Sri Lanka Institute of Information Technology

B.Sc. (Hons) Information Technology-

Cyber Security

Y2 S1

Introduction to cyber security – IE 2022

Ransomware as a service

H.S.A.Silva

IT 23 558182

Contents

Abstraction

Ransomware-as-a-service (RaaS) has emerged significantly in the cyber world as a global threat. This report dives into the Basis of RaaS, the various ransom demanding methods, the notable groups who are responsible for attacks with real world case studies and preventing methodologies against such. This has evolved rapidly as a variation of a software business model where the ransomware operators create code and sell them on dark web for affiliates to purchase them and launch attacks. The evil part of these attacks is that even nonskilled criminals are also capable of launching threatening attacks and extracting large amounts of money. The report further highlights the components of the RaaS model.

This report further enhances how RaaS works. It includes a step-by-step procedure clearly explaining what is done in each step from creating the ransomware by operators to spreading the malware and demanding their ransom. Furthermore, there are three main extortion methods used by ransomware providers to extract money and pressurize the victim. So, this elaborates on the three methods very clearly and a real-world example for each method to get a clear understanding.

RaaS has been widely dispersed around the globe due to some notorious hacking groups. Group effort can be more effective than an effort of an individual. RaaS has been highly successful since it is a group of groups which are aiming towards the same motive. The report also focuses on famous attacks by these groups in the recent past. Additionally, the report highlights the impacts caused by the different attacks both financially and operationally.

Modern problems need modern solutions. This further elaborates on the prevention and mitigation techniques that should be used to handle an attack successfully or reduce the impact. of it. There are several actions that are recommended to follow an attack to reduce and make sure that it will not happen again. The report also consists of graphical analysis, extracting information from reputed surveys and critically analyzing them.

As the world keeps evolving, so is technology. The report focusses on the outlook of RaaS in the future where Artificial Intelligence will play a major role. Finally, the report highlights how cyber security professionals should train themselves to protect individuals and businesses from upcoming threats.

Introduction

Ransomware is malicious software when run on one's computer it encrypts all the data from the system making it inaccessible to the user. The attacker demands a ransom to decrypt files back. The cyber world has evaluated so that this kind of attack is sophisticated into a business model called Ransomware as a service (RaaS).

RaaS is the criminal variation of the business model software as a service. The ransomware operators write malicious or sophisticated codes and are made available for sale on the dark web where anyone can buy it. The code pack is also referred to as the ransomware kit. The danger of this crime is that even people with non-technical skills can launch this attack from the bought software. [1]

In 1989 a scientist sent some floppy disks with ransomware attached to it. The virus locked the files and asked for a ransom of $189 to decrypt it. It was then considered to be a minor problem as the security professionals were able to get the decrypted key easily. But this laid the foundation for the birth of more dangerous attacks. [2]

The importance of studying this is very critical as a cyber security student because it highlights how advanced and how dangerous this type of attack can be in the modern world. Thus, by learning so one can teach others so that they themselves and others will be more cautious about the threat actors and be unharmed.

RANSOMWARE ATTACK
You only have 3 days to submit the payment, or your files will be lost.
Time Left
02:23:59:06

FIGURE 1 RANSOMWARE ATTACK

What is Ransomware as a Service?

Ransomware as a service is a business model where the ransomware operators sell exploitable codes on the dark web for the affiliates to buy and launch ransomware attacks on victims. This can be seen as a model variation of the business model named as 'software as a model'. The difference is that RaaS model sells illegal codes which is also known as the ransomware kit, while the Saas model sells only legitimate products.

There are two main parties to this model. One is the ransomware producer, and the other is the affiliate who is also known as the buyer. The producers are highly skillful personnel who has very deep programming skills and other skills like malware development, encryption and backend infrastructure. The goal of ransomware producers is to rent out the malware for affiliates and gain some income. The other party is the affiliate who distributes the malware to the victims provided by the ransomware producers. They steal credentials, run phishing campaigns and obtain a share of the ransom. The percentage varies from 60 – 80 % while the rest is received by the producer.

There are 3 main components of the Raas model

- **Dashboard** - it is an interface or a control panel where the affiliate can monitor their attacks. It contains information of the number of attacks done, Number of people who got caught into the attacks, generating payloads and viewing other overall statistics.

- **Encryption Tools –** This contains the set of tools where the victim's files get encrypted using strong algorithms likes RSA, AES. The purpose is to disable the access to victims until the ransomware is collected.

- **Payment gateways –** This is a very crucial component with respect to the affiliate where he receives the ransom staying anonymously. This does not work with normal banking payments. The attackers demand for ransom in the form of cryptocurrency mostly Bitcoin and Monero. This has customer support portals to help the victim to pay.

