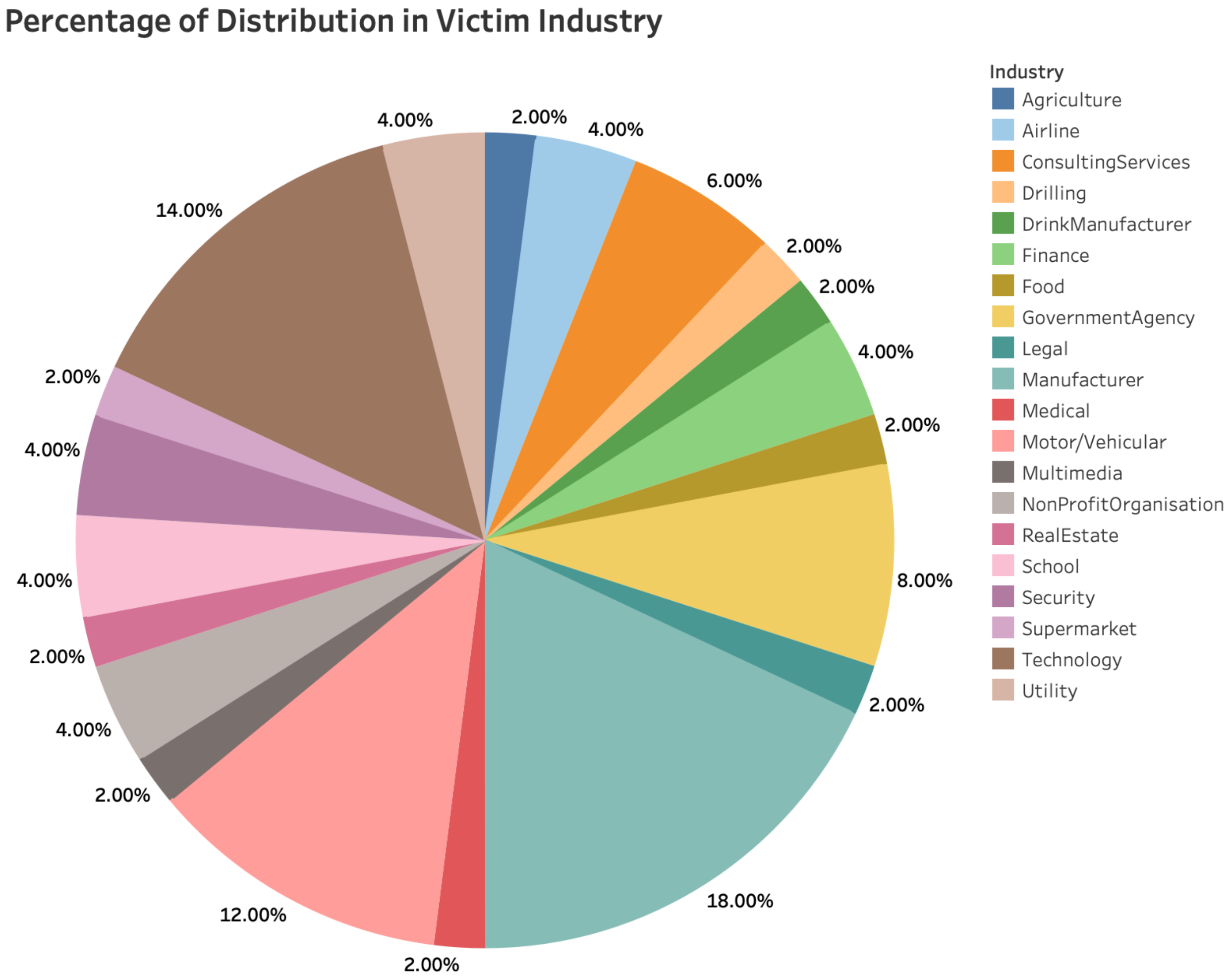
If you want to buy me a coffee for my work, donations are warm welcome to one of those addresses:
DOGE: DBPbrvFShnykgBa8svQ91F9Vgs1zhhgmB1
LTC: LXMDziBcT474Mava74r9BvkTyoXcaUk6MD
BTC/BCH: 1FyCD8kp9ekiTTgdyhFtZRgzR1QCHV4i84
XMR: 48FgeW4fUpyjPDGxJdHaA441F5c9szYtLSVWbNv8T3ZXe9ZN3iLUSSdASof2vDQqdbgRYom9aMeQMWPQkr3SPZUJE2uM8fc

Group Name	Onion V.	Link
Arvin Club	v3	Open
Babuk	v3	Open
Black Basta	v3	Open
AlphaVM/BlackCat	v3	Open
BlackByte	v3	Open
Bl4ckt0r	v3	Open
CL0P	v3	Open
CONTI	v3	Open
CRYP70N1C0D3	v3	Open
Cuba	v3	Open
Everest	v3	Open
Grief	v3	Open
Hive	v3	Open
HolyGhost	v3	Open
Karakurt	v3	Open | DEEP-WEB
KelvinSecurity		DEEP-WEB
LockBit 2.0	v3	Open
LockData Auction	v3	Open
Lorenz	v3	Open
LV BLOG	v3	Open | Open
Medusa	v3	Open
Midas	v3	Open
Moses Staff	v2	Open | DEEP-WEB
Pandora	v3	Open
Pay2Key	v3	Open
Quantum	v3	Open
Ragnar_Locker	v3	Open
RAMP	v3	Open
Ransom Cartel	v3	Open
Ransom House	v3	Open
RansomEXX	v3	Open
REvil	v3	Open
Snatch	v3	Open
Stormous	v3	Open
Onyx	v3	Open

Q1.1 What is the % distribution in the Victim Industry?

