International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 2 Feb. 2023, pp: 25-30 www.ijaem.net ISSN: 2395-5252

Analysis of crypto ransomware in windows system

Shivani Raval, prof. Hetvy Jadeja
Marwadi University, Rajkot

Date of Submission: 01-02-2023 Date of Acceptance: 10-02-2023

ABSTRACT:
Ransomware encrypts all the data on your computer and holds that data for ransom. In today's world, both the public and private sectors are highly affected by ransomware.[1] As there has been a great increase in popularity digitalization. Ransomware is a category of malware that restricts or stops users from accessing their systems, either by locking the system's screen or by encrypting the users' files, until a ransom is paid.A harmful program called "crypto-ransomware" encrypts files on a computer in order to demand payment. The use of crypto currencies has facilitated ransomware attacks, in part because they are decentralized, meaning that criminal organizations can take steps to obscure and hinder transactions.[2] Governments, educational institutions, and healthcare providers in the United States Crypto-ransomware prevents you from accessing your computer data, systems, or networks and demands a ransom payment.In this review paper, I have defined some crypto-ransomware that affects the system, and analysis has been done for static analysis using VirusTotal and for dynamic analysis done using a cuckoo sandbox[3].

Keywords: Windows, operating system, crypto ransomware, and ransomware analysis.

I. INTRODUCTION:

Longer-term data, as per trade watchers, is in Bitcoin's advantage.[4] Investors' confidence in the cryptocurrency market may also increase as a result of their expectation that the US Federal Reserve will implement gradual interest rate increases starting in the second half of this year and continuing through 2023 as a result of positive CPI data.

The Economic Times reported that almost 20 million people in India use crypto currencies.[5]According to Chain analysis, a business that specializes in block chain analysis, the global use of crypto currencies increased by 880% in 2021.

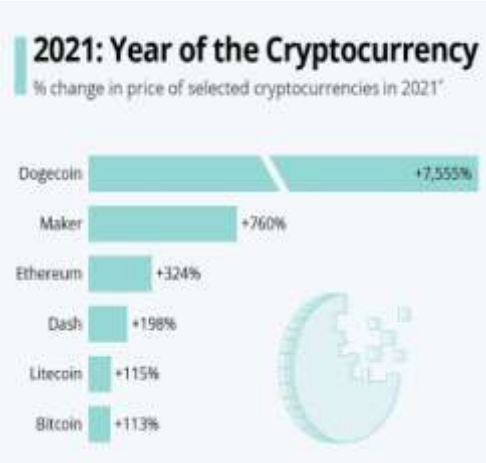

Figure 1.1 Year of the Cryptocurrency

Crypto ransomware means perform encrypt the user system data using strong encryption techniques. These techniques, including email links and attachments, are disseminated through phishing emails and websites that encourage software downloads, pop-up advertisements, and the use of, any software.[6] Ransomware has become an important and developing security issue for the past few years.

Most hackers are capable of installing crypto-ransomware on victims' computers. A very risky assault known as a "Crypto Locker" locks down computer files and demands payment in crypto currency, specifically bitcoin, ethereum, and other altcoins, to unlock the files.[7]

46% of small businesses have been the targets of ransomware attack. Ransomware attack, almost three-quarters (73%) have paid a ransom.[8] 43% of small businesses paid between $10,000 and $50,000 to Ransomware attackers, and 13% paid

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 2 Feb. 2023, pp: 25-30 www.ijaem.net ISSN: 2395-5252

more than $100,000. Of those who paid, however, 17% recovered only some of the company's Data.

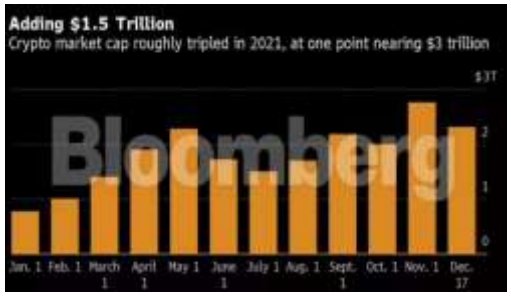

Figure 1.2 Loss of money effect ransomware

There are numerous analysis techniques, including static, dynamic, and hybrid analyses. The proposed detection method for a dynamic analysis detector makes use of numerous application properties while doing the analysis.[6]

Ransomware affected many organizations for that graph defined this category.[9] Like government, education, healthcare, services, technology, manufacturing, retail, finance.