The most threatening part of this is that even a normal person can launch this type of attack. The only things needed are basic reading skills and access to a device. Even without no knowledge of coding, encryption is needed to trick a victim. The process is very simple. Go to the dashboard then download a payload and send it to a victim. Not only that, they also have the ease of getting help from forums and technical support, which is why this has become a very serious issue.

Step By Step Guide How RaaS Works

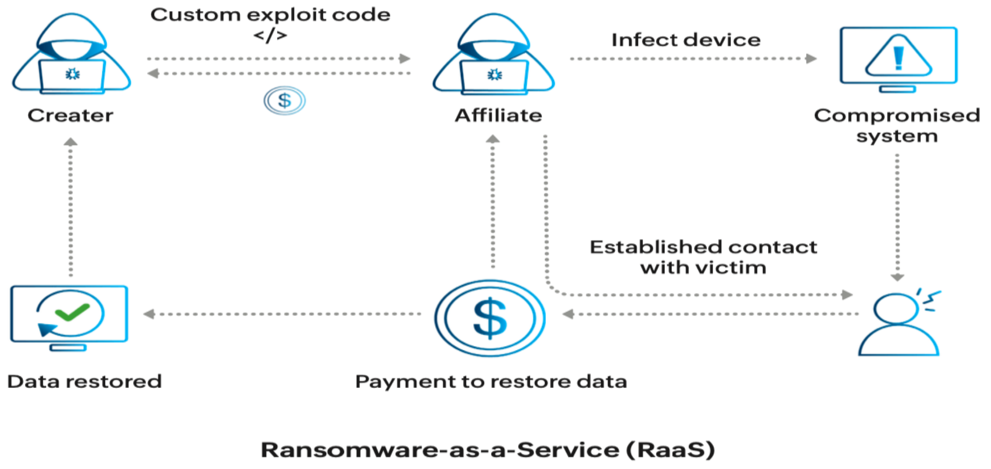


FIGURE 2 HOW RAAS WORK

1. **Developers create Ransomware** - Skilled computer professionals build the ransomware kit and the central dashboard containing payloads, Analytics, tools and payment gateways.

2. **Subscription by Affiliates –** The attackers can subscribe to this model by a monthly subscription or a lifetime access depending on the type of attack. Different levels of affiliates are considered by the skill set and rate of success.

3. **Victims are targeted –** The affiliates conduct phishing campaigns targeting individuals and companies.

4. **Ransom demanded –** once the malware is injected to the victim computer the files are encrypted making inaccessible to the user, thereby requesting a ransom amount to regain access to those files. The ransom is usually received through cryptocurrency to hide the information about the attacker.

5. **Developer gets his portion –** Once the attack is successful and the ransom is received the developer gets a percentage of the amount as a Comision.

Ransomware Extortion Methods

Double Extortion Method

This is a very serious threat to the victim where the attacker encrypts the files and steals the credentials of the victim, making the victim desperate. The victim has fallen into two issues, that is why it is called double extortion. The victim must pay the amount to get his data back and must make sure that the confidential data is not leaked outside. [3] Some real-world examples where double extortion was used was the Travelex attack by REvil which is discussed further down the report.

Triple Extortion Method

This is an advanced version of the double extortion method. The hacker does not only encrypt files and threaten to leak the confidential data But also launches a Distributed Denial Of Service (DDOS) attack as well so that they cannot access the company IT assets. This attack is mostly done to organizations where their reputation becomes a priority. This method was used when the UK national library was attacked by a ransomware where the attackers tried to auction the stolen data for bitcoins. As a result, the criminals leaked 500,000 files [4]

Multi Extortion Method

This method adds another level of pressure to the victim. Consider the victim as an organization. The attackers launch a ransomware attack not only on the organization itself but also the other related links to it as well. Suppliers, customers, and trade partners also fall as victims due to these kind of attacks. This can be very dangerous as it compromises the whole network of businesses. A real-world example for a multi extortion attack was when an industrial company in Sweden was attacked by two groups of hackers where they were able to mount with extra layers of pressure making the whole system go down [4]

Real World Examples

- **Revil (Ransomware Evil) -** REvil is a group of Russian cyber criminals that ran very successful RaaS attacks . The name ransomware evil was inspired from the movie series 'Resident Evil' . This emerged in the year 2019. Revil was a very serious threat back then because it was able to attack very large companies causing severe losses to those organizations. [5]

  Notable REvil attacks

  1. **Attack on JSB Foods –** JSB foods are one of the largest meat suppliers. On the 30th of May 2021 due to a ransomware attack they had to stop the operations in north America and Australia. The users were unable to connect to the system as they were locked out of the database till the ransom payment was made. This was a major problem as it disrupted the food supply chain [6]. A fluctuation in the meat market was seen. This attack was done by a phishing email or an exploited vulnerability. Due to this the Food chain had to incur a loss of $11 million.