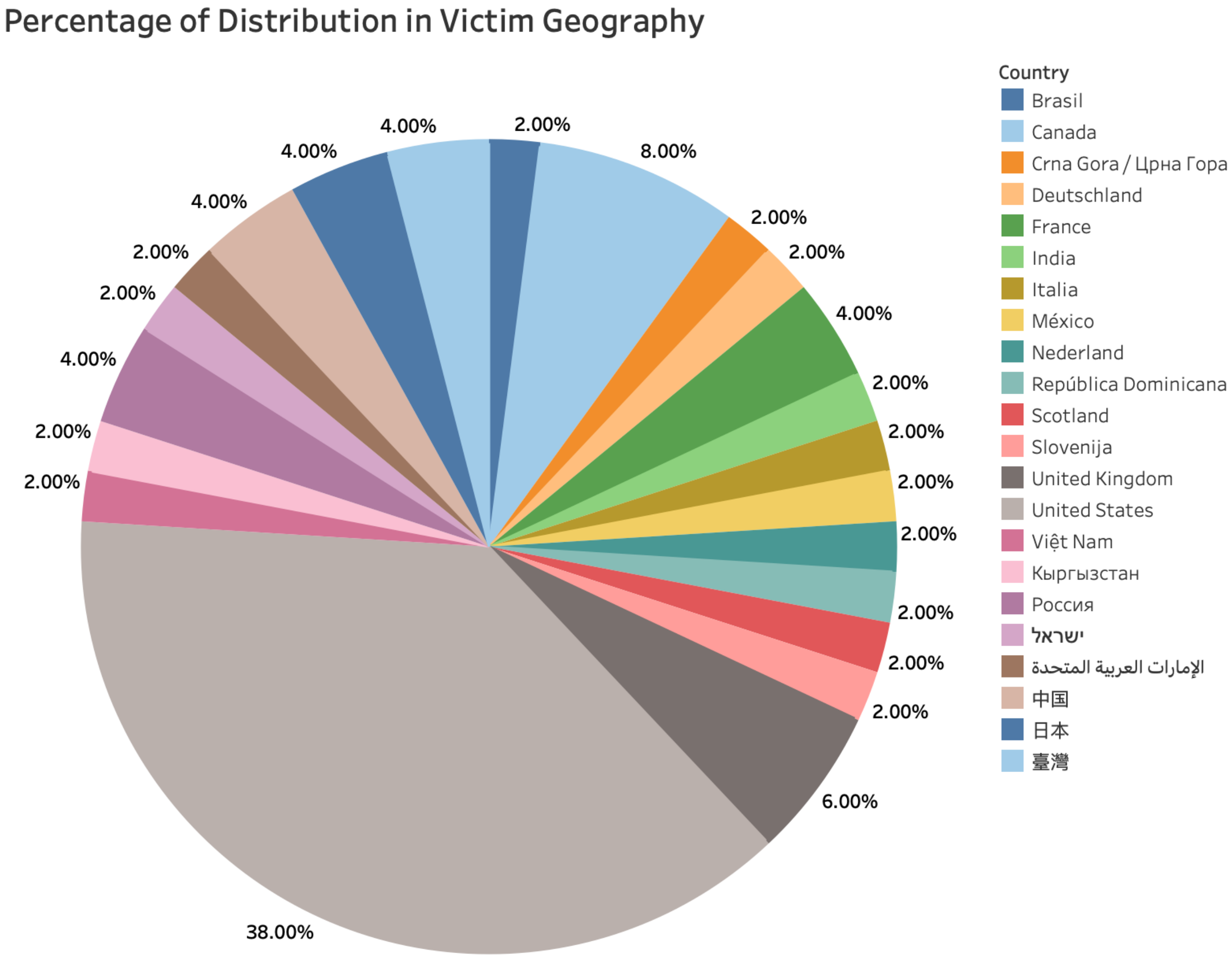
By analyzing the victim industries from the collected data, we were able to conclude that the manufacturing industry was the most targeted, making up 18% of all the sectors collected. The second highest percentage is the Technology industry at 14% closely followed by the Motor/Vehicular Industry at 12%.

Even though the numbers might not be significant, it is important to note that the attacks have targeted a wide range of industries.



Q1.2 What is the % distribution in the Victim Geography?

Unlike industry distribution, location is more focused to specific areas and isn't quite as widespread. The continents of North America (46%) and Europe (20%) are the most affected. Additionally, from the data collected, we did not see any attacks in Africa or Australia.

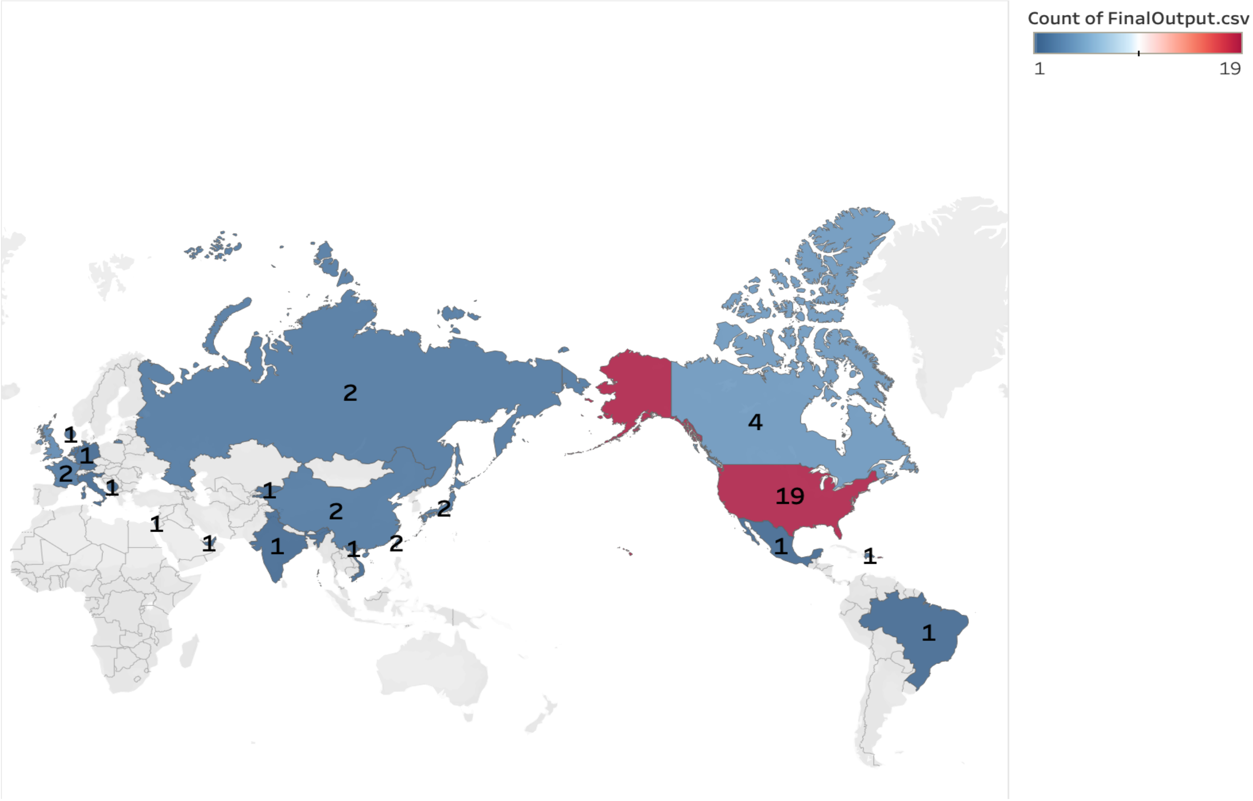


Q2.1 What Countries are most Targeted By Ransomware Actors?

