Ransomware Trends and Countermeasures: A Comprehensive Analysis

Harsh Oza
CSE dept. of Nirma University
Ahemdabad, India
20bce182@nirmauni.ac.in

Vivek Patel
CSE dept. name of Nirma University
Ahemdabad, India
20bce226@nirmauni.ac.in

Aditi Rathod
CSE dept. name of Nirma University
Ahemdabad, India
20bce242@nirmauni.ac.in

***Abstract*—Ransomware is a dangerous type of virus that encrypts data or prevents access to computers while demanding ransom payments from victims. This study divides ransomware into well-known kinds like Locker and Crypto Ransomware, as well as newer varieties like Scareware, Leakware, and Ransomware-as-a-Service (RaaS). Each category is detailed in length, explaining its distinguishing features.The study then digs deeper into well-known ransomware versions such as Ryuk, Maze, REvil, Lockbit, DearCry, and Lapsus$, providing insights into their methods and targets.Importantly, the research emphasizes effective ransomware defenses, such as cyber-awareness education, regular data backups, patching, user authentication processes, and attack surface reduction. It also provides insights into current ransomware attack tendencies, including statistics from McAfee and Kaspersky studies, as well as practical advice for controlling active ransomware infestations.**

***Index Terms*—Ransomware,locker, crypto, Ransomware-as-a-Service (RaaS), maze, dearcry**

I. Introduction

Cybercriminals utilise ransomware, which is a sort of malware (malicious software). When ransomware infects a computer or network, it either prevents access to the system or encrypts its data. In exchange for releasing the data, cybercriminals demand a ransom payment from their victims. A vigilant eye and security tools are suggested for protection against ransomware invasion. After an infection, victims of malware attacks have three options: pay the ransom, try to remove the software, or reset the device. Extortion Trojans commonly employ the Remote Desktop Protocol, phishing emails, and software flaws as attack vectors. As a result, a ransomware assault can affect both individuals and businesses.

A. Types of ransomware:

There were just two major varieties of ransomware for a long time: Crypto and Locker Ransomware. Unfortunately, new varieties of ransomware have evolved, each targeting consumers and companies differently. There are now three varieties of ransomware in use around the world:

- Locker Ransomware
- Crypto Ransomware
- Scareware
- Leakware
- Ransomware-as-a-Service (RaaS)

Let's look at these sorts of ransomware and how they work to make your machine inaccessible.

- **Locker ransomware :** Locker ransomware is a type of ransomware. This sort of malware prevents basic computer processes from functioning. You may be denied access to the desktop, for example, while the mouse and keyboard are partially disabled. This permits you to continue interacting with the ransom demand window in order to make the payment. Aside from that, the PC is unusable. But there is some good news: Locker malware normally does not target essential files; instead, it just wants to lock you out. As a result, complete data destruction is unlikely.
- **Crypto Ransomware :** Crypto ransomware is a type of ransomware. Crypto ransomware's goal is to encrypt your vital data, such as documents, photos, and videos, while not interfering with basic computer functionality. This causes worry because users may view but not access their files. Crypto developers frequently include a countdown to their ransom demand: "If you don't pay the ransom by the deadline, all your files will be deleted." Crypto ransomware can have a devastating impact due to the number of users who are unaware of the need for backups in the cloud or on external physical storage devices. As a result, many victims pay the ransom just to get their files back.
- **Scareware :** As the name implies, scareware shocks consumers by notifying them that their systems have been infected with malware. It dupes consumers into paying a charge or purchasing antivirus software to resolve the issue. Scareware typically displays pop-ups when you access or install malicious software. And here's the main point: your machine hasn't been infected with malware yet, but the antivirus software the scareware wants you to buy is harmful.Malware can only infect your computer if you buy the software. Otherwise, the data will be

Identify applicable funding agency here. If none, delete this.

unaffected, yet popups will continue to assault your computer.Scareware can also be disseminated via spam emails, which deceive people into purchasing worthless goods. These transactions may contain malware capable of stealing important user information.

- **Leakware :** Leakware is ransomware that does more than simply encrypt your sensitive data. Unless you pay their ransom demand, it threatens to release your data to the public or third parties. As a result, it is a riskier form of ransomware than regular crypto-ransomware. Leakware, like crypto-ransomware, encrypts the data set, rendering it inaccessible, and stores the encryption key with the attacker. They ensure that this data is kept private for the victim(s), as disclosing it could harm the individual or the company.
- **Ransomware-as-a-Service (RaaS) :** RaaS, like software-as-a-service, is a business model that distributes ransomware to attackers who lack the time or knowledge to construct it themselves. Instead, attackers can use these "businesses" to purchase or rent ransomware. RaaS is promoted on the dark web in the same manner that adverts for goods and services are promoted on the public internet. Affiliates are the people who buy RaaS. They can gain access to this program by purchasing an online subscription. This subscription may also include standard software-as-a-service features such as 24/7 support and other promotions.This business model enables affiliates with little or little ransomware skills to start a ransomware campaign fast and economically. As a result, RaaS has facilitated the spread of ransomware assaults tremendously. It has also evolved into a self-contained ecosystem of ransomware developers, operators, and other threat actors.

