Sri Lanka Institute of Information Technology

The rise of Ransomware

Individual Assignment

IE2022 - Introduction to Cyber Security

Submitted by:

Student Registration Number	Student Name
IT21119194	J.A.D.S.K Nanayakkara

24/04/2022

Abstract

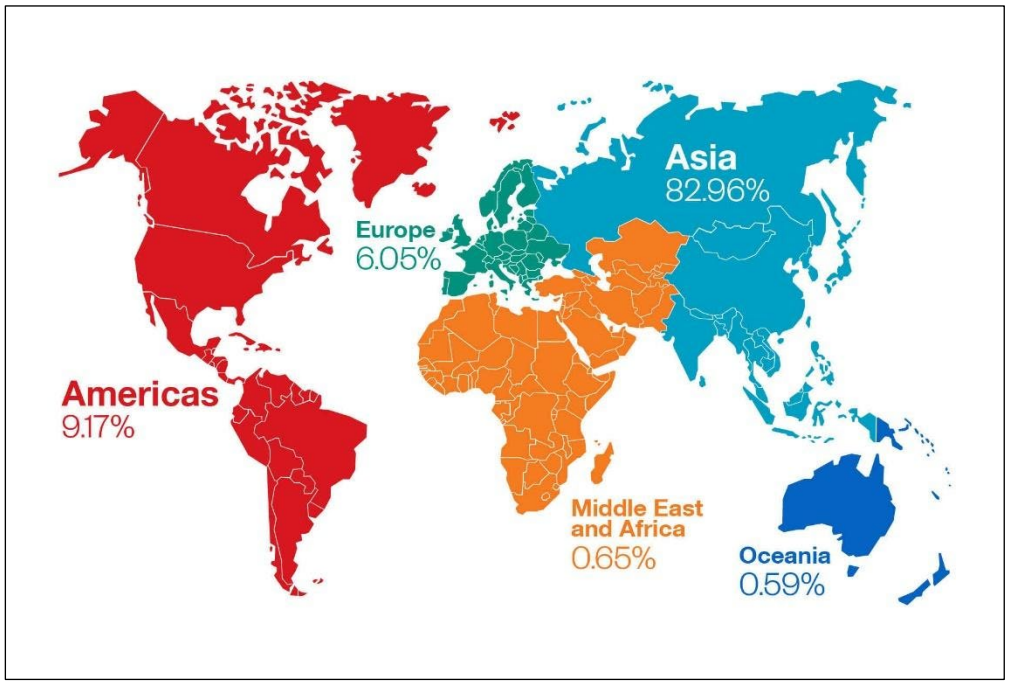
With new variants being distributed on a regular basis, ransomware has quickly become one of the deadliest dangers on the internet. It is becoming a more significant threat to businesses' data, and because there's so much money to be made, new varieties pop up all the time. The ransomware crisis has spread throughout the world, with the primary objective of enhancing money through illegal methods. It might result in the loss of sensitive information, disruption of normal operations, and harm to an organization's reputation. Before the information is unlocked, it encrypts target files and shows messages demanding payment. This malware is responsible for millions of dollars in damages each year. The ransom demands are usually made in the form of a virtual currency, such as Cryptocurrency, which is difficult to track down. This report provides an understanding of ransomware's history, varieties, current prevalence, and future challenges

Table of Contents

1 Introduction

Ransomware is a sort of software that encrypts or locks a user's files and stops them from accessing their computer unless they pay the money. Crypto ransomware encrypts particular file types on infected computers and demands that users pay a ransom via defined online payment channels in order to get a decryption key.

The cost of a ransom is determined on the type of ransomware and the price of digital currency. Because of the perceived anonymity given by cryptocurrencies, ransomware writers usually suggest bitcoin as a ransom payment mechanism. Recent ransomware variants have incorporated alternative payment mechanisms like iTunes and Amazon gift cards. However, paying the ransom does not guarantee that customers will get the decryption key or unlock tool required to regain access to the infected system or captive files.



This danger can be encountered in a variety of ways by users. Malware may be downloaded into unknowing users' devices when they visit unsafe or compromised websites. Any malware that is dropped or downloaded can likewise distribute it as a payload. Some ransomware is distributed as attachments in spam emails, downloaded via malvertisements from malicious websites, or dumped onto vulnerable systems using exploit kits.

This hazard can be encountered in a variety of ways. Malware may be installed on users' devices without their awareness when they visit unsecure or compromised websites. Any virus given or downloaded as a payload has the potential to propagate. Some ransomware is distributed as attachments in spam emails, downloaded via malvertisements from malicious websites, or dumped onto vulnerable systems using exploit kits.

