Mitigating Ransomware Attacks

K.Jaisharma, Suvvala Manoj, K. Manideep, Manoj Kumar Reddy

Abstract: ***In the recent years the attack namely, ransomware have been spreading very rapidly which could concentrated on from home user to the large kind of corporations and organisations. In the recent days many approaches have been found to survive from the ransomware attacks even though there are still many attacks which are being done by the organisational employees. Our approach is different from those kind of approaches which is mainly focused on the mitigating the attacks instead of removing those kind of attacks which is not surely easy.***

Keywords: Cyber Attacks, Ransomware, Unauthorized Users, Wannacry.

I. INTRODUCTION

The term ransomware is nothing but the software which is used to attack on the personalized or official computers and its organisations which could make huge losses and unauthorized gains to the victim computer or its organisation. The ransomware is subset of malware where the data pf the victim to this attack is completely locked.

1.1 Ransomeware in Cyber Security

The term ransomware is nothing but the software which is used to attack on the personalized or official computers and its organisations which could make huge losses and unauthorized gains to the victim computer or its organisation. The ransomware is subset of malware where the data pf the victim to this attack is completely locked. It is used to encrypt important documents or files within a system (crypto ransomware) or simply lock the original user out of the system (locker ransomware). Unlike the other cyber-attacks, in this form of attack the user is notified of the attack.

Ransomware spreads easily when it encounters unpatched or outdated software. In the recent days we have seen the one of the biggest cyber-attack which has occurred in the year of 2017 where the ransomware played a major role in the attack. The attack that has done by the ransomware software namely by the wannacry ransomware crypto worm.

1.2 Victims of attack

1. Targeted computers running the Microsoft windows operating system by encrypting data and demanding ransom payments in the bitcoin cryptocurrency.
2. Ransomware have been attacked on the national security agency of united states of America.
3. WannaCry also made lots of damages and loses to the organisations which rely on huge data.

1.3 Effects of ransomware in current world

1. According to the data given by the international society's online trust alliance globally the losses from ransomware rose by 60% last year to $8 billion.
2. Earlier in this year, services in the U.S cites of Baltimore and Maryland were paralysed when a ransomware attack locked up computer networks.

1.4 Recovery of this attack by major organisational workers

The attack was stopped within a few days of its discovery due to emergency patches released by Microsoft, and the discovery of a kill switch that prevented infected computers from spreading WannaCry further. Microsoft released out-of-band security updates for end of life products windows XP, Windows Server 2003 and Windows 8.

Researcher Marcus Hutchins accidentally discovered the kill switch domain hardcoded in the malware. Registering a domain name for a DNS sinkhole stopped the attack spreading as a worm, because the ransomware only encrypted the computer's files if it was unable to connect to that domain.

II. RANSOMEWARE PROCESS

The ransomware process is discussed in the following:

2. Tools

Table.1 has tools name used for security.

Revised Manuscript Received on July 13, 2019.

K.Jaisharma, Assistant Professor, Saveetha School of Engineering, SIMATS, Chennai.

Suvvala Manoj, UG Student, Saveetha School of Engineering, SIMATS, Chennai.

K. Manideep, UG Student, Saveetha School of Engineering, SIMATS, Chennai.

Manoj Kumar Reddy, UG Student, Saveetha School of Engineering, SIMATS, Chennai

Table.1 Security Tools

Tools Name	Full Form	Year of publish	Applicable of OS	Usage
GNUPG	Gnu Privacy Guard	1999	Linux, CentOS	using GPG keys to send encrypted messages, combination of public key and symmentric key
OWASP	Open Web Application Security Project	2001	web vulnerability	use to develop secure software
Truecrypt	Open Source Security	2014	windows, macOS, Linux	used for on the fly disk encryption
OSSEC	Open Source Security	2019	Linux, OpenBSD	helps customers to meet standard and integrate security
OSSIM	Open Source Security Information Management	2010	OpenVAS	used for monitoring health and security of network/hosts

2.1 Existing Work in Ransomeware

To survive from the ransomware attacks in the existing scenario following are the basic steps that have been using by the organisational workers to resolve the tragedies of the attacks done by the ransomware.

1. Recovering of the data or the files which have been hacked using backup strategies.
2. Restoring of the data and other hardware devices in the whole system to minimize the damages and infected files.
3. Windows Script Host is a frequent tool of ransomware infection. Activation only for users who need it is highly recommended.
4. To avoid suspicious files and run programs from AppData/LocalAppData because it can protect the system against various malware mutations.
5. Regular training of the employees is needed to train them in the fields of cyber security and other security issues.
6. To do the routine backups of files on the workstations and then to disconnect the backup device from the operating system after backing up. This will make the users to get survived from the ransomware attacks by minimizing the damages of those kind of affects.
7. Disabling of the remote desktop protocol where the most of the hackers targeted.