B. Popular Variants of Ransomware :

The 2017 WannaCry outbreak marked the start of the current ransomware mania. This widespread and well reported attack proved that ransomware attacks were both feasible and potentially lucrative. Numerous ransomware variations have since been created and utilized in numerous attacks.

The recent rise in ransomware was also influenced by the COVID-19 pandemic. Gaps in firms' cyber defenses emerged when they quickly shifted to remote work. These flaws were taken advantage of by cybercriminals to spread ransomware, which led to an increase in ransomware attacks. Compared to the first half of 2020, ransomware attacks climbed by 50% in the third quarter.

There are numerous ransomware versions, each with specific features. However, certain ransomware organizations have been more active and profitable than others, setting them apart from the competition.

1) Ryuk :
   An extremely targeted ransomware version is Ryuk. The most prevalent methods of delivery are spear phishing emails or Remote Desktop Protocol (RDP) logins with compromised user credentials. After infecting a system, Ryuk encrypts particular file types (but avoiding those that are essential to a computer's operation), then demands a ransom.
   One of the most expensive ransomware variants in use is known as Ryuk. The average ransom demanded by Ryuk is over $1 million. As a result, Ryuk's cybercriminals mostly target businesses who have the means to satisfy their demands.
2) Maze :
   The Maze ransomware is famous for being the first ransomware variant to combine file encryption and data theft. When targets started refusing to pay ransoms, MazBecause it was the first ransomware strain to combine file encryption and data theft, the Maze ransomware is well-known. When victims started declining ransom demands, Maze started gathering private information from their PCs and encrypting it. This data would either be made publicly available or sold to the highest bidder if the ransom demands were not satisfied. A further inducement to pay up was the prospect for an expensive data leak.
   The organization that created the Maze ransomware has formally ceased operations. This does not, however, imply that ransomware is any less of a concern. The Egregor, Maze, and Sekhmet varieties are said to share a same origin, and some Maze affiliates have switched to utilizing it.
3) REvil (Sodinokibi) :
   Another ransomware strain that targets big businesses is the REvil gang, also referred to as Sodinokibi. One of the most well-known ransomware families online is called REvil. The ransomware organization, which has been in operation since 2019, has been behind many significant breaches, including "Kaseya" and "JBS." It has battled Ryuk for the distinction of most expensive ransomware version over the past few years. It is known that REvil sought $800,000 in ransom. Although REvil started out as a typical ransomware version, it has changed over time. They are stealing data from organizations while also encrypting the files utilizing the double extortion method. As a result, attackers may use other methods in addition to demanding a ransom to decrypt data..
4) Lockbit :
   The ransomware-as-a-service (RaaS) LockBit has been active since September 2019 and encrypts data. This ransomware was created to swiftly encrypt huge enterprises in order to avoid being quickly discovered by security appliances and IT/SOC teams.
5) DearCry :
   Microsoft issued remedies for four Microsoft Exchange server vulnerabilities in March 2021. A new ransomware version called DearCry is intended to exploit four previously discovered vulnerabilities in Microsoft Exchange. Some file types are encrypted by the DearCry ransomware. After the encryption process is complete, DearCry will display a ransom notice telling users to

email the ransomware's operators to request instructions on how to unlock their files.

6) Lapsus$:
A South American ransomware gang known as Lapsus$ has been connected to cyberattacks on prominent targets. The cyber gang is well-known for extortion, threatening the publication of private data if its victims don't comply with its demands. The organization has claimed about getting into companies including Nvidia, Samsung, and Ubisoft. The gang masks malware files as legitimate ones by using stolen source code.

II. Countermeasures :

1) Utilize Best Practices :
An effective plan can significantly reduce the cost and effects of a ransomware attack. Adopting the best practices listed below can lessen an organization's vulnerability to ransomware and lessen its effects
2) Cyberawareness Education & Training:
Phishing emails are frequently used to distribute ransomware. It is essential to educate people on how to recognize and prevent possible ransomware attacks. User education is frequently seen as one of the most crucial defenses a company can employ, as many modern cyber-attacks begin with a targeted email that does not even contain malware but merely a socially-engineered message that tempts the user to click on a harmful link.
3) Regular data backups:
According to the definition of ransomware, this type of malware encrypts data and prevents access without paying a ransom. Automated, secure data backups make it possible for a company to recover from an attack with the least amount of data loss and without having to pay a ransom. To avoid losing data and to ensure that it can be recovered in the case of corruption or disk hardware failure, it is crucial to maintain regular backups of data as part of routine processes. Additionally, working backups might aid firms in recovering from ransomware assaults.
4) Patching:
Patching is a crucial part of preventing ransomware attacks since hackers frequently search the patches for the most recent discovered exploits and then target unpatched systems. Because fewer possible vulnerabilities exist within the company for an attacker to exploit, it is crucial that firms make sure all systems have the most recent fixes applied to them.
5) User authentication:
Using stolen user credentials to access services like RDP is a common tactic employed by ransomware attackers. A password that has been guess or stolen may be more difficult for an attacker to use with strong user authentication.