Because it threatens or intimidates users into paying a fee, ransomware is characterized as "scareware" (or ransom). In this sense, it's comparable to the FakeAV virus, however instead of seizing the infected system or encrypting files, FakeAV presents bogus antimalware scanning results to entice users to buy fake antimalware software.[1]

2 Evolution of ransomware

In the late 1980s, a research scientist used viruses on floppies to extort money from other researchers. Following that, ransomware progressed slowly. Due to the fact that threat actors extorted money by denying victims access to their own services and systems, deployment did not become common until the mid-2000s.

Campaigns in the mid-2010s relied on mass distribution to a large number of casualties. An automated "fire-and-forget" method combined phishing campaigns and vulnerability scans to transmit ransomware to a single server or a small number of hosts. Despite the fact that this tactic was intended to target a huge number of people, the attacks were often ineffectual. The malware spread uncontrollably, and the networks that were impacted were not properly disabled. As a result, victims seldom complied with extortion demands. Ransom demands were low by today's standards.

In 2015, cybercriminals began deploying post-intrusion ransomware. This method was initially used by the GOLD LOWELL threat group, which infected PCs with the SamSam virus. The developers of the Ryuk, BitPaymer, and Defray malware groups quickly followed suit. Threat actors' use of hands-on-keyboard behavior to boost the malware's destructive capabilities is a defining element of post-intrusion ransomware attacks. This change not only reduced the number of victims that a single threat group could target, but it also gave operators significantly more control over ransomware deployment, enabled targeted and effective network data encryption, and justified higher ransom demands. As a result of these conditions, more cybercriminals are engaged in ransomware operations.

The next major thing was the ransomware-as-a-service (RaaS) business model. Ransomware operators employed affiliates to spread malware in exchange for a share of the ransom money. This method allows criminals to extend their operations while simultaneously decreasing the entrance barrier to this type of crime. Even threat actors with little technical skills have successfully stolen money and wreaked havoc on victims' networks by employing RaaS in post-intrusion malware cases.

A noteworthy advance was the "name-and-shame" approach, which was first observed in April 2019 Snatch ransomware operations. The GOLD VILLAGE threat organization fully utilized the strategy in late 2019, promising to reveal data gathered through Maze ransomware operations unless victims paid the ransom. By March 2020,

CTUTM researchers had uncovered three new gangs that were utilizing name-and-shame ransomware. Adoption increased as the events got more effective. As of June 21, 2021, CTU researchers had discovered 27 ransomware activities that used this approach.

The demand for ransom has risen dramatically. Over the course of nine months in 2013 and 2014, the CryptoLocker hackers made a total of $3 million USD. According to estimates, the now-defunct Maze malware group demanded an average of $4.8 million from a single victim in 2020. In less than a year of operation, the threat group GOLD WATERFALL, which is behind the Darkside ransomware, is reported to have accumulated $90 million. A US insurance business allegedly paid $40 million to regain access to its network following the emergence of a Hades ransomware variant coordinated by the GOLD WINTER threat group in late March 2021.

Government-sponsored threat organizations employ ransomware to generate money or cause harm. Possible Iranian threat organizations, for example, used the ransomware N3tw0rm and Pay2Key to disrupt services at Israeli companies in early 2021. The NotPetya ransomware attack in 2017 was initially misdiagnosed as ransomware, but it was eventually traced to a Russian military operation aimed at sabotaging Ukraine's vital national infrastructure. North Korea has a history of using ransomware to raise money, notably GandCrab v4 in 2018 against targets in South Korea and VHD malware in 2020 against high-profile organizations. As a result, the illicit use of ransomware for financial gain is the focus of our inquiry.[2]