  2. **The Kaseya incident –** on 21st of July 2021 the REvil group attacked a set of managed service providers affecting many businesses and individuals. This happened due to a vulnerability found on the virtual system administrator on their cloud based servers. This was a supply chain attack bypassing their systems and distributing ransomware to the users. This is to be noted as one of the largest ransomware attacks that ever happened incurring a massive loss of $70 million.

  3. **Travelex attack –** On the beginning of the year 2020 Travelex which was a foreign exchange company which was in UK was attacked by the REvil group. This was due to a vulnerability found on the Virtual Private Network(VPN) servers of that company [7]. Due to this attack several banks relying on this system failed to do their operations properly and even the banks at the airports had to do their operations manually. While the group demanded $6 million as ransom and they also stole 5GB of customer data.

- **Darkside Group –** This group is comprised of criminals from various other ransomware groups making it a very threatening group for the cyber world. The initial occurrence was stated on august 2020. This group focuses more on malware development and selling it has a business. This group has some notable policies where they do not target government, educational institutions and hospitals. This was a more professional group where they had victim support desks and hotlines. It is also stated that this group donate a portion of their income to charity organizations as well. This group follows the double extortion method the most. Darkside also uploaded the stolen credentials to their website ‘Darkside Leak’ when the victim failed to pay the ransom.

Colonial pipeline attack

On May 07th 2021 the Darkside group got access into the largest fuel pipeline in the United States. This system provided fuel to the airports and some military bases as well. This attack weakened the fuel supply from the gulf to the east coast covering a mammoth 5500 miles. This was a huge impact to the fuel stations where the prices increased rapidly, making people wait in long queues [8]. The power grid had an outdated system dating back to the 1960s so the hackers gained access from stolen credentials found on the dark web and launched the attack. Colonial had to pay $4.4 million to restore their system back where $2.3 million was regained later. This attack was a crucial factor where other organizations thought to invest on cyber security more [9].

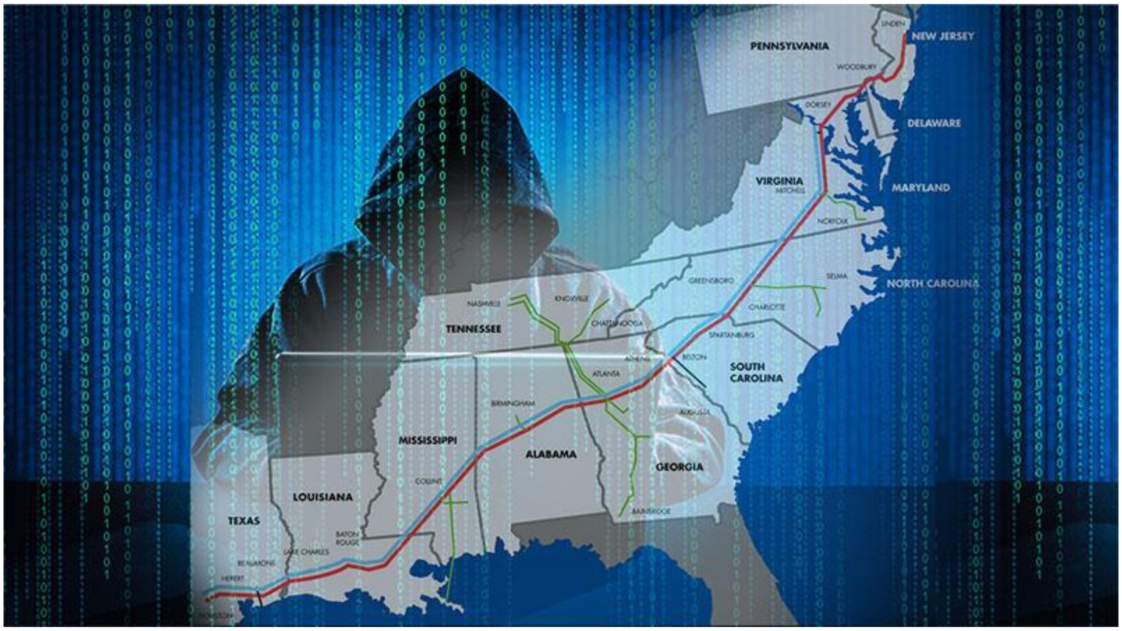


FIGURE 3 – COLONIAL PIPELINE ATTACK

- **Lockbit Ransomware Group –** This is one of the most dangerous active groups in the tech world. This group was founded in 2019 and became more popular by 2020. This group has only monetary motives where they do not care whether it is a government or a hospital. This group was found to be a major threat because of the tools that they possess. They have the fastest encryption tools where they sell those to get an income from the middle attackers. This also have additional features like the customer help desk. In the meantime, they have been able to capture around 2000 victims and stealing more than $120million. [10]

Lockbit had different versions of their ransomware where **lockbit2.0** marked the beginning of it. It targeted sectors like hospitals and legals entities where they used email phishing and SMB for spreading. This is a very dangerous tool that no one has been able to decrypt it so far because of the AES and ECC encryption algorithms used. The ransomware works offline as well making it a very serious threat. Below are some of the attacks carried out using the initial version of Lockbit. [11]

- Attack on Accenture the global professional service company.
- Attack on Thales electric company.
- Attack on La Poste (France) .
- Attack on Pendragon Plc.
- Attack on Port on Lisbon.