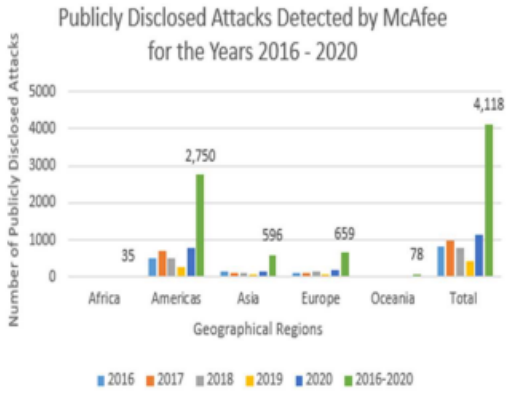

Fig. 1. Publicly Disclosed Attacks for the Years 2016 - 2020

Fig. 2. Top Targeted Industries for the Years 2016 - 2020

A. Reduce the Attack Surface :

With the high potential cost of a ransomware infection, prevention is the best ransomware mitigation strategy. This can be achieved by reducing the attack surface by addressing:

- Phishing Messages
- Unpatched Vulnerabilities
- Remote Access Solutions
- Mobile Malware

III. Ransomware attack trends :

A. Trends from McAfee ISTR

McAfee annual reports offered information on publicly known attacks by area, top targeted sectors, and top attack vectors. Because the McAfee data came in the form of graphs, we extracted estimated values rather than actual values. There were 4,118 publicly acknowledged attacks across five areas. North and South America revealed the most attacks (2,750), whereas Africa revealed only 35 attacks, the fewest of any of the specified locations. 596 and 659 incidents were reported in Asia and Europe, respectively. Oceania reported only 78 attacks. With 1,407 attacks, the malware attack vector ranked first among top attack vectors. There were 1,317 unknown attack vector attacks, and cyber thieves hijacked

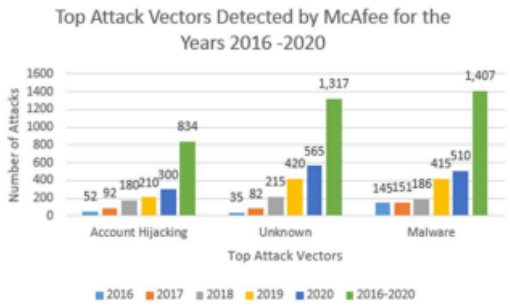

Fig. 3. Top Attack Vectors for the Years 2016 - 2020

Fig. 4. Banking Targeted Countries for the Years 2016 - 2020

accounts 834 times. The riskiest component of this trend is that McAfee classified 1,317 attacks as unknown. This perilous element compelled corporate sectors to take the most precautionary precautions against unknown/zero-day assaults.

B. Trends from Kaspersky ISTR

The Kaspersky quarterly reports included information on banking-targeted nations, top banking malware families, online targeted attacks, and the percentage of vulnerable apps . Kaspersky is a Russian antivirus business that mostly serves Asia and Africa. As a result, we were unable to find much information about American and European countries from Kaspersky ISTR.

With over 1.5 million attacks, Zbot was the financial sector's nightmare among top banking malware families. The Nymaim family of malware has infected the financial sector over 0.5 million times. With 281,877 attacks, "RTM" was the third most deadly malware family. With 227,745 attacks, Emotet was discovered to be the fourth most deadly malware. With 208,177 and 190,476 attacks, respectively, Gozi and SpyEye were among the most devastating malwares.