Top 3 countries in order of being target by ransomware actors (high to low)

1. The United States of America
2. Canada
3. The United Kingdom

Countries most targeted by Ransomware actors

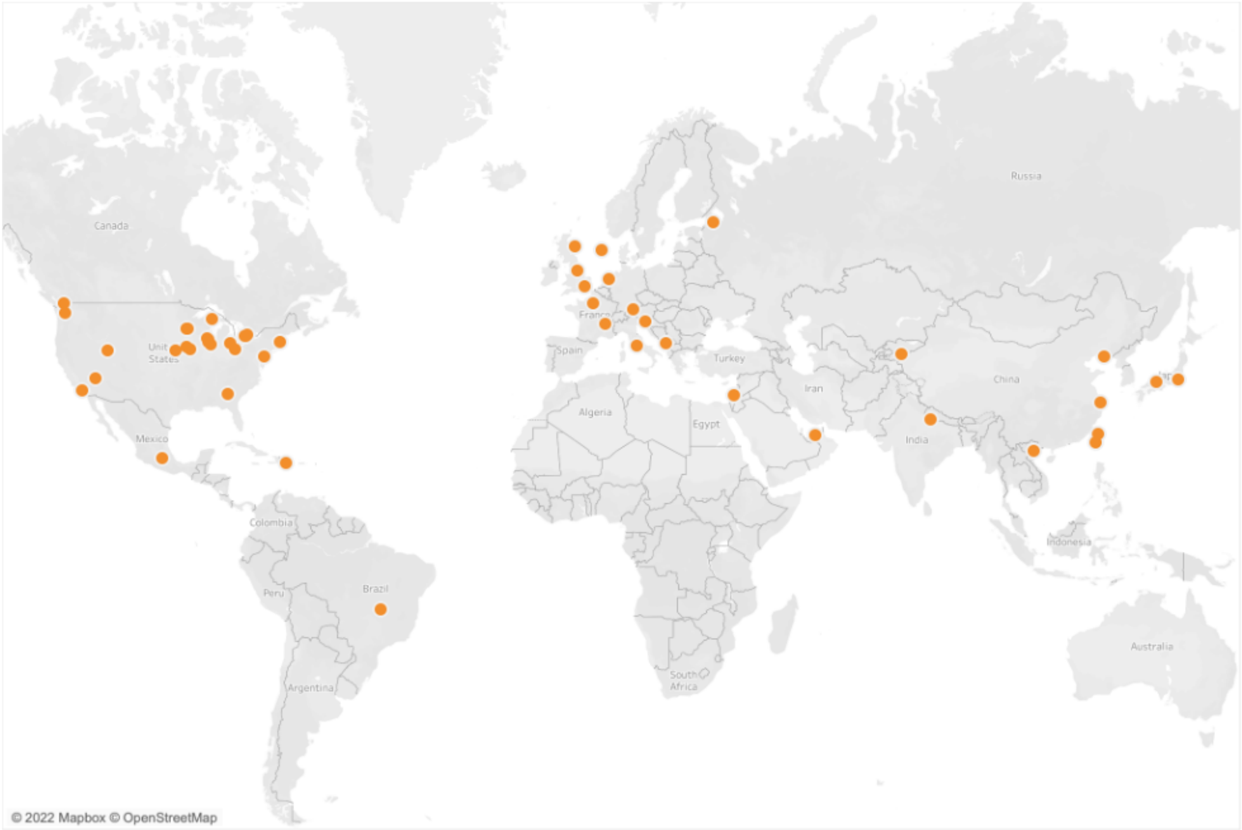


Q2.2 Why are some more targeted than others?

There could be a couple of reasons why some countries are targeted more than others. The first consideration would be how easy it is to attack a particular country. Countries in Europe and North America have more digitalisation of information which means more data is available on digital systems / the internet and therefore is more likely to be exposed to exploits. Another reason could be due to geo-political dynamics. Some attacks could be targeted at specific countries due to recent political events that have upset the attacker.

A study carried out by the BBC showed that ransomware attacks have increased in the United Kingdom as firms are more likely to pay the hackers, allowing them to achieve their financial objective.

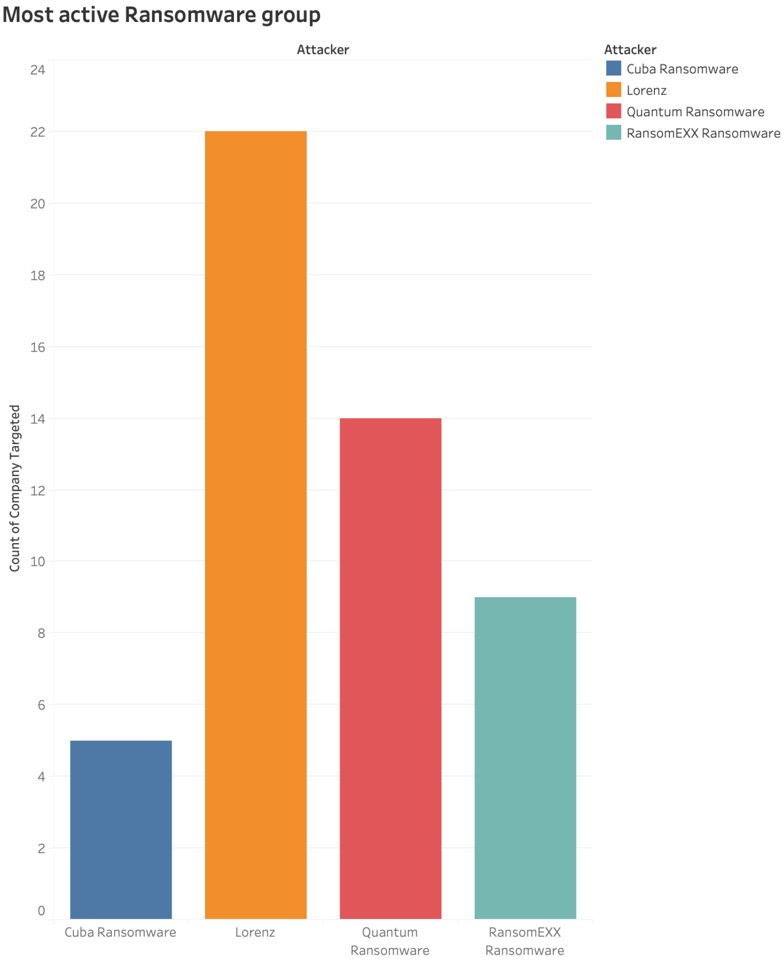
Countries Targeted by Ransomware Groups



Map based on Longitude and Latitude.

Q3.1 Which Ransomware group is the most active?

Since the start of this year, the ransomware group Lorenz has been the most active amongst the 4 groups we studied. Lorenz attacked a total of 22 companies while the second highest group - Quantum attacked 14.



Q3.2 What is so unique about their TTP that makes them so “successful”?

Lorenz, a ransomware strain first identified in February 2021, is thought to be a rebranded version of the ".sZ40" ransomware that was initially identified in October 2020. Lorenz targets businesses all around the world with targeted attacks that seek ransom payments of tens of thousands to several million dollars.

According to its website, the gang has published stolen data from more than 20 victims, but the actual number of successful attacks is thought to be greater. The group mostly targets victims in English-speaking nations.

Tactics, Techniques and Procedures (TTPs)

As a part of their attack strategy, first, Employees, suppliers, and partners of their target are investigated. The Lorenz group moves from one victim who has already been corrupted to another in this manner. They use the information they've gathered to tailor the attack to the victim specifically. In a known incident, the attackers "jumped" from one victim who had been compromised to another. Through a sophisticated phishing email, the group was able to access the network. After conducting research on the target, the group sent the email from an actual employee's account at a supplier that they had already infiltrated. The likelihood of someone falling for the scam increases because the email seems more realistic.

Lorenz was observed utilizing known tools to do credential dumping and subsequent network and domain enumeration. The gang then proceeded to move laterally by utilizing compromised credentials for two privileged administrator accounts, one of which had domain admin access.

According to Arctic Wolf Labs, Lorenz recently attacked a target and used the remote code execution flaw in MiVoice Connect, CVE-2022-29499, to acquire a reverse shell inside the victim's network. The discovered tactics, tools, and procedures (TTPs) are similar to those described in a CrowdStrike report from June describing an incursion by a ransomware gang that used the same vulnerability. Lorenz utilized the open source TCP tunneling tool Chisel to migrate laterally in the environment after the initial intrusion.