Lockbit 3.0 was the next version of the ransomware. Before releasing that they started a bug bounty program to act like legitimate one. Consisting of more advanced evasion techniques and fast encryption options this has become a very popular software in the dark web. It is also stated that the developer who build the **Lockbit 3.0** version was the person behind the colonial pipeline attack as well. [12]

Continental a German product manufacturer was the first victim. The group leaked part of the data while giving access for 50 million Euros. Nuxe a French company was later attacked on January 2023 and leaking 821GB of data from it’s central database. Below are some other attacks carried out using this ransomware.

- January 2023- British postal service called ‘Royal Mail’ attack.
- February 2023 – Canadian Bookstore ‘Indigo books and Music’
- March 2023 – BRL group a French water specialist.
- May 2023 – China daily newspapers
- June 2023 – TSMC group
- July 2023 – Port Nagoya in Japan
- October 2023 – Stole data from Boeing an aircraft manufacturing company.
- November 2023 – Chicago trading company.

Financial Impact And Data Loss of Attacks

Organization	Year	Group	Financial Loss	Impact
Colonial Pipeline(USA)	2021	Darkside	$ 4.4M	Fuel Shortage Business shutdown
JBS Foods	2021	REvil	$11M	Operations Halted
British Library	2023	Rhysida	Not given	Leak of 600Gb of data
Acer	2021	REvil	$50M	Loss of corporate data
Kaseya	2021	REvil	$70M	Interference to managed service providers
Boeing	2023	Lockbit	Not given	Interference to operations
Royal Mail	2023	Lockbit	Not given	Delay in mail services
Twilio	2023	Scattered Spider	Not Given	Leak of customer data
Snowflake	2023,2024	Scattered Spider	Not Given	Leak of customer data
Munster Tech University	2023	BlackCat	Not Given	Leaked data sold on dark web

Prevention And Mitigation From RaaS

1. **Regular Patching and updating software –** An outdated software can be one of the easiest point of entry for the cyber criminals. Every organization using IT devices should implement strong patch managing policies to ensure that all devices are updated regularly. Updated software will be harder to compromise than the outdated ones which is why is much important.

2. **Practice good IT hygiene and user awareness–** Humans are always the weakest link for security. 2021 Verizon data breach investigation report states that 85% of the data breaches are the cause of human involvement. How strong and how reliable the cyber security of an organization can be, Carelessness of a single employee can lead to an attack in the whole infrastructure. So, the management should be able to initiate in organizing awareness programs and teaching them how to prevent and act if in case they are attacked. They should be given frequent awareness as attacks are getting advanced day by day. [13]

3. **Email security and Phishing defense –** Most common methods of hacker entry is through a phishing email. One should have advanced email filtering options which detect those spam mails and block them. Educating employees to identify and ignore phishing emails are also good strategies to be used [13]

4. **Multi-Factor Authentication(MFA) -** Criminals access the system by the stolen credentials and bypassing them with the username and passwords. Implementing multi factor authentication leads to adding another extra set of security layers for the attackers to get in. Consider a website where one needs to enter the username and password and also a one-time OTP code sent to the phone or email to get access to the site. That is know as two factor authentication while a MFA will need an another extra layer like bio metrics to sign in. MFA is considered safe as the ransomware attackers has to bypass several security layers to compromise. [14]

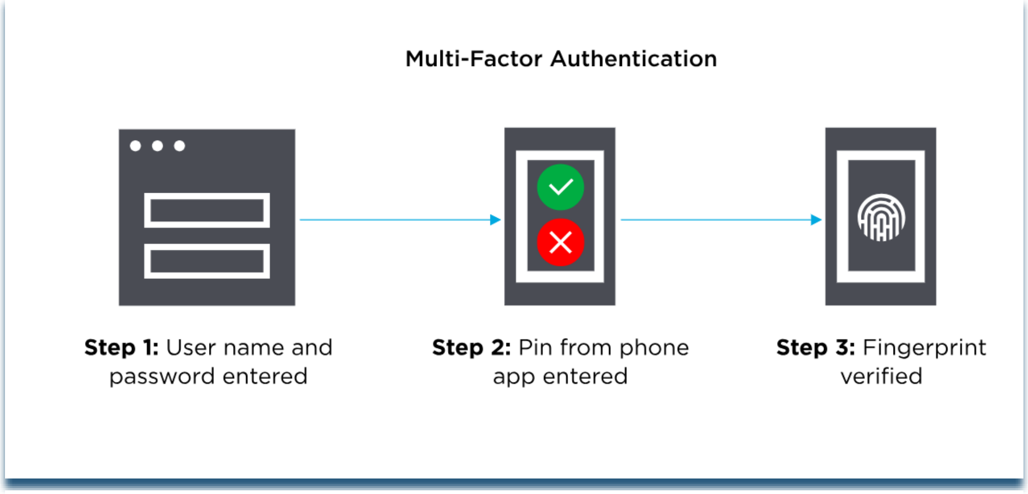

Multi-Factor Authentication
Step 1: User name and password entered
Step 2: Pin from phone app entered
Step 3: Fingerprint verified

