RANSOMEWARE ATTACK, ANALYSIS AND CONSEQUENCES OF MALICIOUS FILE

Janani, R. Gunasundari*

Abstract

Ransomeware is one of the most Wrecking Cyber-attacks. Malicious software deliberately affects the computer systems, which causes long-term consequences to the companies for financial gains. Ransomeware has evolved extensively and has become technically progressive and alarming. Private Organizations was solid to expertise struggle consequences related to public Organizations. Public Organizations had significantly strong police work postures than non-public sectors. Where Private operates to get profit and breach services causes impairment to them, and Public organizations serve the public with government funds. The encrypted data of ransomware request a ransom payment to restore access or decrypt the data of the majority of ransomware families. This research work has provided the researchers with recommendations and strategies for preventing and protecting malware attacks. Organizations can have a recovery plan to prevent ransomware attacks by the disruption caused through a cloud security gateway.

Keywords: Ransomeware, Malware, Recovery, Cloud Security, Prevention, Protection.

I. INTRODUCTION

Ransomware may be a sort of malware that's accustomed to threatening the victims to pay a selected fee digitally. Anyone will fall victim to a digital extortion attack, from non-public people and celebrities to politicians and organizations. These threats do not seem to be restricted to any specific earth science or operating system and might lend a hand on any range of devices. Ransomware exploits everything from Android devices, iOS systems, or Windows systems to be in danger. In the previous year, the ransomware attacks are renewed diligently by the hackers. [1]

The Techie merely square measure obstruction individuals penetrating the computers and posing for ransom to recoup the access. The cyber crooks have conjointly immobilized the government concerns. Little businesses and hospitals were conjointly forced to pay the ransom and Stringent huge pay to regain access.

There is no plan; however, typically, these attacks occur as many victims favour paying the ransom to regain access while not intimating the Government. However, ransomware attacks 2020 show associate acute rise within cybersecurity.[2]

II. RANSOMWARE ATTACKS - 2020

Ransomware spots both big and small trades in an identical manner. According to 2020 news, for around 30 hours, a payload transfer facility was compelled to shut down. It has taken over the company's control system, which included the power files indispensable for the processing. Most of the ransomware knowledge square measure encoded. In the last year, ransomware attacked 51% of small and large trades. Most of the affected data are encoded. In that, 26% of ransom was paid by the victim to get the data access back.[3]

A few did not get the data back even after paying the ransom. Probably around 95% of the victims got back the business information after paying the ransom.

Department of Computer Science,
Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India
*Corresponding Author

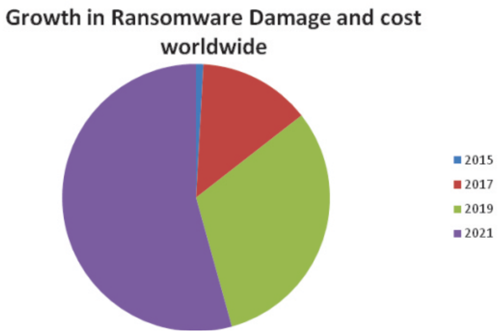

Fig.1: Growth in Ransomware Damage and cost worldwide

The organizations also regain the data that were encoded. Few of them got the information back through backup instead of remitting settlement, and 1 Chronicle of victims who paid the settlement did not get the information back.[4] The ransomware shatters several financial industries and healthcare organizations. Many organizations are invested in stopping ransomware. Either massive or little company is exempt from cybercrime lawbreaking attacks.

Many organizations to restore the data decide to pay the ransoms. Examples of ransomware virus attacks and consequences.[5]

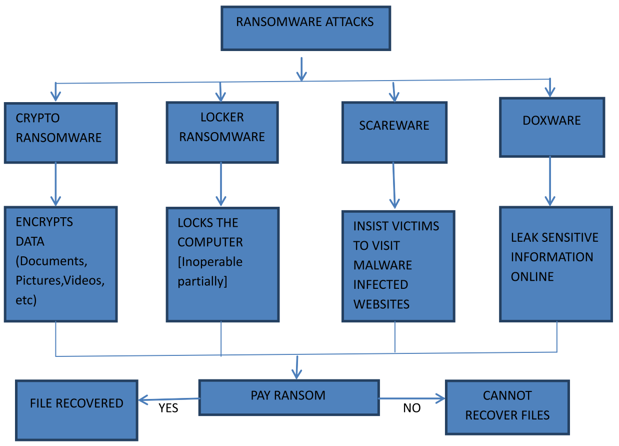
RANSOMWARE ATTACKS
CRYPTO RANSOMWARE
LOCKER RANSOMWARE
SCAREWARE
DOXWARE
ENCRYPTS DATA (Documents, Pictures,Videos, etc)
LOCKS THE COMPUTER [Inoperable partially]
INSIST VICTIMS TO VISIT MALWARE INFECTED WEBSITES
LEAK SENSITIVE INFORMATION ONLINE
FILE RECOVERED
YES
PAY RANSOM
NO
CANNOT RECOVER FILES

