DALHOUSIE UNIVERSITY

Faculty of Computer Science

Summary Report on Ransomware

CSCI 6708 – Advanced Topics in Network Security

Name: Arka Ghosh
Banner ID: B00911033
Assignment: 06

Introduction

Ransomware is one of the biggest forms of cyber security problem and cybercrime that businesses face in today's world. Ransomware is a kind of malware that restricts the access to the data on a computer system by encrypting the data until the victim pays the attacker a ransom money [1]. In some cases, this type of attack comes with a deadline. If the victim fails to pay within the deadline, the data gets erased permanently or the demand for the money increases. The variants of the Ransomware have been observed for several years and the attackers try to extort the money from the users by showing an on-screen alerts [2]. Generally, these alerts notify the user that the files on the user's system have been encrypted and states the information on how to obtain the decryption key by paying the ransom fee which is payable in the form of Bitcoin [3].

Spread of Ransomware across the System

Ransomware can get into a system in many different ways. Ransomware is commonly spread across the system via phishing emails with malicious attachments or drive-by downloads [2]. Drive-by downloading happens when a person accesses an infected or malicious website without realizing it, and malware is downloaded and installed without the user's awareness. Additionally, with employees moving to the work-from-home paradigm from 2020, the use of Virtual Desktop Infrastructure (VDI) has increased rapidly which has regrettably turned into a fast expanding attack surface for the Ransomware. With employees migrating to a work-from-home paradigm in 2020, the use of virtual desktop infrastructure (VDI) [4] has continued to rise rapidly. Regrettably, it's also turned into a fast expanding assault surface. The fact that all infrastructure and apps are frequently on the same server is a huge VDI risk. It might be difficult to identify malware once it has been successfully introduced by an attacker until it is too late. Furthermore, without specific policies to regulate east-west traffic inside a network segment, an attacker can maximize damage by encrypting anything they can reach. Moreover, Managed Service Providers (MSP) are routinely targeted by cybercriminals through phishing attempts and by targeting the Remote Monitoring and Management (RMM) software used by MSP for such kind of attack [5]. After a successful assault on an MSP, fraudsters may be able to spread Ransomware across the MSP's entire client base, putting enormous pressure on the victim to pay the ransom.

Encryption Method of Ransomware

The earlier ransomware attacks, which appeared in the late 1980s and early 1990s, was relied mostly on symmetric encryption, which means the same key was used to encrypt and decrypt the data [6]. As time progresses, the encryption method of the advanced and newer version of the ransomware also evolve a change and adopts a combination of both symmetric and asymmetric encryption. In this type of situations, the attacker generates a unique public-private pair of keys for the victim, in which the private key is used to decrypt data saved on the attacker's server [7]. The attacker usually only gives the victim the private key once the ransom is paid, but as recent ransomware operations have shown, this is not always the case. It's virtually hard to decrypt the data being held for ransom without access to the secret key. Advanced Encryption Standard (AES) is often used for generating such keys [6]. Such kind of malware requires an attack vector to establish its presence on an endpoint. After establishing its presence, malware remains on the system until its mission is completed. Ransomware drops and runs a malicious payload on the affected machine after a successful attack and then looks for and encrypts important files including Microsoft Word documents, photos, databases, and so on. Once the data encryption is done, an on-

screen alert (Appendix A) appears on the victim's system demanding a ransom to be paid within a short period of time.

Mitigation Strategies against Ransomware

The following preventive measures can be taken by the users and administrator to protect their systems from ransomware attacks:

- It is important to keep the operating system patched and updated which reduces the number of exploitable entry points available to an attacker.
- Allowing macros from email attachments should be avoid. If a user opens the attachment and allows macros, the malware will be executed on the system by embedded code.
- Intrusion Detection Systems (IDS) can be used to identify ransomware command-and-control in order to notify against a ransomware system communicating with a command server.
- All vital data should be backed up and recovered using a data backup and recovery strategy. It is critical to regularly backup and test data and systems to reduce the effect of data or system loss and speed up the recovery process.
- Lastly, keep the anti-virus software updated, and scan any application after downloading it from the internet before using it.

References

[1] "What Is Ransomware? - Definition, Prevention & More | Proofpoint US", *Proofpoint*. [Online]. Available: https://www.proofpoint.com/us/threat-reference/ransomware.

[2] "Frequently Asked Questions - Ransomware | Information Security Office", *Security.berkeley.edu*. [Online]. Available: https://security.berkeley.edu/faq/ransomware/.

