IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 8, Issue 6, June 2020

A Survey on Impact of Ransomware, Evolution and Prevention Techniques

Rashmi M.K[1], Dr. Smithamol M B[2]

Student, Dept of Computer Science, LBS College of Engineering, Kasaragod, Kerala, India[1]

HOD, Dept of Computer Science, LBS College of Engineering, Kasaragod, Kerala, India[2]

Abstract: In the current era of technology, there has been an exponential increase in the cyber-attack. One of the most dangerous attacks in this cyber-attack is the ransomware attack which not only corrupt and encrypts the data but also steals the information from the system. 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. 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. . In this paper, discuss the origin, evolution, and prevention techniques of ransomware. The various families of ransomware, their attacks, and prevention from these attacks have been presented.

Keywords: Ransomware, static, dynamic, information security

I. INTRODUCTION

Ransomware is a kind of malware that encrypts files in a victim's computer and requires payment before restoration. It has become a very serious cyber threat. NO MORE RANSOM is a project formed to fight against ransomware attacks. NO MORE RANSOM provides free recovery tools on its website. The tools provided are known to have recovered 28,000 infected devices thus far, but crypto viruses are not in recoverable list.

The basic idea of ransomware was presented in the form of a crypto virus in 1995. They encrypt victims' files and require user's payment to decrypt them. Because they utilize public key cryptography, the key for recovery cannot be found in the footprint of the ransomware on the victim's system. Therefore, once infected, the system cannot be recovered without paying for restoration. Various methods to deal this threat have been developed by antivirus researchers and experts in network security.

Fig1. Working of ransomware

1. Target user receive an email, contains URL link, which looks to be sent from legitimate sender, Example: boss.
2. The user is guided to the link of a website that appears to be authentic.
3. When the web page is loaded, the server exploits the kit which starts interacting with the victim system.
4. When a version is approved, the kit tries to abuse the vulnerability.
5. From this shield, it multiplies the processes, including backup copy, to remove available shadows on the victim machine and formulate different ones to cover in.
6. The binary practices a PowerShell that is executable to propagate the copies of itself throughout the file system.
7. The powershell.exe process generates three number of copies from the originating malware binary, first in the AppData directory, next in the Start directory, and then finally in the C directory.
8. When this process encrypts the victim's files, the malware forwards the encrypted key and rest of the host-specific data to the control server.
9. The server then forwards a note to the victim demanding ransomware.

IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 8, Issue 6, June 2020

II. TYPES OF RANSOMWARE

There are three main types of ransomware. The severity of attacks varies for each of them. Scareware poses the least security threat. These types of ransomware merely post a pop-up on the screen informing the user that the computer has been locked. A ransom is demanded. If the user checks the computer, no files or data is encrypted. The message posted is a hoax. The second type of ransomware is locker. This malware locks up the system and asks for a ransom. It denies the user access to certain programs or to the whole computer till ransom is paid. The severity of this ransomware is medium.
The third type and highly severe ransomware is crypto- ransomware. These malware programs encrypt user data. Hence user is not able to access any of his files till ransom is paid. In certain cases, the ransom amount is doubled after a specific period of time if the ransom is not paid.

A. *Crypto Wall*
Crypto Wall came into picture since November 2013, it mainly encrypts the file and filenames on system and requires ransom to decrypt it. Crypto Wall is spread by mail in form of an attached zip file consisting of a script file and an exploit kit. It starts with injecting itself into explorer.exe and creates a new instance of the process and copying it to %APPDATA% and also create a registry value run key in the local user registry root path. Crypto Wall also deletes the shadow copies from the system and also disables further shadow copies.

B. *CTB Locker*
CTB Locker was found in 2014. CTB is an acronym of Curve Tor Bitcoin where curve refers to the use of Elliptic Curve Cryptography. In this Tor network is used for hiding the command and control server, but it is not needed initially for infection as the encryption of the files can be done without internet connection also. Encryption used is the combination of AES, SHA256 and curve25519. Along with the encryption it also disables the volume Shadow copies feature in Windows.

C. *Locky*
Locky is the youngest additions to the ransomware family. It appeared in February 2016 for the first time and on the first day of its existence it affected 100,000 systems [9]. Programs are distributed by the spam emails containing an attachment of Microsoft Office document which contains the macro that downloads the malicious program. It also deletes the shadow volume copies and can also encrypt external hard drives and database files.

D. *WannaCry*
WannaCry is the most recent and the largest ransomware attack to date. It has affected more than 125,000 organizations in over 150 countries. The ransomware is also known as WannaCry or WanaCryptor and it affected the windows machine through the windows exploit known as EternalBlue which was an unpatched Microsoft Windows Vulnerability.

