Strategies: To Defeat Ransomware Attacks

REETA MISHRA
Department of Information Technology
K. J. Institute of engineering & Technology, Savli
Vadodara, Gujarat, India
Email id- reeta.mishra@kjit.org

Abstract— Ransomware is a malware software design in order to extract or collect a huge amount of money from victims, whose system got infected by this attack. It leads to deny access to a user's (or organization's) data, usually by encrypting the data with a secret key. After the data is encrypted, the malware /hacker instruct the user to pay the ransom amount to the hacker (usually in a digital currency such as Bitcoin) in order to receive a decryption key. The amount of ransom requested typically increases, if the hacker determines the data has substantial value. Normally Financial transaction, Medical details and personal identity theft are the soft target for these attack because of the quantity and value of their data. The objective of this paper is to create awareness among less skilled computer users by providing cyber safeguard knowledge and regular updating practice of prevention techniques.

Keywords- Ransomware Attack, Families, Crypto wall, Tesla Crypto, Locker, Prevention method, Bitcoin.

INTRODUCTION

Ransomware Attacks are one of the most notorious malware floating around the internet. These are a piece of software that locks down your files in your or victims PC or smartphone behind an encrypted paywall. In order to overcome this problem victim need to pay ransom to get back there valuable files. But attacker normally prefer to get the ransom payment through bitcoin. . Even after full payment — there's no guarantee to get that decryption key to unlock victim encrypted files.

Bitcoin is digital currency that lets you anonymously buy goods and services. The victims can send bitcoins digitally using a mobile phone app or computer. It's as easy as swiping a credit card. Each bitcoin transaction is on a public log. Names of buyers and sellers are anonymous – only their wallets IDs are exposed. And it allows buyers or sellers do business without easily tracing it back to them. As a result, it's become a popular choice for cybercriminals to choose bitcoin as a form of payment

Ransomware attacks are typically carried out using a Trojan, entering a system through a downloaded file or a vulnerability in a network service [1][2].

I. TOP FAMOUS RANSOMWARE FAMILIES-

A) Locky- The malware gets spread using spam in the form of an email messages containing malicious links and it is disguised as an invoice. When user opens it, the invoice is scrambled, and the victim is instructed to enable macros to read the document. When macros are enabled, Locky Ransomware begins to encrypt a large array of file types using AES encryption. Bitcoin ransom is demanded when encryption is complete.

B) Tesla Crypt – This type of Ransomware, it uses an AES Algorithm to encrypt files. It is typically disseminated via the Angler exploit kit specifically attacking Adobe vulnerabilities. Once vulnerability is exploited, Tesla Crypt installs itself in the Microsoft temp folder. The ransom money is paid in terms of bitcoins.

C) Crypto Ransomware (Data Locker)- prevents access to files or data via encryption.

D) Locker Ransomware (Computer Locker)- Denies access to a computer / device by disabling the user interface.

E) Crypto Wall- After the downfall of Crypto Locker, the Crypto Wall had gained its importance. It including Crypto bit, Crypto Defense, Crypto Wall 2.0 and Crypto Wall 3.0, among others .Crypto Wall is distributed via spam or exploit kits.

II. CAUSES OF ATTACK

1) Traffic distribution system –Improper distribution of traffic through the data transfer from one network to other in case of distribution system.
2) Mal advertisement .or Data breach-Unnecessary advertisement and add on can be the reason.
3) Spam Email-Frequently usage or checking spam email is one important cause of this attack.
4) Auto downloader & botnet- Never allow auto downloader application to get install if in case it happened then turn off/ disconnect the device from internet.
5) Social engineering & self-propagation-Social media is the most important cause of these attacks.

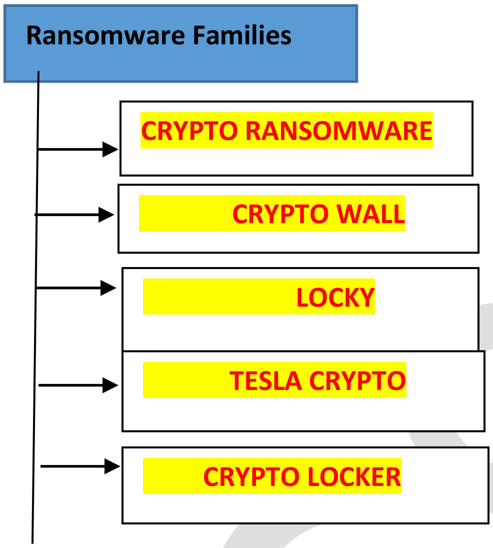

Fig 1. Top Ransomware families

IV.RELATED WORK-In the paper "automatic test packet generation" proposed by Hongyi Zeng, Peyman Kazemian,, George Varghese, ,Fellow, ACM, and Nick McKeown, proposed about the working of the ATPG techniques[5] for testing and debugging networks This method generates a minimum number of dummy nodes or test packets to check every link in the network. Our implementation also augments testing with a simple fault localization scheme also constructed using the header space framework. Thus the liveness of the network is tested.

The work by Nolen Scaife, Henry Carter, Patrick Traynor, Kevin R.B.Butler "Crypto lock (drop it): Stopping Ransomware attacks on user data" explains about the Crypto Drop,[6] an early warning detection system that alerts user during suspicious file activity. It focuses on detecting Ransomware through monitoring the real time change of user data. Indicators have been used to track the suspiciousness. By tracking these, they develop a reputation score, which alerts the user and suspends the suspicious process.