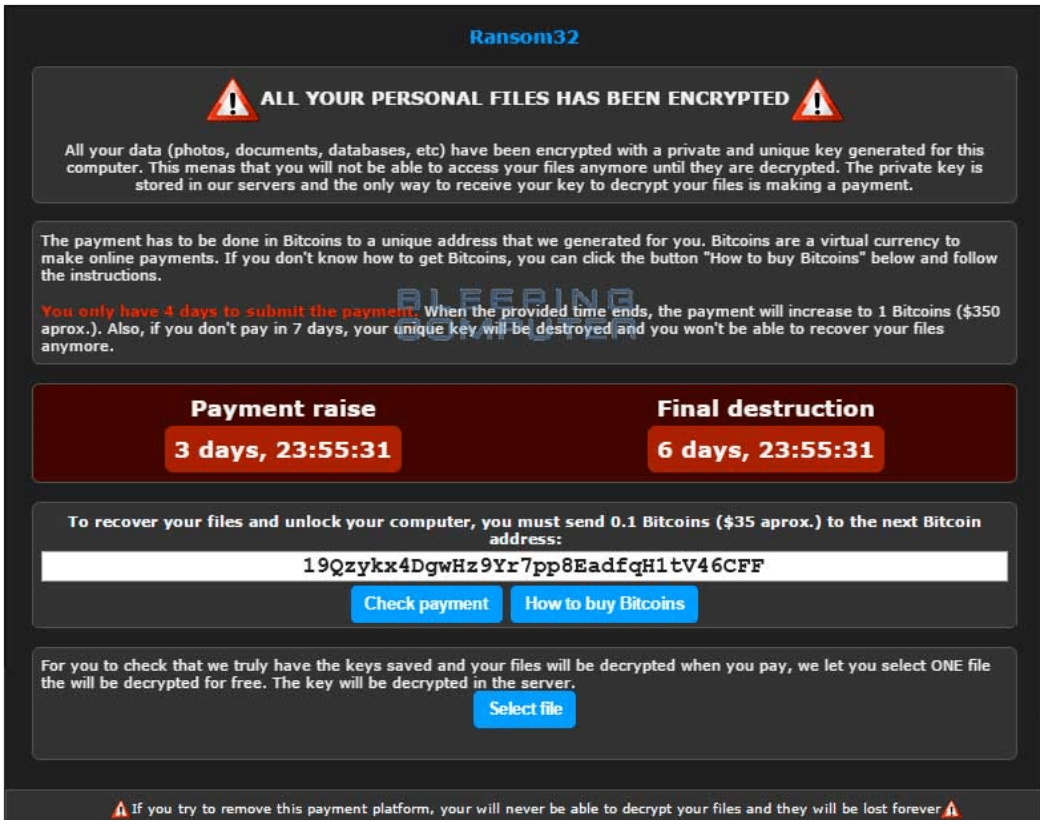
3 Type of ransomware

3.1 Crypto Ransomware

Crypto Malware is a new type of computer virus that prevents people from accessing computer data. The infection compels the user to pay a specific amount of money using an anonymous method like Bitcoin in order to recover access to the firm's data.

Crypto ransomware like CryptoDefense, CryptoWall, and CryptoLocker spreads by email, instant messaging applications, and drive-by downloads. The crypto-ransomware seizes control of all your data as soon as your machine is infected, encrypts everything, and demands a ransom of up to $500 in bitcoin, or company files will be destroyed.

Crypto Ransomware uses social engineering techniques to induce computer users to run it. For example, the victim may get an email with a password-protected zip file attached from a close friend or a reputable institution. The ransomware virus takes over when you open the file and prohibits users from accessing any of the company's data.[3] [4]



3.2 Locker Ransomware

The ransomware Locker encrypts your files and locks the company computer or mobile device. To get the company computer or mobile device returned, the victim is asked to pay a tribute.

Typically, the victim is only allowed limited access to the locked system, forcing them to deal entirely with the ransomware culprit. Parts of the keyboard and mouse may be locked, leaving the victim with little choice but to comply with the ransomware's demands.

Locker ransomware usually does not corrupt a whole computer system or target specific files. This feature enables locating and removing this form of malware without asking for payment.

Because locker ransomware can be uninstalled from a computer, attackers often employ social engineering to persuade victims to pay the ransom. For example, the ransomware pretends to be a tax authority or law enforcement organization, threatening to collect fines and other penalties for claimed illegal online activity. As a result, the victim panics and agrees to pay whatever amount is demanded.

Locker ransomware is also referred to as computer locker. [4] [5]

3.3 Scareware

Scareware is harmful software that tricks users into visiting malware-infected websites. Pop-ups can be scareware, also known as deception software, rogue scanning software, or fraud ware. These appear to be legitimate antivirus software warnings indicating the computer's files have been infected. Because they are so skillfully done, users are frightened into paying a premium to quickly obtain software that will remedy the so-called problem. Instead, they download phony antivirus software, which is malware designed to steal the victim's data.

Scareware is also disseminated through a variety of techniques, including spam email. After opening the email, the victims are misled into purchasing worthless services. You're opening the door to future identity theft if you fall for these con artists and give them your credit card information.[7]

3.4 Ransomware as a service (RaaS)

Ransomware as a service (RaaS) is a subscription-based framework that enables associates to use pre-developed malware tools to perform ransomware attacks. Associates are paid a commission for each valid ransom demand.