To compel victims to pay the ransom, Lorenz first sells the data to other threat actors or potential competitors. As time passes, they begin to distribute password-protected RAR archives containing the victim's data. If a ransom is not paid, Lorenz releases the stolen material to the public.

The gang extracts data from the surroundings before encrypting the victim's files by using the file-sharing application FileZIlla. It then encrypts the victim's files using the official BitLocker tool by executing a forged file directly on the domain controller.

The Lorenz operators have designed a novel attack strategy. Lorenz offers access to a victim's internal network for sale.

The ransomware's capabilities and behavior are frequently altered by the Lorenz gang, making it unique to each victim. These are the most important factors which makes Lorenz unique and more successful than the others.

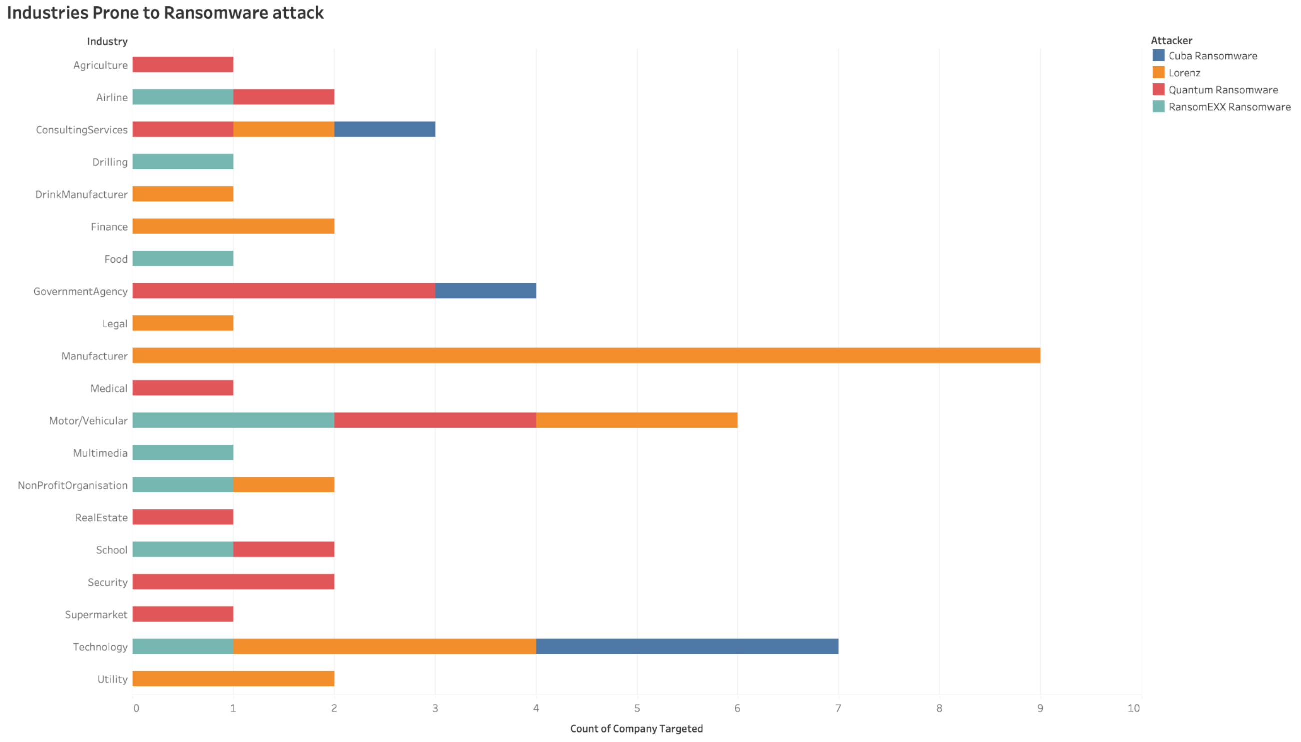
Q4. Which Industries Are More Prone To Ransomware Threats? Why?

As shown in the representation below it was observed that the manufacturing industry has had the highest number of attacks. An interesting observation is that all the attacks on manufacturing companies were carried out by a single group - Lorenz. Another industry exposed to a higher number of attacks is the technology industry, covering about 14 percent of the attacks studied here. This industry was targeted by multiple ransomware groups.

It is interesting to also note that most of these companies are actually not big conglomerates but are Small and Medium Enterprises (SME).

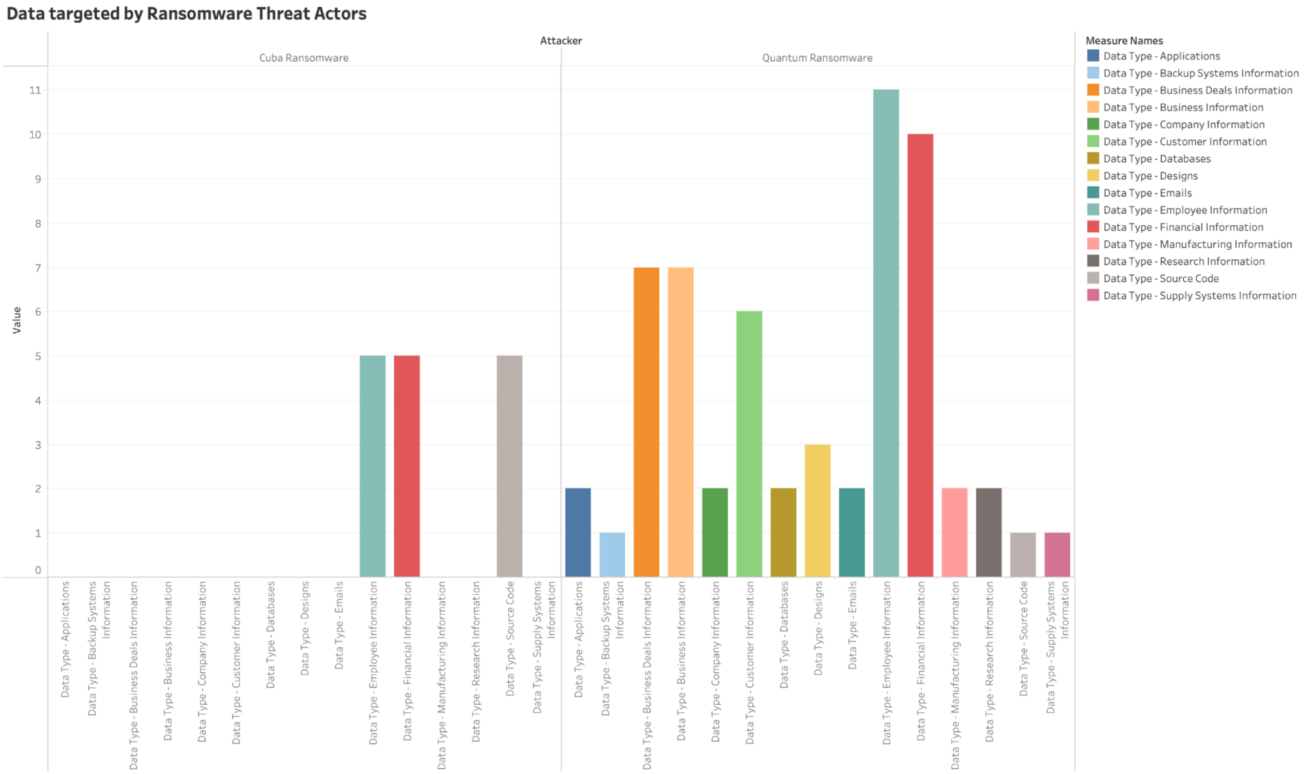
Why Manufacturing?