The United States led the way in online targeted attacks, with more than 4.4 billion online attacks recorded by Kaspersky. With almost 1.8 billion internet attacks, the Netherlands was the second most attacked country. With 1.0 billion attacks, Germany was the third most vulnerable country. In the last five years, cyber thieves targeted

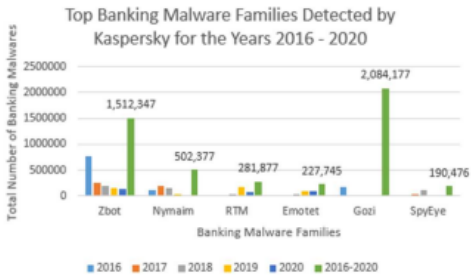

Fig. 5. Banking Malware Families for the Years 2016 - 2020

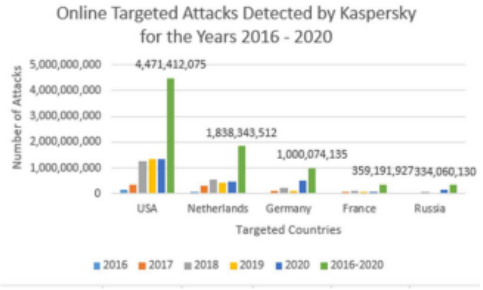

Fig. 6. Online Targeted Attacks for the Years 2016 - 2020

France more than 359 million times, while Russia was targeted more than 334 million times via online attacks.

IV. How to Remove Ransomware ?

A ransom message is not something anyone wants to see on their computer as it reveals that a ransomware infection was successful. At this point, some steps can be taken to respond to an active ransomware infection, and an organization must make the choice of whether or not to pay the ransom.

- How to Mitigate an Active Ransomware Infection. Many successful ransomware attacks are not discovered until after the data has been encrypted and a ransom notice has shown on the screen of the affected computer. The encrypted files are probably beyond saving at this time, however the following actions must be taken right away:
- The machine should be quarantined since some ransomware variations will try to infect other computers and associated drives. By denying the infection access to other potential recipients, you can control its spread.
- Keep the Computer Running: File encryption can cause a computer to become unsteady, and turning off a computer can cause the loss of volatile memory. Keep the computer running to increase the likelihood of recovery.
- Make a Backup: With some ransomware variations, files can be unlocked without paying the demanded ransom. Create a backup of any encrypted files on a portable drive in case a fix is discovered down the

road or the files are damaged during an unsuccessful decryption attempt.

- Check for Decryptors: See if a free decryptor is available by contacting the No More Ransom Project. If so, try using it to restore the files on a copy of the encrypted data.
- Ask for Assistance: Backup copies of files stored on computers are occasionally kept. If the infection has not removed these copies, a digital forensics expert might be able to recover them.
- Wipe and restore: Use a fresh operating system installation or backup to restore the computer. By doing this, the infection is eradicated entirely from the device.

REFERENCES

[1] D. Farhat and M. S. Awan, "A Brief Survey on Ransomware with the Perspective of Internet Security Threat Reports," 2021 9th International Symposium on Digital Forensics and Security (ISDFS), Elazig, Turkey, 2021, pp. 1-6, doi: 10.1109/ISDFS52919.2021.9486348.

[2] A. Adamov and A. Carlsson, "The state of ransomware. Trends and mitigation techniques," 2017 IEEE East-West Design & Test Symposium (EWDTS), Novi Sad, Serbia, 2017, pp. 1-8, doi: 10.1109/EWDTS.2017.8110056.

[3] A. A. M. A. Alwashali, N. A. A. Rahman and N. Ismail, "A Survey of Ransomware as a Service (RaaS) and Methods to Mitigate the Attack," 2021 14th International Conference on Developments in eSystems Engineering (DeSE), Sharjah, United Arab Emirates, 2021, pp. 92-96, doi: 10.1109/DeSE54285.2021.9719456.

[4] Z. Song, Y. Tian and J. Zhang, "Similarity Analysis of Ransomware Attacks Based on ATTCK Matrix," in IEEE Access, vol. 11, pp. 111378-111388, 2023, doi: 10.1109/ACCESS.2023.3322427.

[5] S. R. B. Alvee, B. Ahn, T. Kim, Y. Su, Y. Youn and M. Ryu, "Ransomware Attack Modeling and Artificial Intelligence-Based Ransomware Detection for Digital Substations," 2021 6th IEEE Workshop on the Electronic Grid (eGRID), New Orleans, LA, USA, 2021, pp. 01-05, doi: 10.1109/eGRID52793.2021.9662158.

[6] J. S. Aidan, H. K. Verma and L. K. Awasthi, "Comprehensive Survey on Petya Ransomware Attack," 2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS), Jammu, India, 2017, pp. 122-125, doi: 10.1109/ICNGCIS.2017.30.

[7] D. Zhuravchak, T. Ustyianovych, V. Dudykevych, B. Venny and K. Ruda, "Ransomware Prevention System Design based on File Symbolic Linking Honeypots," 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Cracow, Poland, 2021, pp. 284-287, doi: 10.1109/IDAACS53288.2021.9660913.

[8] N. Aldaraani and Z. Begum, "Understanding the impact of Ransomware: A Survey on its Evolution, Mitigation and Prevention Techniques," 2018 21st Saudi Computer Society National Computer Conference (NCC), Riyadh, Saudi Arabia, 2018, pp. 1-5, doi: 10.1109/NCG.2018.8593029.