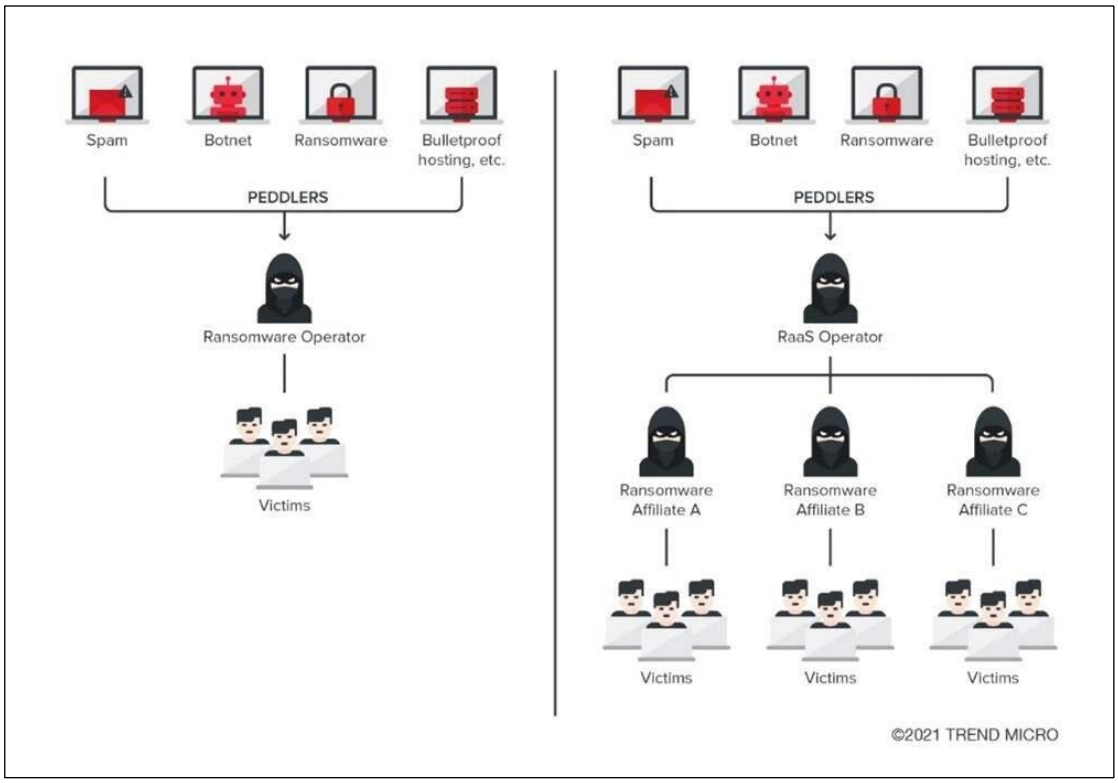
The use of the Software as a Service (SaaS) business model is known as ransomware as a service (RaaS).

In the past, all effective hackers were required to know how to code. This technological need has now been fully diminished with the advent of the RaaS concept.

Users of RaaS, like any other SaaS system, do not need to be skilled or even experienced in order to make efficient use of the product. As a result, RaaS systems make it possible for even the most unskilled hackers to carry out complex operations.

Affiliates that promote RaaS solutions earn a lot of money. The average ransom demand has increased by 33% to $111,605, with select affiliates receiving up to 80% of each ransom payment since Q3 2019.

Because of their low technical barrier to entry and large affiliate earning potential, RaaS systems are largely designed for victim proliferation.[8]