Threat actors understand the critical role manufacturing and energy play in global supply chains and are seeking to disrupt these organizations because of the ripple effect it can have across multiple industries and the pressure these multiplying effects create for victims to pay a ransom.



Q5.1 We know actors target sensitive data, but what kind of data do actors usually target?

**Information for the RansomExx and the Lorenz ransomware are not available*



The graph below shows the different types of data that ransomware attackers like to steal.

From our observation, we have found that the top three types of data stolen by ransomware groups are Employee Information, Financial Information, Business information and Business Deal Information.

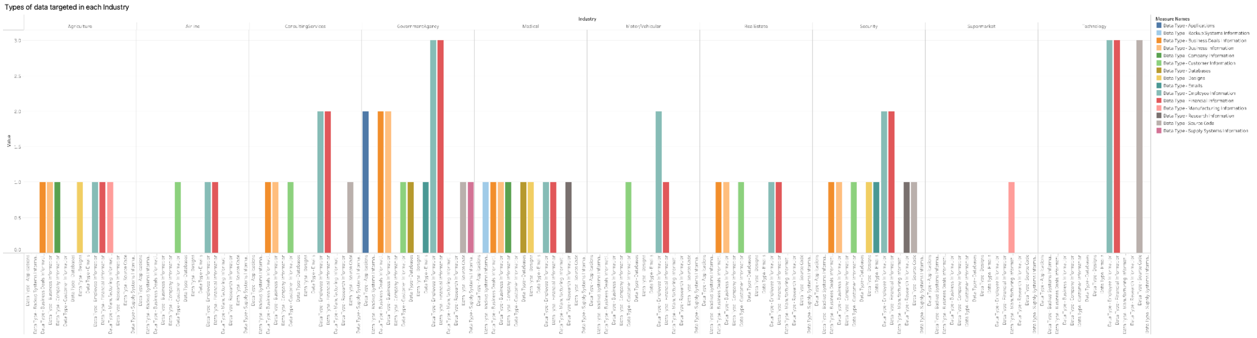
These observations align with the information we have learnt thus far in the Cyber Threat Intelligence module.

1. **Employee Information:** For easier access into systems, ransomware attackers prefer to steal employee credentials. This allows them to not waste resources and time brute-forcing their way in and also allows them to go undetected for a longer period of time, giving them the opportunity to encrypt the data and take control over the system.

2. **Financial Information**: Attackers use the financial information obtained to gauge the ransom amount they can collect from the victim. The price to return data for a higher revenue company will likely be higher than a SME with lesser revenue.
3. **Business and Business Deal Information:** Lastly, business deals and other business information are sensitive data that the companies would want to keep confidential to avoid exploitation of information like merger, intellectual property, etc. Ransomwares can take advantage of this by selling this information on the dark web and earning additional sums for it.

Q5.2 What are the kinds of data targeted in each industry?

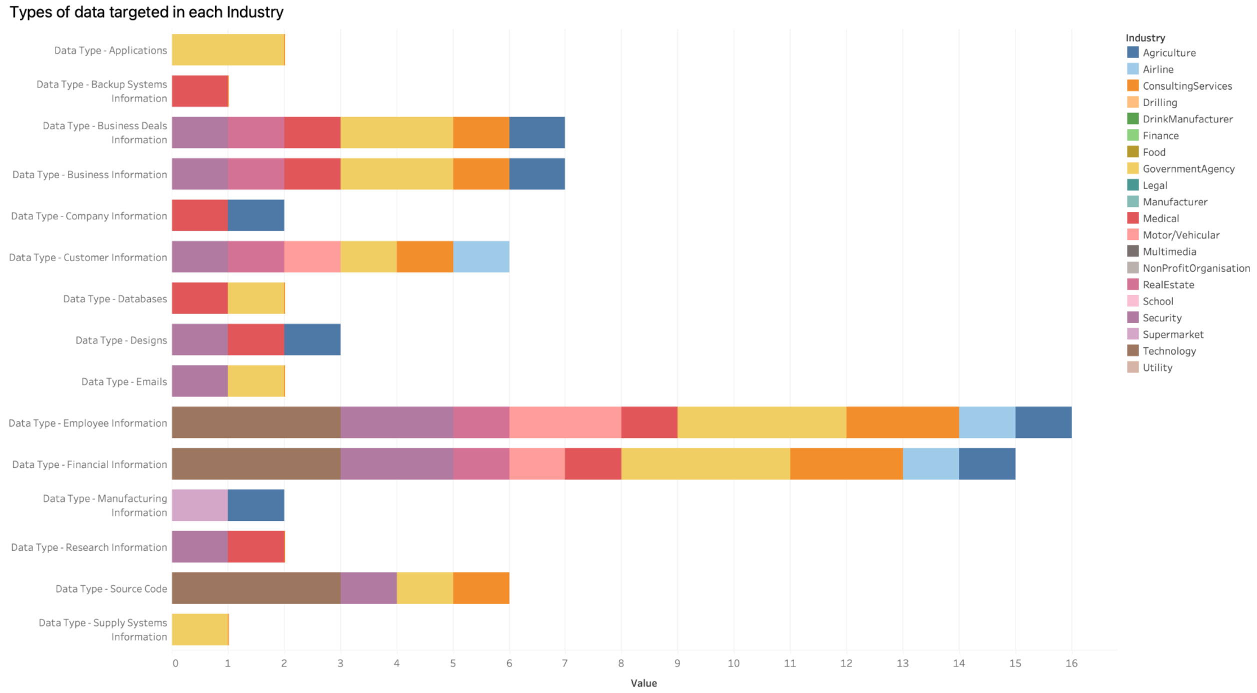
**Information for the Drilling, DrinkManufacturer, Finance, Food, Legal, Manufacturing, Multimedia, NonProfitOrganisation, School and Utility industry is not available.*



