Grenze International Journal of Engineering and Technology, Special Issue

Understanding the Influence of Ransomware: An Investigation on its Development, Mitigation and Avoidance Techniques

Lingala Thirupathi[1], Prof. P.V. Nageswara Rao[2]
[1]Methodist College of Engineering & Technology /CSE Department, Hyderabad, India
Email: thiru1274@gmail.com
[2]GITAM (Deemed to be University)/CSE Department, Vishakhapatnam, India
Email: nagesh.uma@hotmail.com@gmail.com

***Abstract*—Ransomware is a way of money extortion by cyber-attackers in which user's files are encrypted and the decryption key is held by the attackers until a ransom amount is received from the victim. It is a highly advanced malware in which developing new variants is trivial thereby facilitating the evasion of many antivirus and intrusion mitigation systems. The cyber-attackers behind the development of ransomware are constantly improving their attacking strategy by improving the malwares constantly. This is making it harder to develop effective long-lasting countermeasures to prevent such attacks. With the increase in usage of smartphones, even they are being targeted besides desktops and servers. In this paper, we present a brief history of ransomware, best safety mechanisms to prevent such attacks. Recent attacks on famous organizations are discussed with respect to monetary loss involved in those attacks. We propose a model to prevent and detect any cryptographic operations in business organization.**

***Index Terms*— Ransomware, Malware, Ransomware mitigation and Avoidance.**

I. INTRODUCTION

The growth of information and communication Technology, within a society has become increasingly digitized, thus, the overall activity has amounted to various researches for protecting any data from malicious threats. Recently, ransomware has been a rapidly propagated subject for social engineering techniques especially the ransomware. Malicious codes are the primary threat of cyber-attacks, the malicious programs are placed without user's approval at same time access user system's protection to control user system secretly [2].The primary malicious codes are virus-typed to damage the systems. Ransomware is one of the recently surfaced cyber-attacks. One of the sharpest variations between typical malware and ransomware is that the second ransomware ends its activity by declaring its occupation to the user.

Ransomware is very automated, such that exceeding the "distribution stage", most of the ransomware manner works independently without the need of interaction with a C2 (command and control) to get directions. Rather, ransomware are the executable that bears all the logic needed to hijack a computer [3]. In the case of protecting a system from ransomware, it is adequate to execute pre-mitigation, preferably than post-mitigation, to protect user's important data. Ransomware is a new top concern which uses social engineering

Grenze ID: 01.GIJET.4.3.25

techniques that are utilized to ignite user's curiosity and the urge the users to request. That makes such malware to be more dominant threat [4].
This bunch of circumstances initiates our concern in investigating ransomware behavior. Through presenting the outcomes to the security community, the concern is to get a better understanding by security analysts wherever to this kind of malware happens. Fortified with this knowledge, analysts may be able to respond faster in the case, their organization that is invaded by a ransomware infection. Hence, this paper provides a review of ransomware evolution, mitigation, and avoidance techniques by suggesting a model.

II. The Evolution of Ransomware

Ransomware is defined as a kind of Trojan virus that mostly targets computers running on Microsoft Windows Operating System. Ransomware develops through email attachments using social engineering showing it as a normal file. When aroused, the ransomware utilizes the encryption of a secret key stored into its control server and RSA open key to encrypt the files with special formats in the local network drive [5, 6].
Ransomware is a kind of malicious software cyber actors use to reject access to systems or data. The malicious cyber actor takes systems/data hostage until the ransom is paid in the form of bit coin. After the first attack, the ransomware tries to spread in the shared storage drives and other available systems. If the needs do not meet i.e., the ransom is not paid, then the system or encrypted data remains unavailable to the user, or data may be removed [7].
Dublin Midlands Hospital Group has confirmed an isolated ransomware attack at the Midlands Regional Hospital in Tullamore(IRELAND) on **15th Nov-2018**.There was no impact on patient care following the attack, which affected the Laboratory Information System. There is also no evidence of other parts of the wider health service being affected by the attack, the group said.