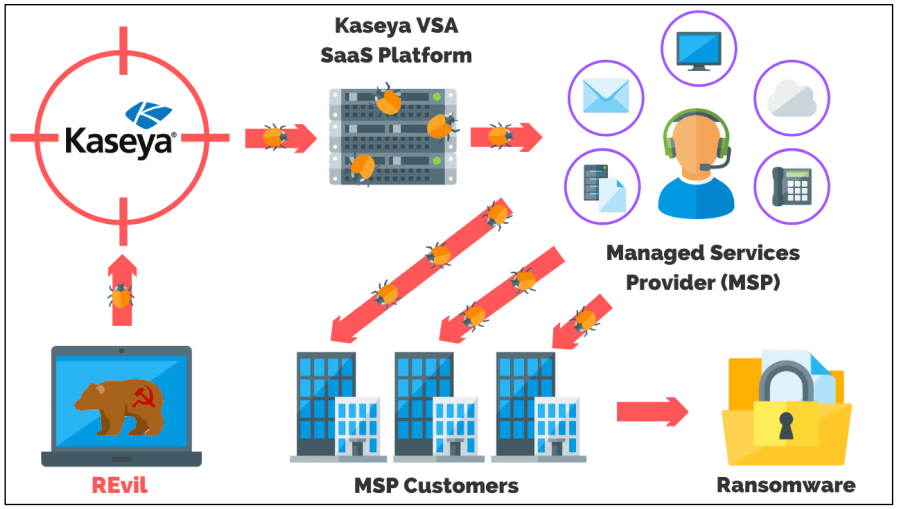


4 Ransomware Attacks

4.1 Kaseya (2021)

On July 2, 2021, Kaseya announced that its systems had been compromised. Kaseya provides IT solutions to other organizations, making it an ideal target for a domino effect that has affected over 1,500 firms across many countries. The cybercriminal outfit REvil claimed responsibility for the attack and demanded ransoms ranging from a few thousand dollars to millions of dollars, according to a Reuters report.

REvil demanded $70 million in bitcoin from Kaseya, but it's unclear how many firms really paid. Rather than paying the punishment, Kaseya opted to work with the FBI and the US Cybersecurity and Infrastructure Agency. On July 21, 2021, Kaseya got a universal decryptor key and sent it to entities affected by the attack.[9] [13]



4.2 JBS (2021)

On May 31, 2021, JBS USA, one of the largest meat suppliers in the United States, disclosed a cyberattack that forced it to temporarily shut down five of its primary US-based plants. The company's operations in Australia and the United Kingdom were also affected by the ransomware attack. JBS paid the hackers an $11 million ransom in Bitcoin to avert further disruption and to limit the damage to grocery stores and restaurants. The FBI attributed the infiltration to REvil, a sophisticated criminal cell known for ransomware attacks. [9] [11]

Ransomware Attack Strikes U.S. Meat Operations at JBS

By Jacob Bunge

Meatpacker JBS SA was hit by a ransomware attack that took a big chunk of U.S. beef-and-pork processing offline, sending buyers scrambling for alternatives and raising pressure on meat supplies.

The attack ratcheted up pressure on a food-supply chain already under strain from labor shortages, production constraints and high transportation costs. Late Tuesday, a company executive said JBS was making progress toward restoring its systems, and that the majority of its meat plants would be operational Wednesday.

Brazil-based JBS, the world's biggest meat company by sales, told the Biden administration that it was the victim of a ransomware attack, White House principal deputy press secretary Karine Jean-Pierre said on Tuesday. She said JBS reported that the attack originated from a criminal group likely based in Russia.

"The White House is engaging directly with the Russian government on this matter and delivering the message that responsible states do not harbor ransomware criminals," Ms. Jean-Pierre said.

JBS didn't comment on the White House's description of the attack.

The attack is the latest in a growing number to hit a range of businesses and institutions, including hospitals, the oil industry and local water supplies.

At JBS, the attack halted operations at meat plants that are among the largest in the U.S., according to worker representatives and notices shared with JBS employees. JBS facilities in Colorado, Iowa, Minnesota, Pennsylva-

Please turn to page A7

1.

4.3 Colonial Pipeline (2021)

On May 7, 2021, America's largest "refined products" pipeline was compromised with malware by a cyber gang known as Darkside. The Colonial Pipeline is a 5,500-mile pipeline that transports around 100 million gallons of oil each day. As a result of the attack, the average price of a gallon of gasoline in the United States surged to more than $3 for the first time in seven years, as motorists rushed to the gas stations.

The hackers were paid $4.4 million in cryptocurrencies, according to the pipeline operator. On June 7, 2021, the Department of Justice announced that it had recovered a portion of the ransom. US law enforcement agents were able to track the transfer and retrieve $2.3 million by using a private key for a bitcoin wallet.[9]

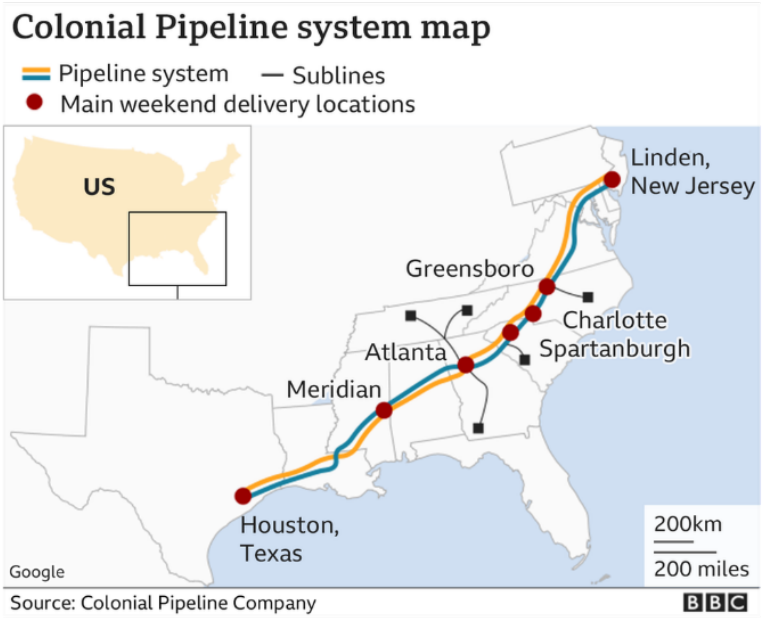
Direct attacks on operational technology are uncommon, according to experts, because these systems are generally more safeguarded. As a result, it's more likely that the hackers got access to Colonial's computer system through the company's administrative side.