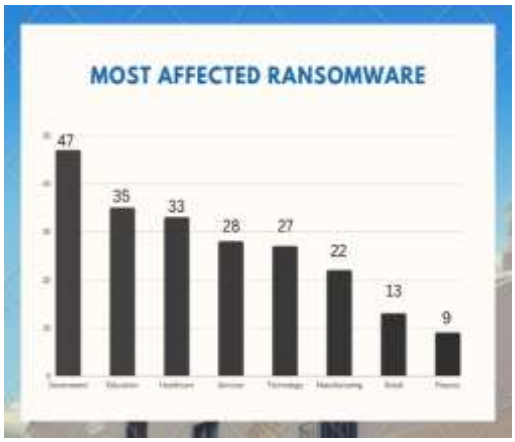

Figure 1.3 most effected ransomware

1.1 How is ransomware working on computer

An extremely common and dangerous form of malware known as ransomware is proving to be particularly harmful to both individuals and businesses.[3] In order to gain access to the victim's hardware, ransomware might lock the victim's screens, preventing users from using the system and requesting a ransom payment.[7]Additionally, it has the ability to hack user files utilizing encryption and demand ransom money from the user to release the files.

An important class of malware called crypto-ransomware seeks to use powerful cryptography to encrypt the files on the victim's device.[1]Following file encryption, the malware alerts the user that their files have been encrypted and requests a ransom (often in the form of Bitcoins or another crypto currency) for the file decryption and release.

1.2 Ways a computer get affected by a ransomware

Ransomware is frequently spread by drive-by downloading or dangerous files in phishing emails.And some other actions, like as seeing advertisements, opening pop-up windows, or downloading software on the PC, are also contaminated.[5] Drive-by downloading happens when a user accesses an infected website inadvertently, at which point malware is downloaded and installed on their computer without their knowledge.

Multiple methods are used by ransomware to access the victim's system:Through spam emails with harmful links or attachments. Utilizing weak software's security flaws. Sending traffic to shady ones via websites.[10]

Phishing mail:

When criminals send harmful emails intended to deceive recipients into falling for a scam, this is known as phishing. Often, the goal is to elicit from consumers the disclosure of sensitive data like system logins, financial information, or other types of data. An attacker starts by looking for a mail id pattern. Additionally, make a malicious link, then send the user a Gmail message.[6] This mail is being received by a victim.Is one of phishing mail?Phishing mail initiated with malware to APTs (Advanced Persistent Threat)

Ads or pop – up:

Attack techniques like adware and spyware malware are used to send advertisements and pop-up windows.[9] Between each pop-up that appears and any advertisements placed there to draw you in, you must look for anything connected to your line of work. These advertisements are harmful, and when you click on them, they threaten your system.That action resembles a drive-by download.

Download software:

Any programme you download must come from an unreliable source. By accident, downloading harmful software and connections. Additionally, it has impacted your system and data via the internet.[11] Effects such as multiple file

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 2 Feb. 2023, pp: 25-30 www.ijaem.net ISSN: 2395-5252

generation, data encryption, and file locking target secret information.

1.3 Ransomware analysis

Static analysis

It is also known as a signature-based, code analysis, white box, or misuse detection approach. Approaches in this category often examine static code structure for infection attributes using a pre-defined set of known assailants' signatures without executing the sample.[9]

Despite the fact that static analysis approaches can quickly identify malware in a variety of applications and offer no danger of infection while doing so, they require a sizable pre-defined signature dataset.[7]

Dynamic analysis

It is also known as a black-box strategy, anomaly-based approach, behavior-based approach, and behavioral analysis technique.[4]

The methods in this category execute samples in a restricted/simulated environment, such as a sandboxed, simulator, debugger, virtual machine, or emulator, and then evaluate the samples based on their behaviors.[10]

Hybrid analysis

It is also known as the gray-box strategy. Both static and dynamic analysis techniques are capable of producing workable solutions.[12] Therefore, hybrid analysis approaches which combine the advantages of static and dynamic analyses are preferred.

For example, created a hybrid technique that combines static and dynamic features with a large number of classifiers.[13]

II. LITERATURE REVIEW

Analysis of ransomware on windows system.

Ransomware analysis using different families related to windows platform.[3]Using different techniques for analysis like this paper is define behavior based analysis through make McAfee lab.