2.2 Regular Software Updates

A cyber-attack occurs when a software patch hasn't been updated. For a malware like Ransomware, it is an open gateway for digital snoopers to make their way. When hackers come across an old patch, it isn't a strenuous task for them to exploit vulnerabilities and do their job. So, we should update the software and its applications regularly to get survived from the ransomware attacks.

2.3 Backups and Recovering Techniques

Each and every single bit of data should be backed up. Recently updated document must be sent to our associates to be saved in the google cloud or email cloud and other kind of storages like USB, hard disk and drives etc. Backup will also provide the workflow easily.

2.4 Detection of Malicious Accounts

Since the ransomware has the techniques to attack the users by entering into the threatening accounts within the organisation detection of those accounts help us to survive those kinds of cyber-attacks like ransomware. Detection of the malicious accounts within the organisation should be removed to sort out the problems that occurred from the cyber-attacks like ransomware.

2.5 Checking Up With Anti Viruses

As we know that internet is open for all so that everybody can use it. It will leads to some vulnerabilities to the organisation. To avoid those kind of vulnerabilities we need to activate our anti-virus or anti malware systems to be installed in our system to survive from the attacks like ransomware.

III. PROPOSED WORK TO SORT OUT RANSOMWARE ATTACKS

1. Usage of block chain technology to avoid attacks in terms of financial transactions and other type works related to multiple organisation.
2. Usage of cryptocurrency like bitcoin and other type currencies which would reduce the loss of these time of attacks. Recently, Facebook also introduced cryptocurrency for all its deals and transactions.

3. Work as well as the network segmentation is very important to get rid off the ransomware attacks since it will provide the organisation with good communication between employees in segments wise as well as network wise.
4. Improving of strong password policies which can't be revealed anywhere within the organization as well as the outside of the organisation.
5. Disabling of some important web services and other websites to avoid those kind of attacks like ransomware.

Windows Defender - Once the threats are found then there is no need of Windows real-time protection analysing, and blocking.

Windows Firewall – Even though it may identify a testing environment, some malicious codes are demonstrated when we activate the firewall in the system or computer.

Windows Update – New updates may modify our configuration and may give an additional protection to the system.

Address Space Layout Randomization - A feature that partially randomizes address space from buffer overflow attacks.

No execute technology - another protection features for specifying areas of memory that cannot be used for execution.

IV. IMPLEMENTATION AND RESULTS

The implementation of proposed solution is typically difficult but by ensuring the above solutions to survive from the ransomware attack we can able implement to get survived from the tremendous cyber-attacks.

Implementation of those suggestions in the real time scenario is as follows;

1. Windows defender.
2. Windows Firewall.
3. Windows update
4. System backup rapidly.

After implementing those kinds of solutions we could see the following drastic changes like how the organisations have been survived from the cyber-attacks like ransomware.

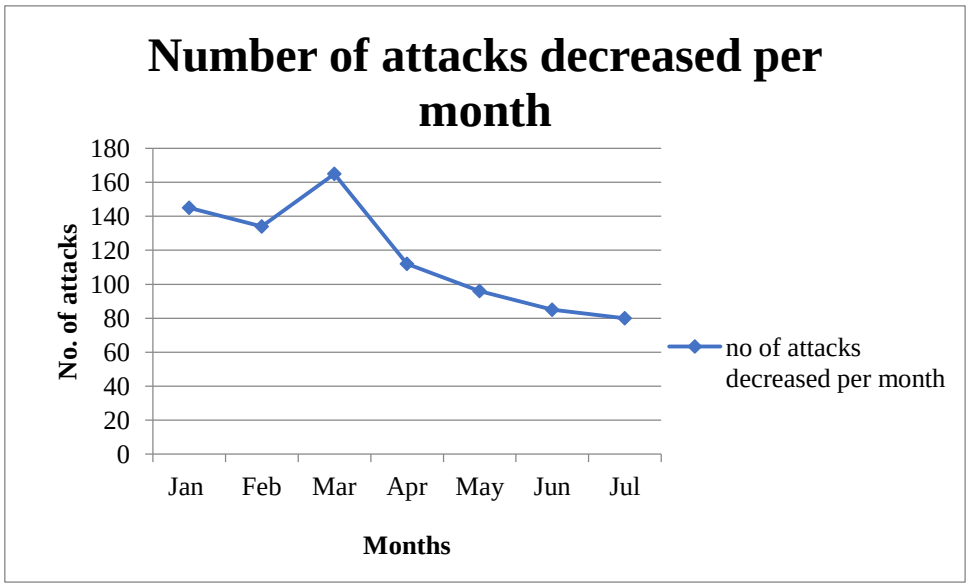

Fig.1 Attacks being decreased per year

V. CONCLUSION

At first we have seen an existing system to avoid ransomware attacks which have not given proper and expected results to survive from the ransomware attacks. To come out of those regressions we have proposed a some solutions which could have worked very progressively that we can observe from the graph that we have incorporated above. Hence, the cyber-attacks like ransomware can be resolved using above techniques which we have proposed to sort out the world cyber crisis where even from small organisations to major organisations facing in recent days.