FIGURE 4 – MULTIPLE FACTOR AUTHENTICATION

5. **Implement Zero trust model –** The zero trust architecture model used by companies are a crucial factor for safeguarding the company IT assets and data from attackers. It is where not only the external party but also the ones inside the network perimeter are not trusted at default. Based on NIST 800-207 below are some of the core principles of zero trust architecture.

   A. "**Never Trust Always Verify**" – This is a key principle as mentioned earlier, any entity whether its outside or inside will have to always verify them to gain access to the system.[15]

   B. **Limit Blast radius** – If in case an attack happens, and zero trust architecture is implemented the attacker will have only a limited movement within the network so the others are protected and the security team can have time to respond to the attack. [15]

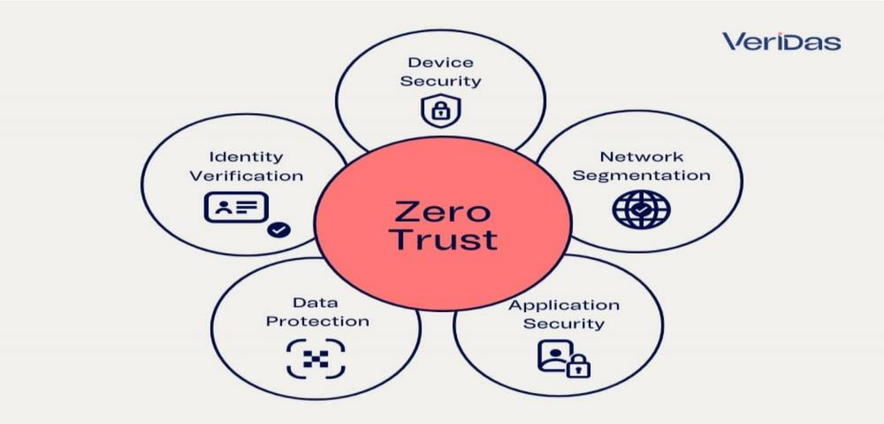


FIGURE 5 – ZERO TRUST ACHITECTURE

6. **Network Segmentation –** Dividing the network of the company into smaller segments can limit the spread of ransomware within the organization premises. Consider an example where there is a large bank with many branches across the globe and the security policy of the company has been implemented in such a way that the employees cannot access the financial reporting system. Whereby they can stop the traffic from coming into the financial segment. Implementing Virtual local Area Networks (VLAN), firewalls and Access control Lists (ACL) are some policies which can be adopted. [16]

7. **Implement endpoint detection and incident response tools -** Implementing these tools can help to look for unusual behavior and block them the very moment they see them. These tools have been advanced with the support of artificial intelligence to recognize possible threats. This also helps the security teams to patch the system quickly which will avoid spreading of the ransomware.

   Below are some minor steps which can be used to prevent from ransomware attacks

   - Disable Remote Desktop Protocol (RDP) if it is not in use.
   - Enabling spam filters for mail.
   - Blocking malicious IP addresses through ACLs
   - Running operating system functions in a virtualized environment.
   - Categorizing data based on logical and physical aspects.

Actions Recommended After RaaS Attack

1. **Isolation –** The infected devices should be isolated from the others preventing further spread of the ransom. They should be logged out of the network to prevent lateral movement.

2. **Collect evidence –** All details which can be collected as evidence should be collected. A note is appeared on the screen most of the time after a ransom attack has occurred so getting a picture will be very helpful for legal and other purposes. Secure the logs for reporting and audits.

3. **Assess the attack** – The compromised entities should be evaluated including systems, data, network and other services which were affected and encrypted.

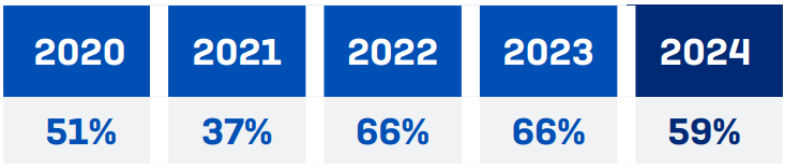
4. **Analysis of root cause** – The security team should look into the vulnerabilities that were exploited and other security controls that have been bypassed from the attack. The most important thing is that they should identify the initial vector.