**Please refer to attached (5.2.1.png) for clearer image*

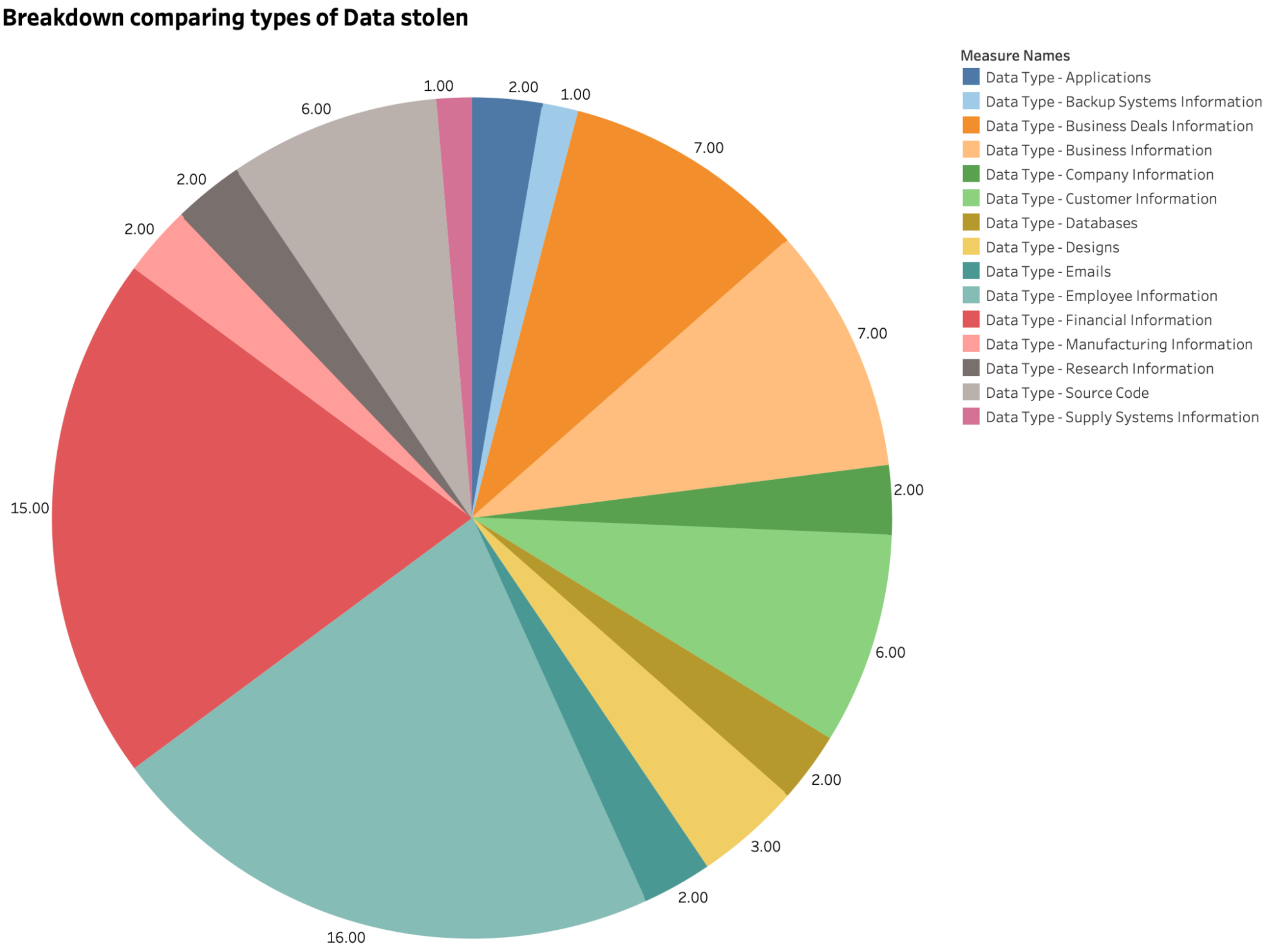
It can be observed that within each industry the attackers give the employee and the financial information equal if not more importance as the other information. While the attackers focused on stealing source code from the companies in the Technology industry, they focused more on customer information and business deals when it came to the consultant services, government agencies (highest), real estate and security industries.

Moreover, attackers also steal additional information regarding Research, Design, Databases, Company, and Backup System.



Q5.3 Show a breakdown comparing types of data stolen.

Based on the data collected, we have found that the top three types of data stolen by ransomware groups areEmployee Information, Financial Information, Business information and Business Deal Information. Ransomware groups are least interested in Backup systems information and Supply systems information.



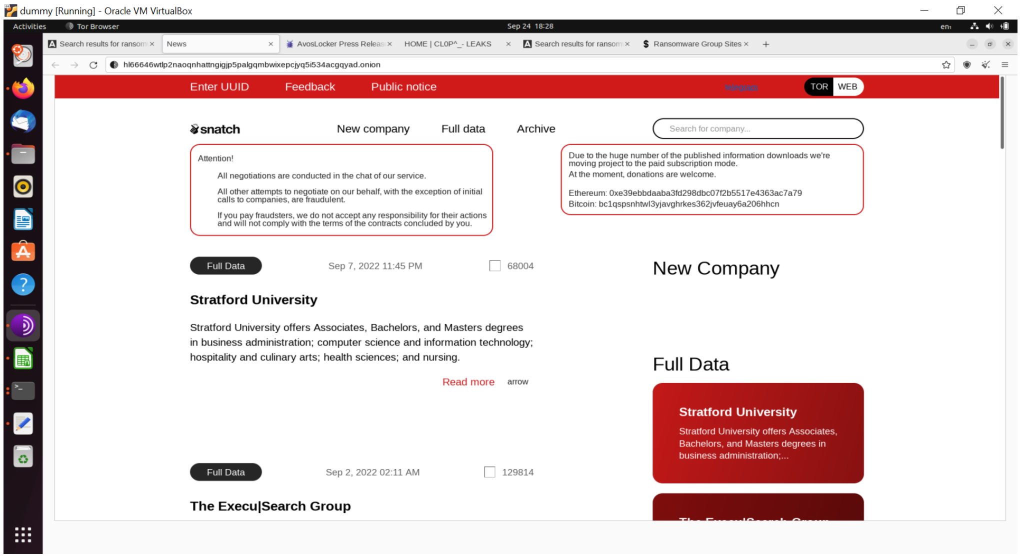
Q6. Any other interesting insights?

One thing we noticed in our analysis is that some of these ransomware groups just wanted to expose vulnerabilities in companies. They specifically mention that they do not wish to disrupt any organizational processes and just want to be paid in return for their discovery. Some ransomwares (like Snatch) even offer to teach the companies how to fix the vulnerabilities so that it wouldn't be exploited again.

Two groups that we had looked into and initially scraped were Vice Society and Snatch and both had very interesting profiles.

From our observation, Vice Society seemed to target only educational institutions and had published data samples of Staff, Student and Administrators' names and emails. It also had some information about the floor plans / maps of these institutions. This has been found to match the alert given by the Cybersecurity and Infrastructure Security Agency (CISA)

The second group we found interesting was Snatch. On their website in the dark web, they explicitly mention how they do not lock any data / disrupt any supply chain processes (see screenshots from data that we scraped, below).



hl66646wtlp2naoqnhattngigjp5palgqmbwixepcjyq5i534acgqyad.onion

Attention!

All negotiations are conducted in the chat of our service.

All other attempts to negotiate on our behalf, with the exception of initial calls to companies, are fraudulent.

If you pay fraudsters, we do not accept any responsibility for their actions and will not comply with the terms of the contracts concluded by you.

Due to the huge number of the published information downloads we're moving project to the paid subscription mode.
At the moment, donations are welcome.