REFERENCES

1. Europol. Internet organised crime threat assessment 2016 (IOCTA); September 2016. URL: https://www.europol.europa.eu/content/internet-organised- crime-threat- assessment- iocta- 2016 .
2. Savage K, Coogan P, Lau H. The evolution of ransomware. Symantec security response; August 2015. URL: http://www.symantec.com/content/en/us/ enterprise/media/security _ response/whitepapers/the- evolution- of- ransomware.pdf .
3. McAfee Labs. Meet 'Tox': ransomware for the rest of Us; May 2015. URL https://blogs.mcafee.com/mcafee- labs/meet- tox- ransomware-for- the- rest- of- us/ .
4. Symantec. Internet security threat report; April 2015. URL https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932 _ GA- internet- security- threat-report-volume-20-2015-social _ v2.pdf .
5. Kreutz D, Ramos FV, Verissimo P, Rothenberg C, Azodolmolky S, Uhlig S . Software-defined networking: a comprehensive survey. Proc IEEE January 2015;103(1):14–76 .
6. Mehdi SA, Khalid J, Khayam SA . Revisiting traffic anomaly detection using software defined networking. In: Proc. of the 14th international conference on recent advances in intrusion detection (RAID 2011); 2011. p. 161–80 .

7. Tofilski A, Couvillon M, Evison S, Helantera H, Robinson E, Ratnieks F. Preemptive defensive self-sacrifice by ant workers. Am Nat 11.2008,;172(5):E239–43.
8. Mazurczyk W, Rzeszutko E . Security - a perpetual war: lessons from nature. IEEE IT Prof 2015;17(January/February 1):16–22 .
9. Gu G, Perdisci R, Zhang J, Lee W . Botminer: clustering analysis of network traffic for protocol- and structure-independent botnet detection. In: Pro- ceedings of the 17th USENIX security symposium; 2008 .
10. Wurzinger P, Bilge L, Holz T, Goebel J, Kruegel C, Kirda E. Automatically generating models for botnet detection. In: Backes M, Ning P, editors. ESORICS 2009. LNCS, 5789. Heidelberg: Springer; 2009. p. 232–49 .
11. Bailey M, Oberheide J, Andersen J, Mao ZM , Jahanian F, Nazario J. Automated classification and analysis of internet malware. In: Kruegel C, Lippmann R, Clark A, editors. RAID 2007. LNCS, 4637; 2007. p. 178–97.
12. Bayer U, Comparetti PM, Hlauschek C, KruegelC, KirdaE. Scalable, behavior-based malware clustering. Network and distributed system system security symposium; 2009 .
13. Jacob G, Hund R, Kruegel C, Holz T. Jackstraws: picking command and control connections from bot traffic. 20th USENIX security symposium; 2011 .
14. Idika N, Mathur AP. A survey of malware detection techniques. Purdue University; 2007. Technical Report .
15. Rieck K, Schwenk G, Limmer T, Holz T, Laskov P, Botzilla. Detecting the phoning home of malicious software. In: Proceedings of the 25th ACM symposium on applied computing (SAC), March; 2010 .
16. Rossow C, Dietrich CJ. ProVeX: detecting botnets with encrypted command and control channels. In: Proc. of 10th international conference, DIMVA 2013, July 18–19; 2013. p. 21–40 .
17. Celik ZB, Walls R, McDaniel P, Swami A. Malware traffic detection using tamper resistant features. Military communications conference (MILCOM), October Tampa, FL, USA; 2015 .
18. Andronio N. Heldroid: fast and efficient linguistic-based ransomware detection M.Sc. thesis. University of Illinois at Chicago; 2015 .
19. Kharraz A, Robertson W, Balzarotti D, Bilge L, Kirda E. 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 Milan, Italy; 2015 .
20. Scaife PTN, Carter H, Butler KR. Cryptolock (and drop it): stopping ransomware attacks on user data. In: 2016 IEEE 36th international conference on distributed computing systems; 2016. p. 303–12.