Fig2: Ransomware Attacks

Crypto Ransomware

The aim is to inscribe the necessary knowledge like docs, pictures, and videos to not interfere with basic computer operations. It creates a panic state of affairs because the files are visible and cannot be accessed. Crypto developers add count down to the ransom demands. If the user does not pay the ransom within the time limit of crypto developers, the data will be deleted. Many victims pay ransoms who are unaware of backups in clouds or on external physical storage devices to get back the data.[6]

Locker Ransomware

This cripples the user from logging in, and the entire system is locked. That is, this sort of malware abandons essential computer functions. For instance, access is also denied to desktop to desktop, whereas mouse and keyboard units are partly disabled. It permits continued to move with windows containing the ransom demand to form the payment. Aside from the PC is inoperable. This locker ransomware does not target critical files; it just wants to lock the computer. Therefore there will not exist destruction of data.[7]

Scareware

Malicious software that insists the users visit malware-infested websites. It is also known as deception software, rogue scanner software, or fraud, which may come from pop-up windows. It displays legitimate warning messages that are from antivirus software companies and affirms that the files are infected[8]. To decrypt the infected files, the users are threatened to pay ransom for quickly purchasing software that fixes the so-called problem. Fraudulent also send spam mail to implement scareware. Falling into it by opening the scam mails and giving credit card details opens the door for future identity thefts.[9]

Doxware

The doxware fraud threatens the victims to release sensitive information if ransom is not paid, also called doxing. It refers to publishing someone's personal information unknowingly to the victim. The malicious websites or the websites which contain malicious attachments are discharged through phishing emails. It works similar to other ransomware, which encrypts the files and demands a ransom. The hackers make a twofold threat that the data will be encrypted, and it steals the sensitive information published online if the victim does not pay the ransom.[10]

III. SOME PREVENTIVE MEASURES ARE GIVEN TO PROTECT THE DATA FROM RANSOMWARE

Identify Ransomware Behaviour:

By putting in ransomware protection, computer code ransomware may be identified by the organizations. As ransomware leaves observable patterns, it can be imprinted easily and blocked once they are detected.[4]

Backing Systems Up:

The lost or hacked data can be saved if the data has a backup on both local and cloud. For further protection, backup on the cloud helps more.

IV. OPEN-ENDED REFLEXIVE MALWARE ANALYTICAL SYSTEM - CUCKOO SANDBOX

Cuckoo sandbox is the leading open-ended reflexive malware analytical system. Any suspectable file may be thrown thereon and in an exceedingly couple of minutes, Cuckoo can offer a consolidated statement tracing the procedure of the file once executed within a sensible, however obscure setting. The attempt of theft is the swiss-army knife of cyber crooks and other disputants to the consortium or agency.

In these developing times, detective work and shedding malware oddments is not adequate. It is exceedingly prominent to grasp; however, it is operated to grasp the conditions, incitements, and intentions of a violation.

The Cuckoo is a simple sandboxing tool for protecting PCs and laptops. The cuckoo sandbox will track the corrupted files that damage the operating system. This tool works on all the operating systems like windows, linux, Macos X and Android. It analyses for virus or malware affected systems. The files, links, videos or games can be downloaded on the PC with the help of this tool without being affected by ransomware attacks.

Cuckoo sandbox is a highly complex standard and 100% open-ended reflexive malware analytical system with boundless application circumstances. By laxity, it is ready to:

- The actualized Android Platforms, Windows, Mac Operating System, and Linux analyses various scurvy files like exe files, MS Office documents, pdf files, electronic mails, and malicious websites.
- The files can be distilled into crucial knowledge and endorsement explicable by anybody by tracing API calls and the generic etiquette of the file.
- Once encoded with SSL/TLS, the web auction has to be abandoned and evaluated. Drop all auction or drag it through Internet services simulation Suite a web interface or a Virtual Private Network with regional web whopping reinforcement.
- To carry out up to date evocation survey of the contaminated implicit system through variability and on a strategy perception refine using yet another regex analyzer.

V. CUCKOO SANDBOX DESIGN WITH CONTROL MANAGEMENT SOFTWARE

The central management software of cuckoo sandbox handles sample analysis and execution. A contemporary isolated virtual or physical machine operates every analysis. A variety of guest machines associates and a host machine are the dominant facets of the Cuckoo's framework. The host machines are the administration software, and also the variety of guest machines are identical or corporal machines for assessment. The complete analysis method is managed by the core part of the sandbox which the host executes. Whereas the isolated environment safely executes and analyzes the malware samples.

VI. Avira Protection cloud Technology

By developing the Avira protection cloud technology, the number increased where there are several hundred thousands of potential malware samples every day, to detect even more. The primary task of the avira protection research lab is to classify the samples and analyze their behaviour, either for inclusion within the virus knowledgebase or for repair. The manual method of the detection and analysis of samples that could be unbelievable quantity is not possible.