Ethereum: 0xe39ebbdaaba3fd298dbc07f2b5517e4363ac7a79
Bitcoin: bc1qspsnhtwl3yjavghrkes362jvfeuay6a206hhcn

Full Data Sep 7, 2022 11:45 PM □ 68004

Stratford University

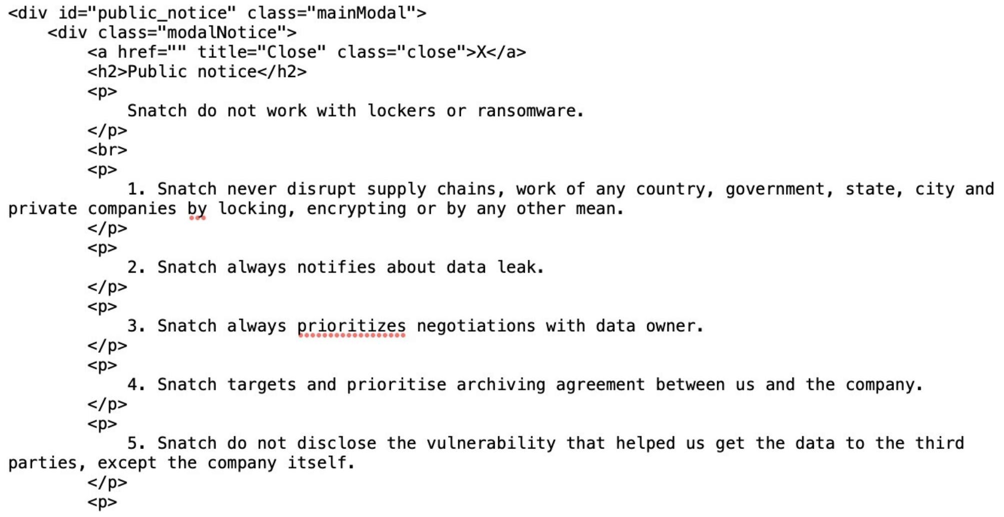
Stratford University offers Associates, Bachelors, and Masters degrees in business administration; computer science and information technology; hospitality and culinary arts; health sciences; and nursing.

Stratford University

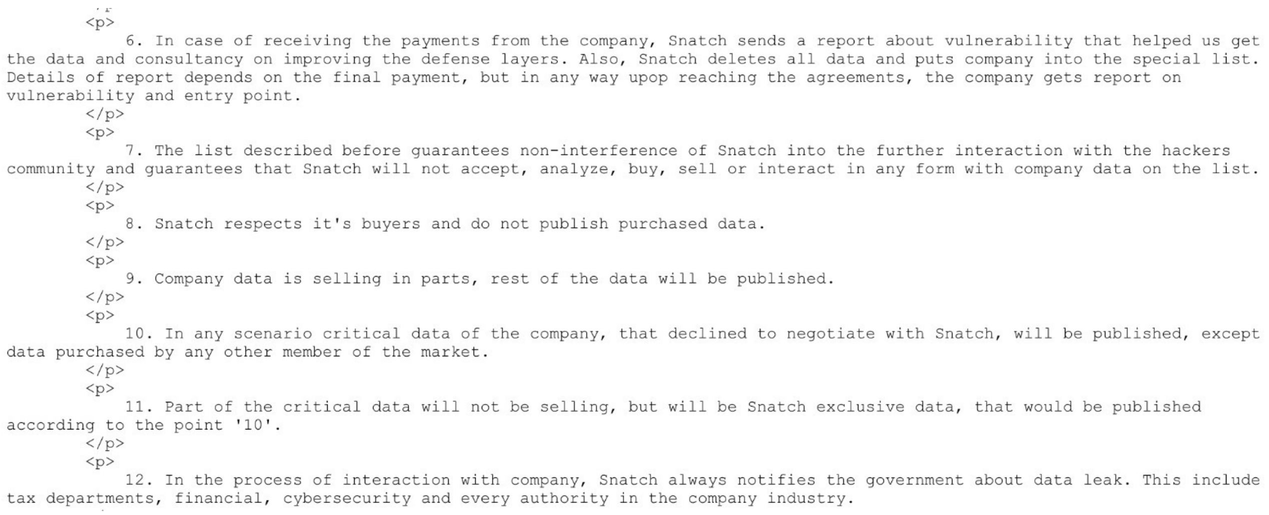
Stratford University offers Associates, Bachelors, and Masters degrees in business administration;...

Full Data Sep 2, 2022 02:11 AM □ 129814

The Execu|Search Group



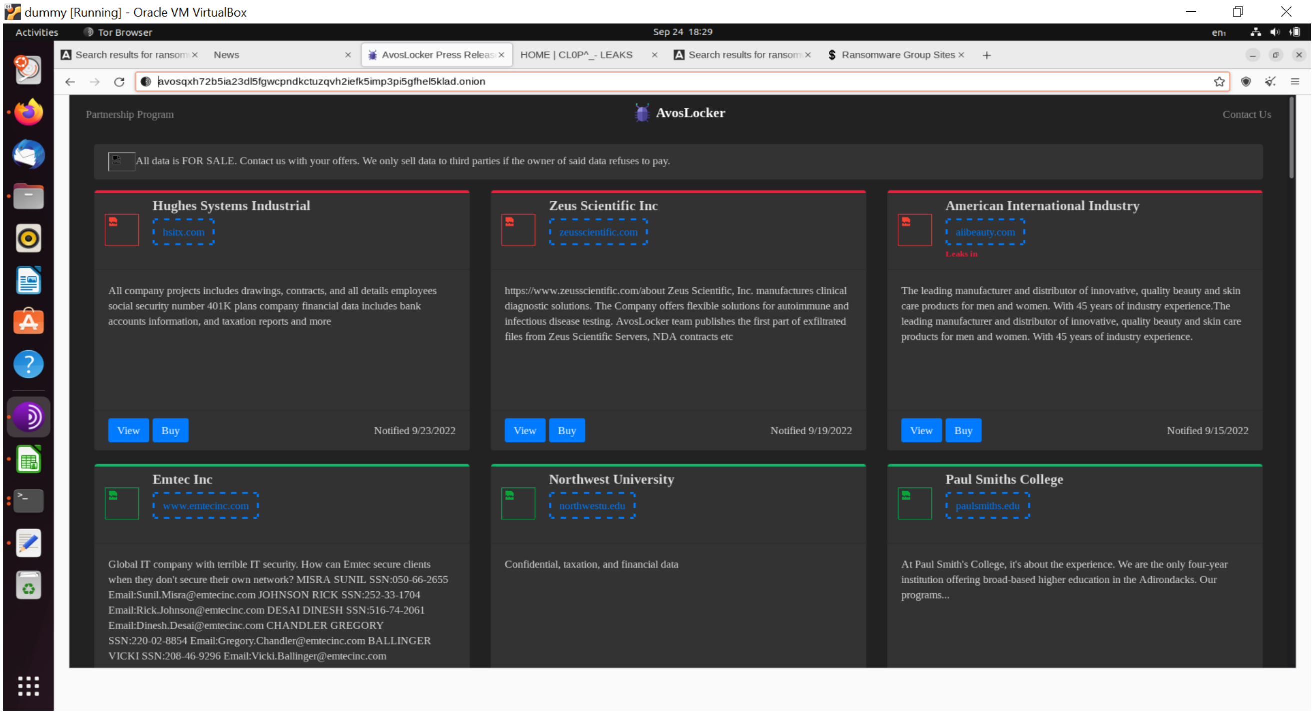
```
<div id="public_notice" class="mainModal">
    <div class="modalNotice">
        <a href="" title="Close" class="close">X</a>
        <h2>Public notice</h2>
        <p>
            Snatch do not work with lockers or ransomware.
        </p>
        <br>
        <p>
            1. Snatch never disrupt supply chains, work of any country, government, state, city and
private companies by locking, encrypting or by any other mean.
        </p>
        <p>
            2. Snatch always notifies about data leak.
        </p>
        <p>
            3. Snatch always prioritizes negotiations with data owner.
        </p>
        <p>
            4. Snatch targets and prioritise archiving agreement between us and the company.
        </p>
        <p>
            5. Snatch do not disclose the vulnerability that helped us get the data to the third
parties, except the company itself.
        </p>
        <p>
```



```
        <p>
            6. In case of receiving the payments from the company, Snatch sends a report about vulnerability that helped us get
the data and consultancy on improving the defense layers. Also, Snatch deletes all data and puts company into the special list.
Details of report depends on the final payment, but in any way upop reaching the agreements, the company gets report on
vulnerability and entry point.
        </p>
        <p>
            7. The list described before guarantees non-interference of Snatch into the further interaction with the hackers
community and guarantees that Snatch will not accept, analyze, buy, sell or interact in any form with company data on the list.
        </p>
        <p>
            8. Snatch respects it's buyers and do not publish purchased data.
        </p>
        <p>
            9. Company data is selling in parts, rest of the data will be published.
        </p>
        <p>
            10. In any scenario critical data of the company, that declined to negotiate with Snatch, will be published, except
data purchased by any other member of the market.
        </p>
        <p>
            11. Part of the critical data will not be selling, but will be Snatch exclusive data, that would be published
according to the point '10'.
        </p>
        <p>
            12. In the process of interaction with company, Snatch always notifies the government about data leak. This include
tax departments, financial, cybersecurity and every authority in the company industry.
```