"Some of the biggest attacks we've seen all started with an email," Mr. Niccolls says.

"An employee may have been tricked into downloading some malware, for example.

"We've also seen recent examples of hackers getting in using weaknesses or compromise of third-party software.

"Hackers will use any chance they get to gain a foothold in a network." [14]



4.4 CWT (2020)

CWT, a US corporate travel management business, said on July 31, 2020, that its systems had been hacked by ransomware and that it had paid the ransom. Using Ragnar Locker ransomware, the attackers claimed to have stolen sensitive corporate data and shut down 30,000 company computers.

The data leak might have been disastrous for CWT, which services one-third of the S&P 500 companies. As a consequence, the company paid the hackers $4.5 million on July 28, only days before Reuters reported the story. [9] [14]

2.

4.5 The University of California at San Francisco (2020)

On June 3, 2020, the University of California at San Francisco stated that a hacker group known as Netwalker had accessed the UCSF School of Medicine's IT systems on June 1. The medical research institute had been investigating COVID.

Netwalker appears to have undertaken research on UCFS in order to have a better understanding of its finances. Netwalker demanded a $3 million ransom, citing UCSF's billion-dollar annual revenues. To stop the incident, UCSF decided to pay Netwalker $1,140,895 in bitcoin after discussions. Netwalker was allegedly tied to at least two other ransomware assaults against institutions in 2020, according to the BBC. [9] [10]

5 Damage cost of Ransomware

If the ransom is paid, the ransom demand, which varies depending on the type of ransomware and the size of your firm, is certainly the most important immediate expense associated with being struck by ransomware.

According to a new poll, one-quarter of organizations who paid a ransom got their encrypted data for more than 5,000 pounds, while the other quarter got it for between 3,000 pounds and 5,000 pounds.

Small and medium-sized firms frequently paid ransoms ranging from 500 pounds to 1500 pounds, implying that targeting small and medium-sized organizations is still profitable.

High-profile targets who pay five-figure sums to recover access to their encrypted networks and files are also available, particularly when hackers threaten to erase data if they do not pay.

Finally, regardless of your company's size, time is money, and the longer your network is down due to malware, the more money it costs you.

If you pay a ransom to re-enter your encrypted documents, you will be charged additional fees. Plan to invest in additional cybersecurity software and pay for extra staff training to avoid recurring assaults, especially if you've been identified as a simple target.

Customers may lose trust in your organization as a result of poor cybersecurity and shop elsewhere.

6 Prevent Ransomware Attacks

6.1 Education, Training, and Measurement

The average user might not be ready to tell the difference between a daily email, phishing, and spear-phishing attempts. they are aware, however, that if you click on the incorrect thing, you risk losing all of your data and infecting your machine. The human side of social engineering will be minimized in some manner if the threat of ransomware is put into language that the common user understands. Because phishing emails are wont to propagate ransomware, training should include the risks, a way to recognize phishing emails, and therefore the tough lesson of knowing what to click on and when to not open a file. Before moving further, we want to instruct team members on a way to verify the source of the e-mail with a straightforward telephone call. It's not difficult to do, even as looking both ways before crossing the road isn't difficult, but we must teach all users about safe internet practices. Most companies should do penetration testing with phishing samples to judge the effectiveness of their training programs. [16]

6.2 Back-up data

Even if ransomware compromises the data of a company. If there is a backup of data, it can be recovered and there is no need to pay for it. The backup should always be up to date but just having a backup will not restore the system. Therefore, updating all sensitive data at all times can greatly reduce the damage caused by ransomware. Also, the backup data should be well-protected and stored off-line or out-of-band to avoid being targeted by hackers.