Analysis:- In this paper we main focus on the top 3 Ransomware threads, which is now-a-days at its fame. we try to have a comparative study between these three threads for that we collect 18 affected countries data of April-May 2016 for crypto wall , locky and Tesla as given below-

Country	Crypto wall	Locky	Tesla Crypto
US	43	53	14
FR	2	18	NA
JP	8	8	3.5
SK	NA	5	NA
CA	2.5	4	11
MX	4.5	3	1
CL	NA	2.5	NA
GB	NA	2.5	NA
ZA	NA	1.5	NA
IL	3.5	1.5	NA
TR	NA	NA	13

ES	**5**	**NA**	**2**
IT	**3**	**NA**	**3.5**
CO	**2**	**NA**	**NA**
KR	**NA**	**NA**	**39**
TR	**7**	**NA**	**NA**
IN	**NA**	**NA**	**2**
DE	**NA**	**NA**	**2**

Table 1. Data to measure effect of this attack

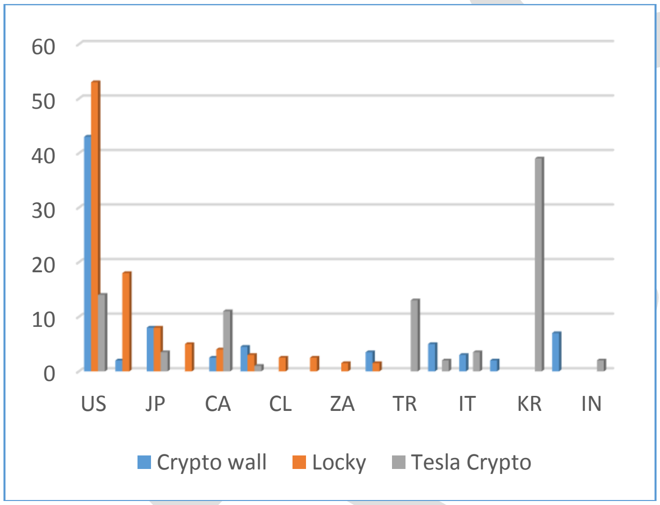

Fig 3. Attack effect show through graph

In case of crypto wall top two most hit countries are US & JP

In case of locky top two most hit countries are US & FR

In case of Tesla crypto top two most hit countries are KR **& US**

V. IMPACT OF ATTACK

1) Shutdown Cost: Organization may be forced to shut down systems to deal with the infection. Customers may be affected as target not achieved on time or may have financial loss, which can't be repay. It surely damage organization goodwill in market.

2) Data or Information loss: Loss of data due to files being encrypted and stolen can have a huge impact on businesses. The loss of company records, personally identifiable information, or intellectual property can significantly impact the organization. On other side those personal data can be mishandle by attacker. The aim behind the attack may threaten to publish stolen data online and attempt to extort more money from victim.

3) Financial Cost: Companies may have to pay for the incident response and other security related solutions in response to ransomware. Organizations could also be hit with large legal bills if customers are affected. Fines and other penalties may also apply.

4) Loss of life: In the case of a hospital or other medical organization, patients' lives may put at risk as essential medical equipment may be affected. Patient record including medical history may be inaccessible, leading to delays in treatment or even incorrect medication.

VI. PREVENTION FROM RANSOMWARE ATTACK

1. Install a good & license antivirus: First tip is to install a top-notch antivirus that often scans your online activity and applications in your PC.

2. Secure back up of your data: We need to create secure backups of data on a regular basis to USBs or an external hard drive and always remember to disconnect your external memory devices from computer after backing up otherwise they will also infect with ransomware. We can also use a Cloud storage with high-level encryption and multiple-factor authentication features to store confidential files.

3. Download files from trusted sources: Always try to download files from trusted sources or websites. Be alert and check file description before downloading from torrents. Try to avoid websites that have too many pop ups.

4. Scan email attachments before download: So always double-check email attachments before downloading even if it is came from your relatives/friends or office. Also never open email attachments from strangers. And check thoroughly email details like sender name and email address, company logo, spelling — because potential scammers forge emails that looks like coming from official source. And in Gmail make sure you scan attachments before open.

5. Update operating system and other applications: Using Windows or Android always update your operating system and other applications.

6. Browser Protection- Apart from antivirus it is also important to use firewall or other secure measure to provide protection to the browser

7. Use a sandboxing solution

8. Block risky file extension- End user must avoid from opening risky files extension with .wsf, .chm, .jscript,. vbscript etc.

9 Use URL filtering-It means block the access of C&C Server so the system get protected.

10. Use HTTPS filters-Instead of using simple HTTP it is recommended to use a secure HTTPS filters

11. Use HIPS or other signature less technologies -User must use host HOST INTRUSION PREVENTION SERVICE, these will help the user to protect from attack.

12. Encrypt data-As security point the user must keep all his confidential data in encrypted form.

13. Use security analysis tool and whitelisting solution-User must use whitelisted (trustful) solution and security tool as well as have a periodic check on the functioning of system.

VII. CONCLUSION & FUTURE SCOPE- In this complete paper try to explain overview, causes of ransomware attack, to show the effect of these attack through comparative study, its impact and the preventive measure for those people who are not much aware of these type of computer related attack threads .In continuation of this paper in my next paper , basically focus on the proposed model in order to fetch ransomware code and eliminated it without delay by using multilevel filtration techniques.

REFERENCES:

[1] G. Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. *(references)*

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[3] I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[4] K. Elissa, “Title of paper if known,” unpublished.

[5] R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.

[6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].