5. **Validating recovery** – Check for backups so data can be regained without paying the ransom.

6. **Report** – A detailed report containing all possible data regarding the attack. Including the timeline impact and techniques used.

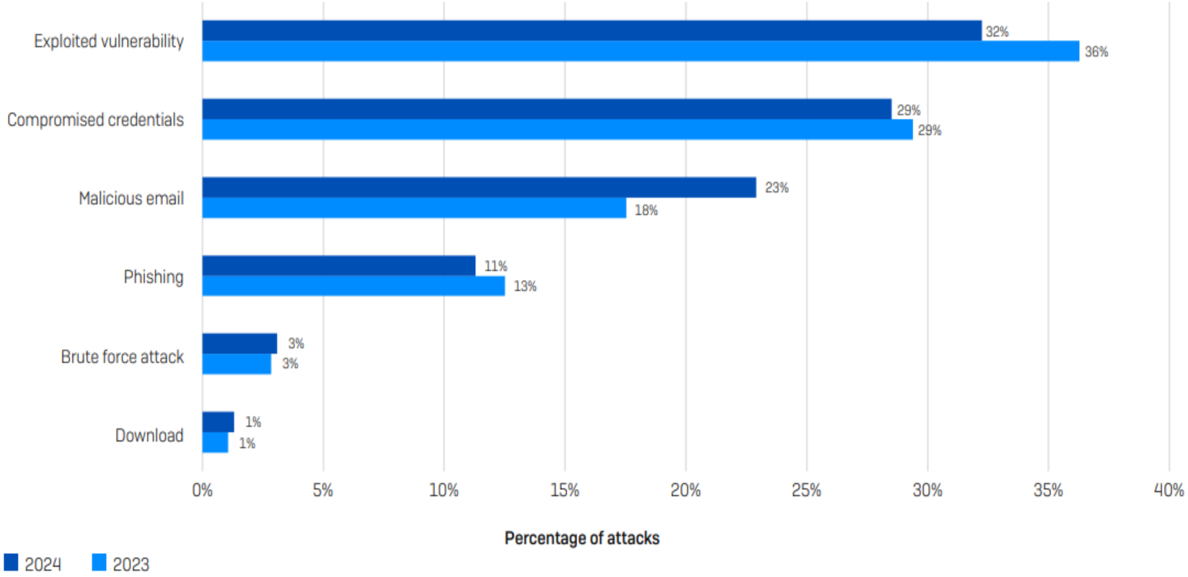
7. **Update security policies** – By taking into consideration of the previous attack the organization should implement new and upgrade policies so that they might not get infected again.

Rate of Ransomware attacks

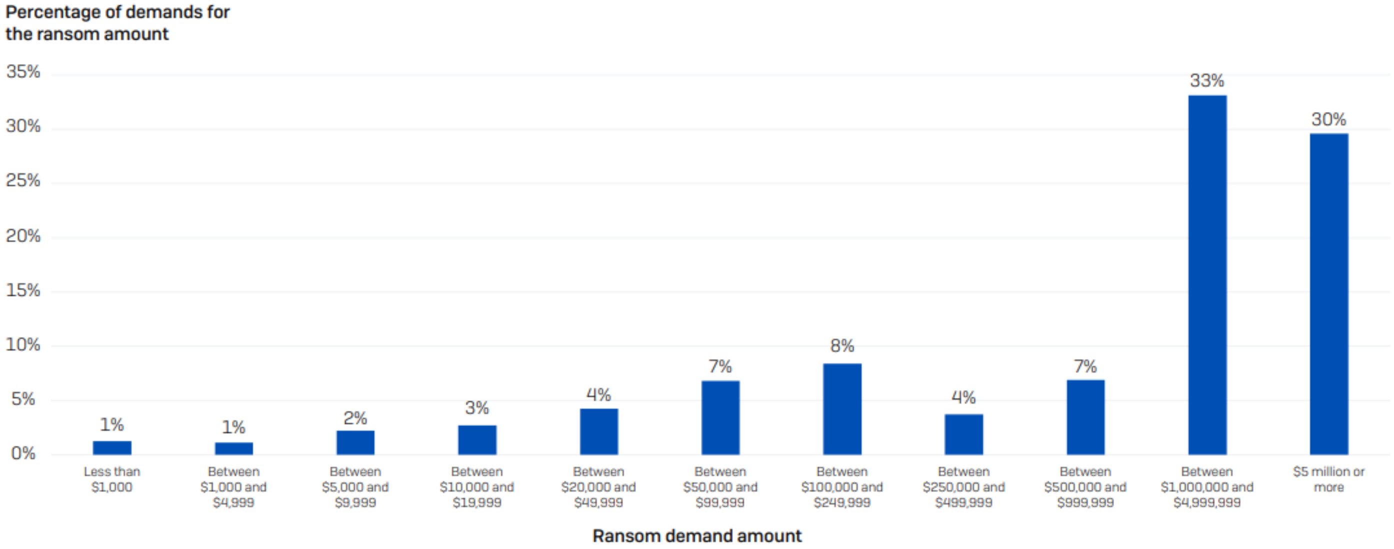


2020	2021	2022	2023	2024
51%	37%	66%	66%	59%

The above diagram illustrates the percentage of ransomware attacks in recent years. This was extracted from "Sophos Rate of ransomware report". Accordingly, the highest percentage was seen in the 2022nd and 2023rd year while it has been reduced by a very small margin in the 2024th year. The trend is expected to increase in the coming years with the facilitation of artificial intelligence and machine learning capabilities. [17]