6.3 Use protection software and Always update OS

Operating system updates are routinely distributed by companies like Microsoft and Apple for a reason. These updates address vulnerabilities and loopholes that may be exploited by hackers. It is a cat-and-mouse game when it involves cybersecurity.

The company will be a step behind the curve if a company employs old technology, and the company will be more vulnerable to unscrupulous individuals.

Most antivirus software now includes email scanning and is capable of detecting the nice majority of viruses and malware on the computer. Despite the fact that hackers are always devising new techniques to urge access to a system while evading antivirus protection, this degree of security remains required.[15]

6.4 Remove Administrator Rights

Ransomware spreads by utilizing a user's privileges to infect files within its scope. If the user simply has normal user capabilities, only files that the user owns or has access to through a network share are shown. While the extent of this is often broad, it might be made substantially worse if the person gets administrator access. Then any file readable by an administrator is theoretically at risk, putting the whole environment in danger. This does not rule out the chance of the ransomware being unleashed by a daily user. Actually, the bulk of ransomware requires administrator privileges to launch. Macro-based ransomware, like WannaCry, could be a significant exception to ransomware that exploits vulnerabilities. Giving the correct administration power may prevent getting infected by ransomware.[16]

7 Future developments in the area

Predicting how the ransomware environment may alter in the future is never easy. We can look back at past trends to predict what will happen in the future. We feel that the concept of ransomware has progressed tremendously. The number of people in the room, as well as the quantity and sorts of fluctuations that occur, demonstrate this. The arrival of RaaS implementations might be another evidence that the crypto ransomware idea is reaching maturity and market saturation.

For the time being, we're responding to a number of events in the ransomware threat landscape that might have an influence on ransomware's near-term trajectory.

7.1 Focus on operational security

Cybercriminals behind ransomware will be obliged to constantly develop and evolve their methods as security companies and law enforcement pay greater attention to attack operations. Other cybercriminals are already tightening operational security to hide their activities and identities, with the FBI already offering a reward of up to US$3 million for arrest and conviction and/or belief of Evgeniy Mikhailovich Bogachev, the alleged mastermind behind the notorious Cryptolocker.

As a result, the Invisible Internet Project has gained pace. Many businesses have already adopted operational security measures such as the use of Tor (I2P). Such solutions mask the location of their websites and enable network connection anonymity, thereby preventing any attempts by law enforcement or security services.

Cryptocurrencies such as Bitcoin are being used by hackers to pay ransoms, making it more difficult for law enforcement to track down any ill-gotten gains.

They're using bulletproof hosting, a service provided by certain dubious domain hosting and web-hosting businesses that gives its clients a lot of legal liberty. Many of these fraudsters use name generating algorithms (DGA) with many levels of redirection to increase obfuscation and reduce the danger of getting caught.

7.2 Ransomware meets Internet of Things

Computers are becoming increasingly mobile, networked, and omnipresent, which is a clear trend in the world today. The Internet of Things and wearable computing are two technological advancements that may help the IT industry prosper, but they also give new opportunities for ransomware authors. Smart TVs, smartwatches, smart garments, smart fridges, smart locks, and internet-enabled automobiles are already on the market, and the list continues to increase. Both of these devices are effectively linked PCs that might theoretically be hijacked and held for ransom. Several types of devices are more vulnerable than others due to their use or design features. Data-rich equipment, such as Network Attached Storage (NAS) devices, have previously been attacked by crypto ransomware. Trojan. Syno locker is an example of a threat that targeted Synology NAS devices specifically.

Consider the case when your smart house lock is disabled or your car has been infected with ransomware and will not start, allow access, accelerate, or slow down unless a ransom is paid.

This idea might not be as improbable as it seems. Researchers recently proved that they can gain remote access to a driving Jeep Cherokee and seize control of the vehicle from the driver. Lights, air conditioning, wipers, the entertainment system, steering, gearbox, and brakes were all tracked by the researchers. Unless they are effectively designed and implemented, we may see more malware attacks on autos as more people grow addicted to connected computer technology. In the past, ransomware outbreaks did not always endanger people's lives. This terrifying idea may become a reality in the near future. [17] [18]

8 Conclusion

In this study, we looked at a broad review of ransomware, including its origins, evolution, malicious repercussions, and prevention strategies. Ransomware has emerged as one of the most dangerous cyber threats to date. Individuals, organizations, healthcare institutions, and information security specialists are fast seeing it as a major danger and concern.

Because of the potential monetary incentives, ransomware has become a popular target for many computer hackers, resulting in its rise. How they're propagated, and how they've mastered the art of manipulating human psychology to increase their demands. We looked at how widespread the malware problem is and found that it affects most of G20 countries.