[3] J. Fruhlinger, "Ransomware explained: How it works and how to remove it", *CSO Online*, 2020. [Online]. Available: https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html.

[4] T. Howard, "How does ransomware actually spread?", *Guardicore*, 2021. [Online]. Available: https://www.guardicore.com/blog/how-ransomware-actually-spreads/.

[5] "How ransomware spreads: 9 most common infection methods and how to stop them - Emsisoft | Security Blog", *Emsisoft | Security Blog*, 2019. [Online]. Available: https://blog.emsisoft.com/en/35083/how-ransomware-spreads-9-most-common-infection-methods-and-how-to-stop-them/.

[6] M. Lessing, "How Does Ransomware Work?". [Online]. Available: https://www.sdxcentral.com/security/definitions/how-does-ransomware-work/.

[7] "What Is Ransomware? | McAfee", *Mcafee.com*. [Online]. Available: https://www.mcafee.com/enterprise/en-ca/security-awareness/ransomware.html#:~:text=How%20does%20ransomware%20work%3F,stored%20on%20the%20attacker's%20server.

[8] N. J. Rubenking, "The Best Ransomware Protection for 2022", *PCMAG*, 2022. [Online]. Available: https://www.pcmag.com/picks/the-best-ransomware-protection?test_uuid=06r4MYCu5PZzCkufjQSV3po&test_variant=b.

Appendix

Appendix A

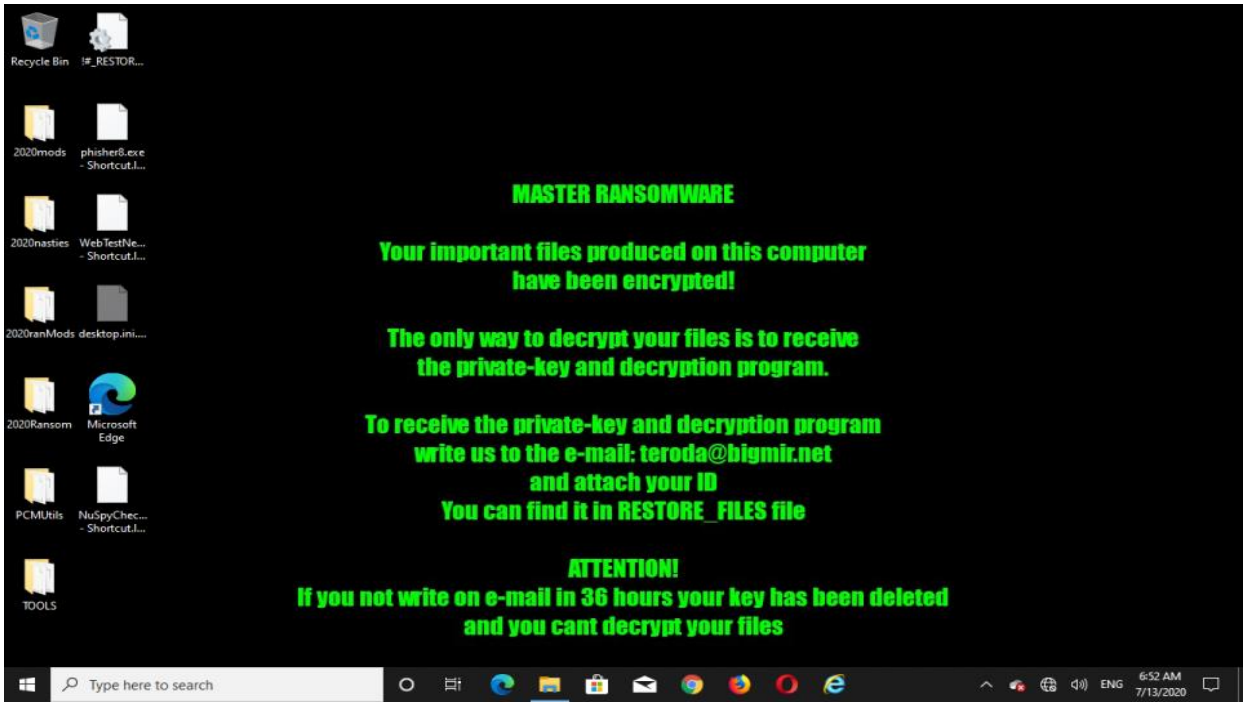

Figure: Ransom Note on the Victim's Screen [8]