An empirical study of ransomware attacks on organizations: an assessment of severity and salient factor affecting vulnerability.[6]This paper to ransomware attack is most of target system and site to generate a report.Choose crypto-ransomware attack and how many percentage affected is define the user system.

Malware analysis by combining multiple detectors and observation windows. Malware developer's attempts to modify the execution pattern of malicious code hiding.[10]Proposes an ensemble detectors which exploits the capabilities of main analysis algorithms.

A Framework for supporting ransomware detection and prevention based on hybrid analysis.The attacker using this malware through encrypt the files located in the infected machine and block the access to them.[4]Attackers will restore the file and provide decryption key and unlock the file after pay amount of money usually given in bit coin.

Detecting ransomware using process behavior analysis.[9]Ransomware is biggest and attractive threats in cyber security.Anti-virus software's are often inefficient against zero-day malware and ransomware attacks, important network infections is result in large amount of data loss.

An Emerging Malware analysis techniques and tools: A comparative analysis. It is conceivable for this malicious software to be installed in a machine without the user knowing.[11] And it's deployed by a third party to steal, corrupt, and destroy the user's confidential material.

Ransomware detection, avoidance, and mitigation scheme: a review and future direction.[5] Cyber-attacks on individuals and corporations across the world. This attack aims to bypass basic security mechanisms and security vulnerabilities in small and large corporations' IT systems.

Analysis on the crypto locker ransomware

Prior to the deployment of the system for data locking mechanism, the malware runs stealthily in the background.[7] Although this attack uses a 2048-bit high-level encryption that is virtually impossible to break, the company stands to lose a great deal of money.

Table: 2.1 Types of analysis to done on crypto ransomware.

Sr. no	Ransomware	Analysis
1	Crypto	Dynamic
2	WannaCry	Static & Dynamic
3	Locker	Dynamic
4	Pet wrap	Dynamic
5	Jipsaw	Static
6	Tesla	Static

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 2 Feb. 2023, pp: 25-30 www.ijaem.net ISSN: 2395-5252

1.4 Crypto Ransomware on windows system

The idea that Macs are immune to ransomware is simply wrong, despite the fact that Windows computers are the most frequent targets for malware attacks. There are a number of ransomware applications that have been made expressly to target Mac OS, according to reports. Malware can infect Macs, and they aren't always more safe than Windows PCs.[14]

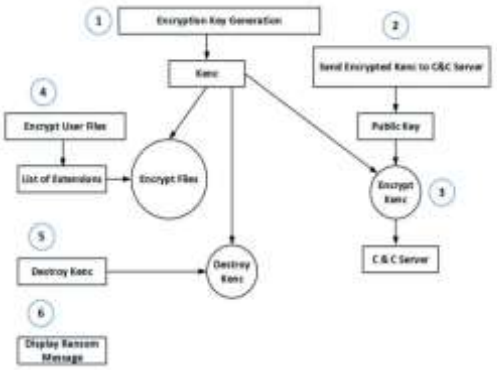

Figure 2.1 Crypto ransomware

One of the most current types of malware, Crypto Ransomware, targets computers by preventing users from accessing the files they have stored inside.[15]In order to restore access to their files, the spyware advises the user to pay a specified sum of money using anonymous payment processors like Bitcoin.

III. CRYPTO RANSOMWARE FAMILIES

1. **Locky:**

- Malware called "Locky" was launched in 2016. Locky assaults victims by encrypting their files, making them unavailable and useless, and demanding cryptocurrency payment.[16]
- Locky all different kinds of organizations have been targeted by ransomware, but the top victim has been the healthcare industry. In the hopes that only one person will open the malicious attachment, the hackers launch an email campaign that targets all the hospital computers they can identify.

Protect our system of Locky Ransomware

- Your greatest line of defense against Locky and other ransomware is robust protection from a trusted provider.
- Regularly back up your files.
- Don’t download unverified attachments.
- Use an anti-malware tool.
- Keep your software up-to-date.
- Disable macros in your Microsoft Office programs.

2. **WannaCry:**

- In May 2017, the ransomware infection known as WannaCry spread quickly across several computer networks.
- WannaCry infected more than 230,000 computers in over 150 countries and $5 billion loss the money.
- WannaCry spreads via a flaw in the Microsoft Windows implementation of the Server Message Block (SMB) protocol.[12]

Protect our system of WannaCry Ransomware

- WannaCry ransomware is to update your OS to the most recent version and then download the correct patch from Microsoft for your version of Windows.
- Even though Microsoft had classified the patch as critical, numerous systems remained unpatched as of May 2017, when WannaCry started spreading quickly.

