A Study on- Identifying and Evading Ransomware

(Ransomware)

Mrs.V. Usha Bala, Dr.B.D.C.N.Prasad

[1]*Research Scholar, Rayalaseema University, Kurnool, Andhra Pradesh, India,*

[2]*Professor (Retd.) P.V.P.Siddhartha Institute of Science and Technology, Vijayawada, Andhra Pradesh, India*

Abstract

Ransomware has become widely threatening the user of the internet. It is a malware that damages the victim's system and makes it useless and then demands the user for a ransom which can also be called as crypto currency to revert the system's usage. In this paper we propose analysis and detection of ransomware by which the features of ransomware can be identified and perform operations to protect the user's system. We also propose the methods of protecting the user's system before it's attacked. This increases the business continuity of the organizations thereby increasing the organization's performance.

Keywords:

Ransomware, Unauthorized access, crypto currency, business continuity, malware, ransom, false positives.

I. Introduction

Security can be termed as protection from unwanted harm or unwanted resources. Information security protects the data from unauthorized users or access. It can also be termed as an important asset for any organization which plays a vital role. Security can be tagged as protecting the system and its resources to be in use whilst keeping away from threats and vulnerabilities, which can be achieved by following the principles of security which are confidentiality, integrity and availability that forms the CIA triad.

In earlier days it was difficult to identify ransomware before it enters or attacks the user's system. These attacks would damage the mail servers, databases, expert systems and confidential systems. In this paper we propose the analysis and detection of ransomware which will have major impact on the business continuity.

II. Ransomware

Lately with the extensive usage of the internet, the cyber criminals are rapidly growing targeting the naïve users thru threats and malware to generate a ransom. Currently this ransomware has become the most agonizing malware. Ransomware comprises of two. They are locker ransomware and crypto ransomware. Of them, crypto ransomware is the most familiar type that aims to encrypt users' data and locker ransomware prevents the users from accessing their data by locking the system or device. Both types of ransomware demand a ransom payable via electronic mode for restoring the access of the data and system. Locker ransomware claims fee from the victims in terms of fine for downloading illegal content as per their fake law enforcement notice. Crypto ransomware has a time limit that warns the victims to pay ransom within the given time else the data will be lost forever.

Our main motto is to identify and evade ransomware through mails and also to retrieve the data if it's already attacked the victim's machine. In this paper we suggest techniques to avoid and avoid ransomware attacks through mails.

III. Vulnerability assessment and tools

Vulnerability can be termed as an unsafe or unauthorized access by an intruder into an unprotected or exposed network. Common vulnerabilities are worms, viruses, spyware applications, spam mails etc.

Vulnerability Assessment is the most important technique that is conducted to rate the spontaneous attacks or risks that occur in the system thereby affecting the business continuity of an organization. They can also be termed as Vulnerability Assessment Tools. It plays a vital role in providing security to the organizations' assets. The process of identifying and investigating the vulnerabilities paves a way to mitigate the security issues or to exploit these security issues. Vulnerability assessment has many steps such has

a) Vulnerability analysis
b) Scope of the vulnerability assessment
c) Information gathering
d) Vulnerability identification
e) Information Analysis and
f) Planning

A. *Assessment Tools*

Vulnerability assessment which is nothing but testing can be carried out by best known tools which are called as vulnerability assessment tools. These tools are used to mitigate the identified vulnerabilities such as investigating on unethical access to copyrighted materials, policy violations of the organizations' etc. The red alert issue about the vulnerability assessment is that it warns us about vulnerability before the system is compromised and helps us in avoiding or preventing the attack. These vulnerability assessment tools can also be categorized as proactive security measure of an organization. The major step of the vulnerability assessment is the accurate testing of a system. If overlooked, it might lead to either false positives or false negatives. False positive can be presumed as quick sand where we can't find what we are searching for. False negative can be presumed as black hole where we don't know what we want to search for. False positives can be rated as significance level in testing.

B. *Common Vulnerability Assessment Tools*

- Vulnerabilities are the most crucial part of information systems. An error in configuration or violation of a policy might compromise a network in an organization. These attacks can be for a personal gain or corporate gain.
- Not only the local area networks but also the websites are also more susceptible to attacks where the systems can be exploited either by the insiders or outsiders of an organization.
- Some of the very commonly used vulnerability assessment tools are listed below:
  - Wireshark
  - Nmap
  - Metasploit
  - OpenVAS
  - AirCrack

C. *Limitations of Existing Vulnerability Assessment Tools*

The concept of false positives is the dangerous and horrendous limitation of the existing vulnerability assessment tools. These false positives require lots of testing and study for assessing the nature of the errors occurred, which is very expensive and time taking process. All the identification related information mostly leads to false positives.

D. *Penetration Testing*

- Penetration Testing also called as Pen Test is an attempt to assess a malicious activity or any security breach by exploiting the vulnerabilities.
- It includes the testing of the networks, security applications and processes that are involved in the network.
- Penetration testing is done to improve the performance of the system by testing the system's efficiency.