The above graph illustrates the percentage of attacks which are the root causes of ransomware attacks in the years 2023 and 2024. The least possible way that an attack can happen is through downloads which shows less than 5% while the higher percentage of them is through an exploited vulnerability or a compromised credentials. A considerable number of attacks have happened through phishing and malicious emails while only a very small amount is done through brute force attacks. [17]



How much was the ransom demand from the attacker(s)? n=1,701

The above line graph depicts the amount of ransom and percentage of demands for ransom amount. While the x axis shows the percentage, and the y axis shows the demand amount. According to this it is very clear that the attackers are not interested in smaller amounts. Almost about 66% of the time that ransom demanded is more than $1,000,000 while 30% of it is even more than $5 Million . Only 24% of them demand less than $500,00 and which is why ransomware is considered as the most destructive malware in the cyber world. [17]

Outlook of RaaS

Market Expansion

The RaaS economy is expected to grow rapidly in the next few years. As discussed earlier the rate of ransomware attacks have increased year by year where RaaS model is responsible for a significant percentage of it. The ease of access and the non-need of technical knowledge has eased the entry of many cyber criminals into this business variant. So accordingly, RaaS shows a higher success rate than normal ransomware attacks and it is quite evident that RaaS model will be made interested by new criminals as well. Not only beginners but also the current attackers will also be motivated to launch more and more attacks because of the massive gain that they can get. The decentralized affiliate model is helpful to penetrate various entities using technology.

Increase in Sophistication

The RaaS operators or the initial developers are continually motivated to produce more and more tools to increase attacks and gain more wealth. The operators have started to target supply chains as when they attack the gain they receive is very high compared to a normal attack. The best way they can launch a supply chain attack is to target managed service providers and the software providers to target several victims. The payloads are becoming more modular where developers can customize attacks based on the victim environment. This is usually done through targeting files types and disabling backups.

Artificial Intelligence in future Ransomware

Use of AI is increasing rapidly, and it has both the positive and the negative sides to it. As there is no barrier for use of AI and it does not identify one as a criminal and stops giving responses. Therefore, with the evolving world the ransomware capabilities have advanced. AI automates reconnaissance which helps ransomware to notice high-value targets within a network independently. Where machine learning algorithms has the capability to analyze network traffic and configure the systems to pinpoint critical servers and database for encryption.

With the development of AI attackers can write customized and better deceptive emails and phish the victim. Deep-fake technology can be used to impersonate people and obtain trust and legitimacy.

AI is capable of processing bulks of data in a short period like extracting information from breached databases, dark web and other social media sites. This will also facilitate identifying and targeting vulnerable individuals and businesses.

Different AI mechanisms and tools can be used to analyze the stolen information and strengthen blackmailing methods. This also allows the operators to launch automated commands where one does not have to manually input constantly. AI chat bots can also be used by attackers to save their time and energy making AI do it for them.

Role of security professionals for RaaS in future

The role of a cybersecurity professional can be very critical from safeguarding from ransomware attacks soon. As threats and attacks become more advanced day by day the defense teams will have to be more prepared and evolved. Ransomware will increase in impact, scale and complexity and it will be the time when security professionals need to strengthen their security policies, response planning and problem-solving skills. Not only from cyber criminals but they will have to battle against AI driven attacks as well very soon.

Cybersecurity professionals will have to strengthen their defense mechanisms. Mechanisms like implementing zero trust architecture, Network segmentation and endpoint security will be pivotal. Because this will prevent attackers from moving laterally in the network minimizing the impact. Leveraging machine learning and artificial intelligence will help to detect unusual behavior and alert the necessary entities to prevent an intrusion. The systems should be updated regularly, and patches should be managed to deteriorate and prevent an attack from happening.

Threat intelligence and proactive hunting are very crucial for security people. When an attack happens the rate of response is very critical. They should train themselves in a way that they react very fast to the attack. This will facilitate reducing the damage. Having a good backup plan will be a good solution and it will even help to restore the data without paying any ransom. A strong incident response policy can be used as a finer deterrent control.