Juxtaposed to this, the information we could find about Snatch Ransomware on the internet suggested they were using a windows vulnerability to enter the system and encrypting the files. They use a double extortion technique to get ransom from the victims. It is interesting to see that even though they do exploit system vulnerabilities and take ransom, **they do not want to label themselves as being associated with any ransomware / lockers**.

We also visited some marketplaces that were selling the data exfiltrated from a plethora of industries.



dummy [Running] - Oracle VM VirtualBox
Activities
Tor Browser
Sep 24 18:29
en
Search results for ransom
News
AvosLocker Press Releas
HOME | CL0P^_- LEAKS
Search results for ransom
Ransomware Group Sites
avosqxh72b5ia23dl5fgwcpndkctuzqvh2iefk5imp3pi5gfhel5klad.onion

Partnership Program

AvosLocker

Contact Us

All data is FOR SALE. Contact us with your offers. We only sell data to third parties if the owner of said data refuses to pay.

Hughes Systems Industrial

hsitx.com

All company projects includes drawings, contracts, and all details employees social security number 401K plans company financial data includes bank accounts information, and taxation reports and more

View Buy Notified 9/23/2022

Zeus Scientific Inc

zeusscientific.com

https://www.zeusscientific.com/about Zeus Scientific, Inc. manufactures clinical diagnostic solutions. The Company offers flexible solutions for autoimmune and infectious disease testing. AvosLocker team publishes the first part of exfiltrated files from Zeus Scientific Servers, NDA contracts etc

View Buy Notified 9/19/2022

American International Industry

aiibeauty.com

Leaks in

The leading manufacturer and distributor of innovative, quality beauty and skin care products for men and women. With 45 years of industry experience.The leading manufacturer and distributor of innovative, quality beauty and skin care products for men and women. With 45 years of industry experience.

View Buy Notified 9/15/2022

Emtec Inc

www.emtecinc.com

Global IT company with terrible IT security. How can Emtec secure clients when they don't secure their own network? MISRA SUNIL SSN:050-66-2655 Email:Sunil.Misra@emtecinc.com JOHNSON RICK SSN:252-33-1704 Email:Rick.Johnson@emtecinc.com DESAI DINESH SSN:516-74-2061 Email:Dinesh.Desai@emtecinc.com CHANDLER GREGORY SSN:220-02-8854 Email:Gregory.Chandler@emtecinc.com BALLINGER VICKI SSN:208-46-9296 Email:Vicki.Ballinger@emtecinc.com

Northwest University

northwestu.edu

Confidential, taxation, and financial data

Paul Smiths College

paulsmiths.edu

At Paul Smith's College, it's about the experience. We are the only four-year institution offering broad-based higher education in the Adirondacks. Our programs...

Q7. Share lessons learnt, what were your struggles in executing the project and how did you overcome them?

The biggest struggle we faced when starting the project was accessing the ransomware group sites safely. In order to achieve this, we first connected to a reliable VPN service, created a guest user on the system (with limited privileges) and then set up a virtual machine. We downloaded the tor browser and configured it to navigate the onion links safely and anonymously.

The next challenge was finding the ".onion" links for which we used a search engine for tor's hidden services called "ahmia", as it filters out explicit content. However, many links we found were not available or had captcha enabled to prevent DDoS attacks, ultimately making scraping difficult.

Through this project we learnt that ransomware attacks are more frequent and common than we realize, since only a few actually make it to the news. For the Cuba ransomware group, between the period we accessed the site again i.e. around 3 days, they had already attacked another company and posted the update. It was also interesting to learn that many ransomware groups think they are actually helping the companies they attack by finding exploitable vulnerabilities in their systems.

We also learnt that even the most active threat actors use strategies like phishing emails to gain access to more accounts and the network. Therefore, a lot of attacks can actually be avoided by reading emails and messages carefully, assessing their authenticity and checking the legitimacy of the software being downloaded or the links being accessed. In addition to this, we should keep our systems up to date with latest security patches to ensure that the ransomware groups cannot take advantage of known vulnerabilities.

References:

1. “The worst outcomes: Lorenz Ransomware, a new double extortion strategy,” *CyberTalk*. [Online]. Available: https://www.cybertalk.org/the-worst-outcomes-lorenz-ransomware-a-new-double-extortion-strategy/. [Accessed: 30-Sep-2022].
2. C. Nocturnus, “Cybereason vs. Lorenz Ransomware,” *Cybersecurity Software*, 08-Feb-2022. [Online]. Available: https://www.cybereason.com/blog/research/cybereason-vs.-lorenz-ransomware. [Accessed: 30-Sep-2022].
3. I. Arghire, “Lorenz Ransomware Gang Exploits Mitel VoIP appliance vulnerability in attacks,” *SecurityWeek*, 13-Sep-2022. [Online]. Available: https://www.securityweek.com/lorenz-ransomware-gang-exploits-mitel-voip-appliance-vulnerability-attacks. [Accessed: 30-Sep-2022].
4. J. Tidy, “Study: UK firms most likely to pay ransomware hackers,” *BBC News*, 23-Feb-2022. [Online]. Available: https://www.bbc.com/news/business-60478725. [Accessed: 30-Sep-2022].
5. “Alert (AA22-249A) - #StopRansomware: Vice Society,” *CISA*, 08-Sep-2022. [Online]. Available: https://www.cisa.gov/uscert/ncas/alerts/aa22-249a. [Accessed: 30-Sep-2022].