III. Types of Ransomware

1. Reveton- Declares itself a lawful and legitimate authority.
2. CryptoLocker- It is a file encryption ransomware that encrypts the private records.
3. CryptoLocker.F and TorrentLocker- It is a Trojan horse virus.
4. CryptoWall- It applies it as a Java Script code as a part of an email attachment.
5. FuSob- It is a type of malware which will affects the mobile phones.
6. WannaCry- It is the latest ransomware executed in may-2017, and mainly targets MS-Windows.

IV. The Financial Impact of Ransomware

Nowadays the business organizations are continuously affected by ransomware attacks. The organizations have to be fully aware of the consequences posed by ransomware and its impacts by employing robust IT infrastructures and effective defenses techniques. The financial loss is the main reason for ransomware development. Hence, being infected with such malware cause the business to loss thousands of dollars, especially without using robust defenses.
In 2017, the US is the most affected region by ransomware, as it is accounted for 29% of ransomware infections. Followed by Japan, which reported 9% infection. Also, Italy, India and Germany reported as heavily affected regions.

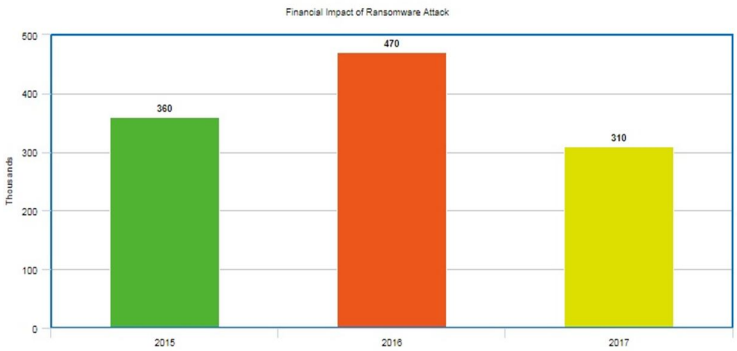

Figure 1.The infections rate of ransomware attack [19]

Table 1 summarizes some of ransomware threats with respect to the monetary impacts.

TABLE I. RANSOMWARE THREATS AND ITS MONETARY IMPACTS [19]

Threat name	Monetary impacts
Cerber	2000$ (0.5 bit coin)
Jaff	1.,467$
Sage	2000$
GlobeImposter	1,401$ (0.35 bit coin)

V. THE MITIGATION AND AVOIDANCE TECHNIQUES OF RANSOMWARE

Avoidance is recognized to be the most powerful protection against ransomware, and it is important to consider precautions for the protection. Infections could be destructive for both individuals and corporations, and restoration may be a tough task demanding the assistance of a reliable data recovery specialist.
Set up spam filters to quarantine suspicious emails and send attachments for advanced inspection in a malware sandbox.Use an exploit execution avoidance module and regularly consume the latest threat intelligence.
To prevent execution of exploits in a user's system. If an attack is stopped before encryption is completed, a user has a chance to get a file encryption key stored in a file system or memory. The encryption process can be interrupted by simply hibernating a system. To block ransomware when ransomware starts encryption, it is recommended: to define additional trust boundaries in an operation systems that will help block a crypto lockers accessing shared folders and network drives.

VI. RECOMMENDATIONS TO MINIMIZE THE IMPACT OF RANSOMWARE

1. Develop and perform a strategy for an end-user awareness program
2. Document your incident response plan for ransomware

VII. MODEL TO PREVENT RAMSOMWARE IN BUISSNESS ORGANIZATION

In the case of malicious attacker to use social engineering techniques, by applying the gastrointestinal technology, the user receives a ransomware code it has been able to be situation (access, receive, peruse, download) for analyzes social engineering threat [10] factors including information collection, rapport, and disguise and ransomware existing characteristics. Based on the analyzed information the model use IP trace-back method that analyzes the possibility and situational frequency by conducting frequency analysis on user's access, receipt, opening, downloading and execution.
With the use of Dynamic and Static Heuristic mitigation Code for white and black list and user's PC registered file lists, it analyzes the frequencies of registered signatures or events and unregistered signatures or events and checks that any codes and drivers are included in unregistered signatures or not . With the results of infection possibility and situational frequency, the model analyzes a risk level. If the analyzed risk level exceeds a designated risk level, the model determines an alarm degree and gives a warning to a user in advance.
Apart from the above suggested model, the organization can also restrict the user from compilation of some executing file which may lead to the ransomware attack. In case the user in the organization want to execute the certain type of the files for example *. exe, *.zip, * etc. from the internet or from the CD or flash, The ticket need to be send to the IT support in order to allow admin access so that the user can execute the desired. The IT support will monitor the request and check the requested file from the user is in the whitelist or blacklist. If the request is from the whitelist, the IT will allow the user to execute the file by allowing remote access.