3. **Bad rabbit:**

- Bad Rabbit ransomware was created in 2017 by the Europe Petya family. The virus locks victims' computers, servers, or files and prevents them from regaining access until a ransom, usually in Bitcoin, is paid.[15]
- In truth, FedEx and other affected organizations suffered significant financial losses as a result of the attack. Merck also suffered financial damages of approximately $275 million, which made numerous companies reevaluate their cyber security insurance plans.
- Bad Rabbit is a form of ransomware that targets unsecure websites and encrypts and locks files.[12] It says that "without our decryption service, no one will be able to recover files."

Protect our system of Bad Rabbit Ransomware

- Only download updates from a reliable source; not third-party websites.
- Perform regular backups.
- Enforce strong password controls.
- Have updated antivirus software.
- Implement network architecture and security controls that segment a corporate network.

4. **Rynk:**

- Ryuk is distinctive in that it is a human-operated ransomware operation, and attackers utilize extremely precise targeting to harm victims.While Hermes, an older ransomware programme, was offered on dark net forums in 2017, Rynk first surfaced in August of that year.[17]
- Hermes and Rynk were reportedly developed by North Korean hackers after the Lazarus Group, an organization supported by the North Korean government, used them in an attack on the Taiwanese Far Eastern International Bank (FEIB) in October 2017.

Protect our system of Rynk Ransomware

- Protect using antivirus software and other security features that have been purposefully turned off by managers in order to boost performance.
- These safeguards are frequently not implemented out of concern that security controls may interfere with operations or have an adverse effect on performance.

5. **Samsam:**

- Introduced in 2018 and Samsam ransomware is a specific infection that is frequently used in targeted assaults and is spread utilizing a variety of exploits or brute-force methods.A successful SamSam attack will almost certainly cause significant disruption to any targeted organizations.[5]
- In 2018, Samsam either utilizes brute force attacks against weak passwords or vulnerabilities in Java-based web servers, file transfer protocol, or remote desktop protocols to access the victims' network.

Protect our system of Samsam Ransomware

- Look for systems on your network that employ RDP for remote connection. If not required, disable the service or apply any available patches.
- Users might have to consult their technology vendors to ensure that patches won't interfere with system operations.
- Set up account lockout procedures and strong passwords to thwart brute force attacks.
- Update your system and software frequently. Keep a solid backup plan in place.

6. **Petya:**

- The Petya ransomware was first identified in May 2016. Its signature technique entails infecting the Master Boot Record in order to run the payload and encrypt any local data that is accessible.[11]
- Petya is able to spread itself like a worm by attacking computers and leveraging the Eternal Blue exploit.
- It also uses classic SMB network spreading techniques, and as a result of that, it can spread within organizations, even if they are patched against Eternal Blue (Symantec Security Response, 2017).[13]

Protect our system of Petya Ransomware

- Cleanup
- Review of the postmortem
- Evaluate user awareness:
- Both formal and informal:
- Strengthen your defenses

7. **Teslacrypt:**

- In early February 2015, Dell Secure Works Counter Threat Unitresearchers researched Teslacrypt, a new file-encrypting ransomware family delivered via the popular Angler browser exploit kit.
- Teslacrypt targets a wide variety of popular file extensions that are present on all general-purpose computing systems. It disregards music and video file formats like MP3s and MP4, as well as several file extensions associated with standard business-class programs.[16]

Protect our system of Teslacrypt Ransomware

- Make regular backup copies of all of your crucial files. After the backup copying is finished, copies should be retained on physically unconnected media.
- The most up-to-date security package with activated security modules will be able to deal with any harmful software that might still find its way onto your PC.

IV. CONCLUSION

This review illustrates several crypto-ransomware together with various tools and methods for analysis. In a recent publication, some crypto-ransomware employed in WannaCry was defined. The reference provides a description of the crypto and lists various families and analysis, including software for static and dynamic analysis. The ransomware file is found by the dynamic analysis tool using the cuckoo sandbox, static analysis, string sysintertional tools, and the online Virustotal tool.[11] With the help of this

application, you can find out which file extensions, the most recent analysis date, common key features, and the number of vendors who have successfully checked these files for ransomware.We will also seek to identify the cuckoo sandbox and other analytical tools, as well as the potential use of other crypto-ransomware such as Petya, Tesla, and others.in future I have find more ransomware and analysis tool.