It is becoming increasingly localized, demonstrating that the problem is both global and local at the same time. We also looked at how technological breakthroughs like the Internet of Things (IoT) may allow hackers to attack new industries with ransomware.

What this study demonstrates more than anything else is that putting a focus on security is critical for everyone. Combating cybercrime may be a massive undertaking, and we all have a role to play. Simply examining the traditional benign use scenarios is no longer sufficient for application developers developing new technologies or goods.

Cybercriminals will find weaknesses that allow things to be controlled or denied functioning to owners. The challenge for innovators is to increase security while simultaneously considering potentially damaging uses and scenarios.

Innocent victims must take simple security steps, such as ignoring malicious programs and correcting vulnerable software faults, to safeguard their data from ransomware. Analyze the potential of ransomware and devise a strategy to mitigate the potentially dangerous situations.

9 Reference

1. Trend, Labs. “Ransomware - Definition.” Ransomware - Definition - Trend Micro, Trend Micro, https://www.trendmicro.com/vinfo/us/security/definition/ransomware
2. Ransomware Evolution. https://www.secureworks.com/research/ransomware-evolution
3. “Crypto Ransomware: What’s That?” Document Management System Folderit, 27 Sept. 2017, http://https%253A%252F%252Fwww.folderit.com%252Fblog%252Fcrypto-ransomware%252F
4. “Hackers Adopt SaaS Model to Support Bitcoin Ransomware Schemes.” NewsBTC, 7 Jan. 2016, https://www.newsbtc.com/news/bitcoin/meet-the-javascript-ransomware-demanding-bitcoin/
5. What Is Ransomware? | Techniques & Prevention | Terranova Security. https://terranovasecurity.com/what-is-ransomware/
6. KnowBe4. Locker Ransomware | KnowBe4. https://www.knowbe4.com/locker-ransomware
7. “What Is Scareware? Definition and Explanation.” Www.Kaspersky.Com, 9 Dec. 2021, https://www.kaspersky.com/resource-center/definitions/scareware
8. What Is Ransomware as a Service (RaaS)? The Dangerous Threat to World Security | UpGuard. https://www.upguard.com/blog/what-is-ransomware-as-a-service.
9. Dossett, Julian. “A Timeline of the Biggest Ransomware Attacks.” *CNET*, https://www.cnet.com/personal-finance/crypto/a-timeline-of-the-biggest-ransomware-attacks/
10. James, Alex. “University Hit With $1.14m Ransomware Attack.” Hut Six, https://www.hutsix.io/university-of-california-ransomware-attack/.
11. Good, Keith. “JBS Systems Coming Back Online After Ransomware Attack • Farm Policy News.” *Farm Policy News*, 2 June 2021, https://farmpolicynews.illinois.edu/2021/06/jbs-systems-coming-back-online-after-ransomware-attack/.
12. “Colonial Hack: How Did Cyber-Attackers Shut Off Pipeline?” *BBC News*, 10 May 2021. *www.bbc.com*, https://www.bbc.com/news/technology-57063636.
13. “Kaseya Ransomware Attack Explained: What You Need To Know.” *PurpleSec*, 23 July 2021, https://purplesec.us/kaseya-ransomware-attack-explained/

14. Sze, Maricar. “CWT Pays $4.5M Following Ransomware Attack.” *Myce.Com*, 6 Aug. 2020, https://www.myce.com/news/cwt-pays-4-5m-following-ransomware-attack-93873/
15. Krehel, Ondrej. “Council Post: The 2021 Kaseya Attack Highlighted The Seven Deadly Sins Of Future Ransomware Attacks.” Forbes, https://www.forbes.com/sites/forbestechcouncil/2022/01/25/the2021-kaseyaattack-highlighted-the-seven-deadly-sins-of-future-ransomware-attacks
16. 5 Strategies Ransomware Prevention | BeyondTrust. https://www.beyondtrust.com/blog/entry/ransomware-5-prevention-strategies
17. U. Javed Butt, M. Abbod, A. Lors, H. Jahankhani, A. Jamal and A. Kumar, "Ransomware Threat and its Impact on SCADA," *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*, London, United Kingdom, 2019, pp. 205-212. .[Online].Available:https://ieeexplore.ieee.org/document/8688327/references#references
18. D. Garg, A. Thakral, T. Nalwa and T. Choudhury, "A Past Examination and Future Expectation: Ransomware," *2018 International Conference on Advances in Computing and Communication Engineering (ICACCE)*, Paris, 2018, pp. 243-247.[Online].Available:https://ieeexplore.ieee.org/document/8441743/references#references