VIII. Conclusions

This paper discussed the emerging cyber-threat of ransomware from the security perspective. We analyze the monetary impact of the attack with recent attacks on various organizations. The various security measures to be in place in an organization to prevent such an attack were discussed. We propose a model that can be used in the organization to take preventive measures to avoid ransomware attacks.

Acknowledgment

I would like to thank my supervisor for his valuable suggestions.

References

[1] Han, B.J., Choi, Y.H. and Bae, B.C. (2013) Generating Malware DNA to Classify the Similar Malwares. Journal of the Korea Institute of Information Security & Cryptology, 23, 679-694.

[2] Gazet, A. (2010) Comparative Analysis of Various Ransomware Virii. Journal in Computer Virology, 6, 77-90.

[3] Exabeam, INC. (2016) Threat Research Report- The Anatomy of A Ransomware Attack. Accessed in 18/4/2017, available at: http://cdn2.hubspot.net/hubfs/472699/White_P aper/Exabeam_Ransomware_Threat_Report_F inal.pdf?

[4] Kim, D., Soh, W., & Kim, S. (2015). Design of quantification model for prevent of cryptolocker. Indian Journal of Science and Technology, 8(19).

[5] Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., & Kirda, E. (2015, July). Cutting the Gordian knot: A look under the hood of ransomware attacks. In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (pp. 3-24). Springer, Cham.

[6] Mansfield-Devine, S. (2016). Ransomware: taking businesses hostage. Network Security, 2016(10), 8-17.

[7] Sylvia N. Burwell. (2016) Ransomware-what is it and what to do about it. Accessed in 20/4/2017, available at: https://www.justice.gov/criminal-ccips/file/872766/download.

[8] Gandhi, K. A. (2017). Survey on Ransomware: A New Era of Cyber Attack. International Journal of Computer Applications, 168(3).

[9] Tailor, J. P., & Patel, A. D. A Comprehensive Survey: Ransomware Attacks Prevention, Monitoring and Damage Control.

[10] Aurangzeb, S., Aleem, M., Iqbal, M. A., & Islam, M. A. (2017). Ransomware: A Survey and Trends. Journal of Information Assurance & Security, 6(2).

[11] Liao, Q. (2008). Ransomware: a growing threat to SMEs. In Conference Southwest Decision Science Institutes.

[12] Kharraz, A., Arshad, S., Mulliner, C., Robertson, W. K., & Kirda, E. (2016, August). UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware. In USENIX Security Symposium (pp. 757-772).

[13] Mohan, J. C., & Kumar, R. (2017) On the Efficacy of Android Ransomware Detection Techniques: A Survey. International Journal of Pure and Applied Mathematics.

[14] Shakir, H. A., & Jaber, A. N. (2017, November). A Short Review for Ransomware: Pros and Cons. In International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (pp. 401-411). Springer, Cham.

[15] Andronio, N. (2015) Heldroid: Fast and efficient linguistic based ransomware detection, Master's thesis, University of Illinois at Chicago.

[16] Song, S., Kim, B., & Lee, S. (2016). The effective ransomware prevention technique using process monitoring on android platform. Mobile Information Systems, 2016.

[17] Mercaldo, F., Nardone, V., Santone, A., & Visaggio, C. A. (2016, June). Ransomware steals your phone. Formal methods rescue it. In International Conference on Formal Techniques for Distributed Objects, Components, and Systems (pp. 212-221). Springer, Cham.

[18] Cabaj, K., & Mazurczyk, W. (2016). Using software-defined networking for ransomware mitigation: the case of cryptowall. IEEE Network, 30(6), 14-20.

[19] Symantec (2017). Excutive summary and key findings – Ransomware: An overview. Acessed in 20/4/2017.