REFERENCES

[1]. F. Cicala and E. Bertino, "Analysis of Encryption Key Generation in Modern Crypto Ransomware," IEEE Trans. Dependable Secur. Comput., vol. 19, no. 2, pp. 1239–1253, 2022, doi: 10.1109/TDSC.2020.3005976.

[2]. U. Urooj, B. A. S. Al-Rimy, A. Zainal, F. A. Ghaleb, and M. A. Rassam, "Ransomware Detection Using the Dynamic Analysis and Machine Learning: A Survey and Research Directions," Appl. Sci., vol. 12, no. 1, 2022, doi: 10.3390/app12010172.

[3]. A. H. Mohammad, "Analysis of Ransomware on Windows platform," IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 20, no. 6, 2020, doi: 10.13140/RG.2.2.11150.59202.

[4]. F. Mercaldo, "A framework for supporting ransomware detection and prevention based on hybrid analysis," J. Comput. Virol. Hacking Tech., vol. 17, no. 3, pp. 221–227, Sep. 2021, doi: 10.1007/s11416-021-00388-w.

[5]. A. Kapoor, A. Gupta, R. Gupta, S. Tanwar, G. Sharma, and I. E. Davidson, "Ransomware detection, avoidance, and mitigation scheme: A review and future directions," Sustain., vol. 14, no. 1, pp. 1–24, 2022, doi: 10.3390/su14010008.

[6]. L. Y. Connolly, D. S. Wall, M. Lang, and B. Oddson, "An empirical study of ransomware attacks on organizations: An assessment of severity and salient factors affecting vulnerability," J. Cybersecurity, vol. 6, no. 1, 2020, doi: 10.1093/CYBSEC/TYAA023.

[7]. T. Evin, "Analysis on the crypto locker ransomware," no. November, 2021.

[8]. F. Tang, B. Ma, J. Li, F. Zhang, J. Su, and J. Ma, "RansomSpector: An introspection-based approach to detect crypto ransomware," Comput. Secur., vol. 97, p. 101997, 2020, doi: 10.1016/j.cose.2020.101997.

[9]. A. Arabo, R. Dijoux, T. Poulain, and G. Chevalier, "Detecting ransomware using process behavior analysis," in Procedia Computer Science, 2020, vol. 168, pp. 289–296. doi: 10.1016/j.procs.2020.02.249.

[10]. M. Ficco, "Malware Analysis by Combining Multiple Detectors and Observation Windows," IEEE Trans. Comput., vol. 71, no. 6, pp. 1276–1290, Jun. 2022, doi: 10.1109/TC.2021.3082002.

[11]. A. Datta, K. A. Kumar, and A. D, "An Emerging Malware Analysis Techniques and Tools: A Comparative Analysis," Int. J. Eng. Res. Technol., vol. 10, no. 4, pp. 112–116, 2021, [Online]. Available: www.ijert.org

[12]. I. Kara and M. Aydos, "Cyber Fraud: Detection and Analysis of the Crypto-Ransomware," 2020 11th IEEE Annu. Ubiquitous Comput. Electron. Mob. Commun. Conf. UEMCON 2020, pp. 0764–0769, 2020, doi: 10.1109/UEMCON51285.2020.9298128.

[13]. "IET Information Security - 2021 - G mez-Hern ndez - Inhibiting crypto-ransomware on windows platforms through a.pdf."

[14]. S. R. Davies, R. Macfarlane, and W. J. Buchanan, "Differential area analysis for ransomware attack detection within mixed file datasets," Comput. Secur., vol. 108, p. 102377, 2021, doi: 10.1016/j.cose.2021.102377.

[15]. E. Berrueta, D. Morato, E. Magana, and M. Izal, "Open Repository for the Evaluation of Ransomware Detection Tools," IEEE Access, vol. 8Open Repo, pp. 65658–65669, 2020, doi: 10.1109/ACCESS.2020.2984187.

[16]. P. Ryan, J. Fokker, S. Healy, and A. Amann, "Dynamics of Targeted Ransomware Negotiation," IEEE Access, vol. 10, pp. 32836–32844, 2022, doi: 10.1109/ACCESS.2022.3160748.

[17]. X. Ling et al., "Adversarial Attacks against Windows PE Malware Detection: A Survey of the State-of-the-Art," Forthcom. ACM Publ., vol. 0, no. 0, 2021, doi: 11.1111/1111111.1111111.