VII. Sample Deeds And Functionalities Of The Ascendable System

For this, an ascendable system has got to be built with detailed data concerning sample behaviours and functionalities. An automatic and reliable system is required. Cuckoo sandbox is that the tool accustomed the elaborate data.

- **Stability**

If Cuckoo crashes once in thousand samples, it desires numerous maintenance to try to. Therefore the main task is bug fixing.

- **Performance**

The better performance suggests that less hardware running. Much hardware required is that the costlier and becomes worst. By raising the performance, the results are going to be achieved quicker.

- **Classification**

The samples have to be compelled to be classified at least into two teams, either good/wrong samples that ought to be automatically done by the Cuckoo. Meta signatures are the most essential feature that runs at the end for classification wherever many weaker sections are combined.

- **Data Collection**

The registry keys, services, files are modified, which might be read, stopped, deleted and a lot. With this data, the repair and automatic generation of an outline is simply one step away.

- **Other Monitor**

The open source tool volatility is in the position to require a memory snapshot of the OS and scan for anomalies, whereas Cuckoo commonly monitors malware within the user area. Its specialty is distinguishing DKOM [Direct Kernal Object Manipulation].

Use Cases

Cuckoo is intended to use as discrete operations in addition on integrated in larger frameworks. It is accustomed to inspect:

- Universal windows Exe files
- Dynamic-link library Files
- Portable document format Files
- Microsoft Office documents
- Universal resource locator Files
- Hypertext markup language
- Hypertext preprocessor scripts
- CPL files
- VB Script
- ZIP files
- Java JAR files
- Python files and
- Almost everything else

As it has portable and influential scraping credentials, there is no constrict to Cuckoo’s attained.

VIII. CONCLUSION

Ransomware onsets have immobilized consortium and agencies dazed within the consciousness of the extermination determined. Consortiums should deluge in protective software that confirms the cyber crooks from intruding perceptive data knowledge.

Furthermore, coaching the human resources to notice and preclude these assaults is requisite. Moreover, enterprises should routinely observe their knowledge secured regionally together within the cloud.

Because the malware endures emerging, therefore will the software to notice and exile it. Enterprises should steadily stay one or many steps sooner than technocrats to keep their knowledge and PC safe.

Cuckoo and supporting processes perform a lot of reliable cleanups. It also aimed to cleanse the code base, raise stability, scale back impulsive behaviour, and support virtual boxes.

To backlog and sustain digital knowledge for each task, the technology has been raised the province of working-class person on the cybernetic equipment to take care of the knowledge. The projected research technique prevents from the ransomware execution for analysis of each new generated file in the system

REFERENCES

[1] Lena Y.Conolly, David S.Wall, The rise of cryptoransomware in a changing cybercrime landscape: Taxonomising countermeasures, computers and security, volume 87,2019,101568,ISSn 01674048 https://doi.org/10.1016/j.cosc.2019.101568.

[2] Lena yuryna Connolly, David S.Wall, Michel Lang, Bruce oddson, Journal of cybersecurity, Volume 6, Issue 1, 2020, tyaa023, https://doi.org/10.1093 /cybsec/ tyaa 023.

[3] S.H.Kok, Azween Abdullah, NZ Jhanjhi, Early detection of crypto-ransomware using Pre-encryption detection algorithm, Journal of king saud university-computer and information sciences,2020,ISSN 1319-1578, https://doi.org/10.1016/j.jksuci.2020.06.012.

[4] Mamoona Humayun,NZ Jhanjhi,Ahmed Alsayat, Vasaki Ponnusamy, Internet of things and ransomware: Evolution, mitigation and prevention, Egyption Informatics, Journal, volume 22, Issue 1, 2021, ISSN 1110-8665 https://doi.org/10.1016/j.eij.2020.05.003.

[5] E Russell Ritenour Hacking and ransomware challenges for institutions both large and small American Journal of Roentgenology 214(4), 736-737,2020.

[6] Adam B Turner Stephen MCCombie, Allon J uhlamnn Discoverning payment patterns in Bitcoin from ransomware attacks Journal of Money laundering Control, 2020.

[7] Yahye Abukar Ahmed, Barkoer, Shamsal Huda, Bander Ali Saleh AI-rimy,Mohammed Mehedi Hassan, A system call refinement based enhanced Minimum Redundancy Maximum Relevance Method for ransomware early detection, Journal of Network and Computer applications, volume 167,2020,102753, ISSN 1084-8045 https://doi.org/10.1016/j.jnca.2020. 102753.

[8] J Hernandez-castro, A cartwright, E carwright Royal society open science 7(3), 190023,2020. An economic analysis of ransomware and its welfare consequences.

[9] Shubham Sharma1 Satwinder Singh1 Texture-Based Automated classification Ransomware J.Inst.Eng.India Ser.B https://doi.org/10.1007/s40031-020-00499-w.

[10] M.Botacin, P.L. De Geus, A.Gregio." Vanilla" malware Vanishing antiviruses by interleaving layers and layers of attacks J.comp.virol.Hack Techn.154,233-247 (2019).