IV. Methodology

Spreading of ransomware is possible by the following methods:

a. Phishy e-mail messages with malicious file attachments;

b. Software patches that download the threat into the victim's machine whilst working online.

A. *Spreading of Ransomware Attack*

a. Phishing mails: The most common way of spreading Ransomware is thru phishing emails or spam emails. These mails include .exe file or an attachment, which when opened launches ransomware on victim's machine.

b. Exploit kits: these are the compromised websites planned by the attackers for malicious use. These exploit kits searches for vulnerable website visitors to download the ransomware on to their machine.

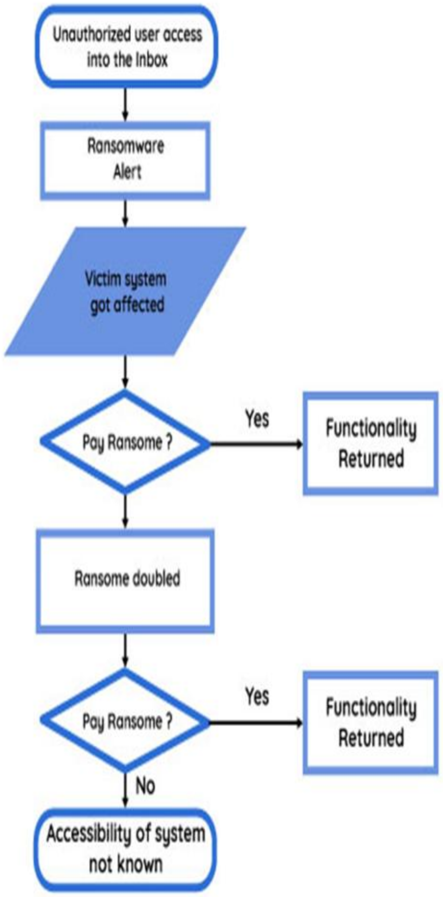

Fig 1: The Ransomware Process[13]

B. Steps in Ransomware Process

There are various steps in the ransomware process which are elucidated below:

a. Malicious code or file infects the victim's machine;

b. User's access to his/her system is lost. Demands for ransom;

c. User's decision to pay ransom or not within the given timeline;

d. Timeline extended;

e. User decides to pay the ransom after the given timeline exceeded as there is no access to the system's functionality;

f. No guarantee for return of the functionality of the system even if the ransom paid or not.

C. Crypto-Ransomware thru website

Ransomware attacks usually originate either thru spurious emails or phishing websites.

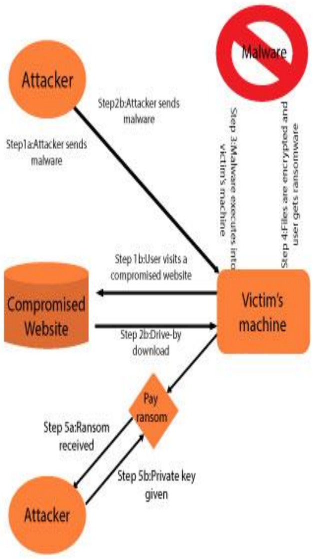
Attacker
Malware
Step2b:Attacker sends malware
Step1a:Attacker sends malware
Step 3:Malware executes into victim's machine
Step 4:Files are encrypted and user gets ransomware
Step 1b:User visits a compromised website
Compromised Website
Victim's machine
Step 2b:Drive-by download
Pay ransom
Step 5a:Ransom received
Step 5b:Private key given
Attacker

Fig 2: The Working Life Cycle of Ransomware Process thru Websites

Steps in Crypto-Ransomware:

- Encrypts the files: Crypto-ransomware encrypts a file using a mathematical algorithm and makes it impossible for the victim to use that file unless ransom is paid.
- Blocks the victim's device: if the victim fails to pay ransom within the given time limit it might lead to loss of data.
- Demands ransom: the demand for the ransom is usually planned thru digital currency or electronic cash.

D. Working of Crypto Ransomware

Crypto ransomware is a program that attacks the users' machine, locks the machine and demands ransom from the victim to revert the functionality of the victim's machine. This attacking of the user's machine is done thru encrypting files stored on the victim's machine. The encryption is a program that shuffles the contents of the file using an encryption key and makes it difficult to read for the user and locks the system. After the encryption is done the crypto ransomware displays a message to the user to pay a ransom within a given time limit. To unlock the victim's machine and to restore the encrypted contents of the file a decryption key is required to rearrange the contents of the file in a readable form. To execute this procedure the attackers or hackers demand a ransom as an exchange for the decryption key for reverting the functionality of the contents of the file. At this juncture the users will be put in pressure such that if the demanded ransom is not paid then either the ransom will be increased or the decryption key used to unlock the functionality of the system will be deleted.