Education and experience are another vital factor to reduce ransomware. They should follow reputable certification which will help them to enhance their skills. Not only following certifications they should also conduct awareness programs to educate the non-security workers. Especially employees should be taught to identify and ignore phishing emails as it is one of the most common methods of how attackers gain unauthorized access.

Cybersecurity professionals should update policies that impact cyber defense. Collaborating with government agencies and international entities to develop and share robust standards will be critical. They should also help the victims in what every way they can as they will be under immense pressure.

Emerging technologies such as blockchain and quantum computing will also play a pivotal role very soon. The quantum computing will be able to crack any encryption algorithms which will increase the complexity of cyber security. While on the other hand attackers can use blockchain mechanisms for ransom payments enabling transparent incident response and tracking.

Conclusion

Ransomware-as-a-service (RaaS) is no longer a threat which is limited to skilled cybercriminals, but it has evolved into a black-market economy which enables even non-technical criminals to launch massive cyberattacks. Taking the legitimate form of the Software-as-a-service (SaaS) model this created major upsets in the global economy. The profit gained through these massive ransomware attacks has motivated the criminals to target more victims. The ability to stay anonymous has made this one of the most persistent threats targeting governments, businesses and high-profile individuals

The report has highlighted the basic structure of how RaaS operations run, with the inclusion of the roles of ransomware operators and affiliates differently. The use of advanced encryption mechanisms and untraceable payment platforms were highlighted too. The use of extortion methods was clearly explained with the use of real-world examples for a better understanding for the user. The use of several layers of attacks like Distributed Denial Of Service (DDOS), selling stolen credentials on dark web and other multilayered tools very examined.

Thanks to the digital library where I was able to investigate real-world examples very deeply. The case studies of colonial pipeline attack, attack on JSB Foods, Kaseya attack were some major attacks which I was able to analyze the root cause of the attack, affected agents, and the amount of disruption caused. I was able to identify how costly and threatening these attacks can be and was motivated to share the news with others so that they might not fall into trouble.

Looking ahead of the future, the growth will be more complex and threatening with the advent of artificial intelligence and machine learning so as cyber security professionals and students it's our responsibility to learn the skills to handle and win against these attacks. Not only preventing and mitigating attacks but we should also stand up and help the victims who are under immense pressure.

References

[1] "Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/Ransomware_as_a_service. [Accessed 17 04 2025].

[2] "techTarget," [Online]. Available: https://www.techtarget.com/searchsecurity/feature/The-history-and-evolution-of-ransomware. [Accessed 17 04 2025].

[3] "Zscaler," [Online]. Available: https://www.zscaler.com/resources/security-terms-glossary/what-is-double-extortion-ransomware. [Accessed 17 04 20225].

[4] "prolion," [Online]. Available: https://prolion.com/blog/double-extortion-ransomware/. [Accessed 17 04 2025].

[5] "Akamai," [Online]. Available: https://www.akamai.com/glossary/what-is-revil. [Accessed 19 04 2025].

[6] "Mitnicksecurity," [Online]. Available: https://www.mitnicksecurity.com/blog/an-overview-of-the-2021-jbs-meat-supplier-ransomware-attack. [Accessed 17 04 2025].

[7] "Onsecurity," [Online]. Available: https://www.onsecurity.io/blog/cyber-nightmares-what-went-wrong-with-travelex/. [Accessed 19 04 2025].

[8] "Checkpoint," [Online]. Available: https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/darkside-ransomware-group-explained/. [Accessed 17 04 2025].

[9] "youtube," [Online]. Available: https://youtu.be/qJM5zG9XhZ8?si=mZVSto0BtPp1oAP6. [Accessed 18 04 2025].

[10] "Akamai," [Online]. Available: https://www.akamai.com/glossary/what-is-lockbit-ransomware. [Accessed 18 04 2025].

[11] "sentinelone," [Online]. Available: https://www.sentinelone.com/anthology/lockbit-2-0/. [Accessed 18 04 2025].

[12] "youtube," [Online]. Available: https://youtu.be/0EQenbbPSaE?si=VwZV0McvcjVBIrX9. [Accessed 18 04 2025].

[13] "Crowdstrike," [Online]. Available: https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/how-to-prevent-ransomware/. [Accessed 18 04 2025].

[14] "onelogin," [Online]. Available: https://www.onelogin.com/learn/what-is-mfa. [Accessed 19 04 2025].

[15] "Crowdstrike," [Online]. Available: https://www.crowdstrike.com/en-us/cybersecurity-101/zero-trust-security/. [Accessed 19 04 2025].

[16] "Cisco," [Online]. Available: https://www.cisco.com/c/en/us/products/security/what-is-network-segmentation.html#~how-segmentation-works. [Accessed 19 04 2025].

[17] "sophos," [Online]. Available: https://assets.sophos.com/X24WTUEQ/at/9brgj5n44hqvgsp5f5bqcps/sophos-state-of-ransomware-2024-wp.pdf. [Accessed 19 04 2025].