E. Steps in Crypto Ransomware

- Attacking the user's machine through social engineering techniques: in this case the malware that is installed in the affected system launches itself, installs its own keys in the registry of the operating system and takes over the booting functionality of the computer.
- Attacking the user's server: in this case the user's system will be controlled by the third party servers in order to attack the user's system.
- Server and Client: in this case the user's computer and the attacker's computer identify themselves on the network and plan for a handshake. Then the attacker's system generates a pair of cryptographic keys. Of which, one key will be saved in the user's machine and the other will be saved in the attacker's machine.
- Encryption: in this case all the files in the user's machine are encrypted by the ransomware.
- Extraction: This is the final case in which the attackers gets the unauthorized access into the victim's machine and displays a message for ransom payment using the untraceable digital payment schemes within a given time limit.

F. Best Suited Strategies for Ransomware Avoidance

- Backup the entire data in a timely manner;
- Updating the anti-virus regularly;
- Updating the other system files regularly
- Hosting Security awareness programmes for the employees within the organizations and making them aware of these ransomware attacks;
- Implement the revision of security policies regularly to avoid monotony;
- Implementing regular penetration testing techniques;
- Avoiding downloading files or patches from unknown sources; and
- Restrict write permissions on your computer.

V. CONCLUSION AND FUTURE WORK

In order to provide security to the confidential data and information assets vulnerability assessment tools or the penetration testing tools can be deployed. This paper mainly focuses on the types of ransomware attacks and the harm caused by these attacks. This work can be further extended by the implementation of the different types of ransomware attacks.

ACKNOWLEDGMENTS

We would like to thank the staff and management of Rayalaseema University for encouraging and supporting throughout. Our special thanks to our mentors for giving us this opportunity.

REFERENCES

[1] Kim Boatman, "Beware the Rise of Ransomware",http://in.norton.com/yoursecurityresource/detail.jsp?aid=rise_in_ransomware

[2] Carrier, B. "File System Forensic Analysis", Addison-Wesley Professional, (2005).

[3] CISCO, Inc. Ransomware on Steroids: Cryptowall2.0.http://blogs.cisco.com/security/talos/cryptowall-2.

[4] Krebs on Security, "Inside a Reveton RansomwareOperation"http://krebsonsecurity.com/2012/08/inside-a-reveton-ransomware-operation/

[5] Kharraz, W. Robertson, D. Balzarotti, L. Bilge, E. Kirda, "Cutting the gordian knot: A look under the hood of ransomware attacks",12th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2015), July 9-10, 2015, Milan, Italy.

[6] Zeng, Kazemian, Varghese,and Nick "Automatic Test Packet Generation",VOL. 22, NO. 2, APRIL, 2014.

[6] Bowen, B. M., Hershkop, S., Keromytis, A. D., Stolfo, S. J. "Baiting inside attackers using decoy documents", Springer, (2009).

[7] K.Cabaj, P.Gawkowski, K.Grochowski, D. Osojca, "Network activity analysis of CryptoWall ransomware", Przeglad Elektrotechniczny, vol. 91, nr11,2015,ss.201-204,URL:http://pe.org.pl/articles/2015/11/48.pdf.

[8] Dewan P, Kashyap A, Kumaraguru P. Analyzing social and stylometric features to identify spear phishing emails. In: APWG Symposium on Electronic Crime Research (eCrime), Institute of Electrical and Electronics Engineers. 2014. p.1–13. doi:10.1109/ecrime.2014.6963160.

[9] Green B, Prince D, Busby J, Hutchison D. The impact of social engineering on industrial control system security, in: Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or Privacy, ACM, 2015, pp. 23–9. Huber M, Kowalski S, Nohlberg M, Tjoa S. Towards automating social engineering using social networking sites, in: International Conference on Computational Science and Engineering, 2009 (CSE'09), Vol. 3, IEEE, 2009, pp. 117–24.

[10] Knowles W, Baron A, McGarr T. The simulated security assessment ecosystem: does penetration testing need standardisation? Comp Sec 2016;62:296–316. Kontaxis G, Polakis I, Ioannidis S, Markatos EP. Detecting social network profile cloning, in: Pervasive Computing and Communications Workshops (PERCOM Workshops), 2011 IEEE International Conference on, IEEE, 2011, pp. 295–300.

[11] Zhang H, Yao DD, Ramakrishnan N, Zhang Z. Causality reasoning about network events for detecting stealthy malware activities. Comp Sec 2016;58:180–98

[12] Narayanan A, Shmatikov V. De-anonymizing social networks, in: Proceedings of the 30th IEEE Symposium on Security and Privacy (S&P 2009), IEEE Computer Society, 2009, pp. 173–87. Perito D, Castelluccia C, Kaafar MA, Manils P. How unique and traceable are usernames? In: Privacy Enhancing Technologies. Springer; 2011. p. 1–17.

[13] Azad Ali, Ransomware: A research and a personal case of Dealing with this nasty malware (IISIT.org), Volume 14, 2017.

[14] Ali, Murthy, R., & Kohun, F.(2016). Recovering from the nightmare ransomware-How savvy users get hit with viruses and malware: A personal case study: Issues in Information Systems, 17(4),58-69.

[15] Bharadwaj, A.,Avasthi, V.,Sastry, H.,& subrahmanyam, G.V.B.(2016). Ransomware digital extortion: A rising new age threat. Indian Journal of Science and Technology, 9,14.