E. *Petya*
Petya ransomware was first witnessed in March 2016 and again attacked with the new variant in June 2017.It also uses the same vulnerability that is used by the WannaCry ransomware .The first infection began across Europe, mainly in Ukraine. Other than this another 64 countries also got affected including Brazil, Germany, Russia, India and United States.

III. THE IMPACT AND PREVENTION TECHNIQUES OF RANSOMWARE

Ransomware is a malware that breaches the security of the system by using malicious codes. It encrypts the information and available data before noticing it. It hostage the data to earn money. Traditional vaccination system does not cure the infected system without obtaining information on ransomware. Since the data is encrypted hence cannot be recovered without encryption key. Users can avoid the infections of ransomware by updating vaccination system from time to time. However, this method has limited efficacy. This approach cannot trace modified ransomware with new pattern. Hence an active instead of a passive prevention method is urgently required. Analysed some of ransomware attacks and the suggested action against ransomware attack. Also ransomware removal and preventional methodology.

As rest of the nations India is less influenced by the WannaCry ransomware. The principle reason for this is, India is right now less digitalized when contrasted with different nations. This doesn't imply that India isn't influenced in any way, many organizations and people are influenced in India too. The risk from ransomware is real and the risk is big. It is clear that ransomware is a big threat and effective measure and technique must be developed for prevention.

IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

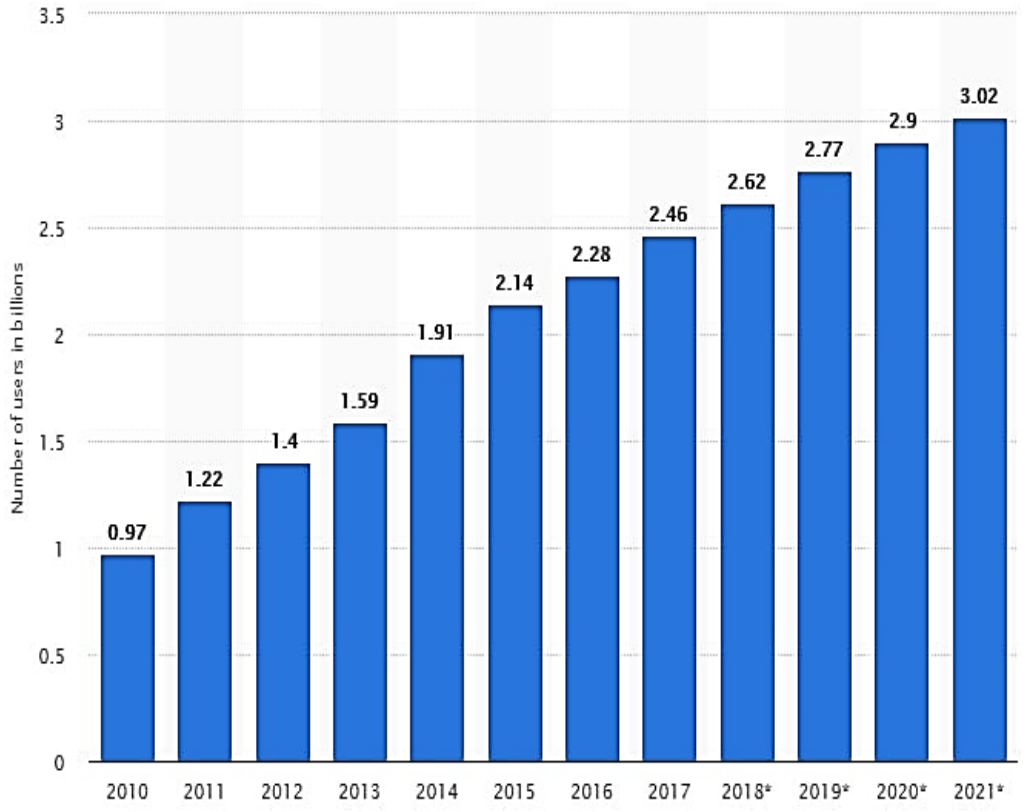
International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 8, Issue 6, June 2020

The former method is operated within an analysis sandbox, and the latter method can be avoided if the ransomware uses its own encrypting functions. To protect users, a detection method should be able to detect ransomware in the user's real-time environment and make it difficult for the ransomware to avoid detection.

Another prevention method, it is aimed to find solutions to these problems and to minimize possible harm. In order to do so, an area called safezone has been created and prevented from being replaced by other software by moving important documents to this zone. The software keeps all the files in a single file by compressing them for creating a safe area.

Another prevention method includes a DGA-detector, and a novel monitoring framework called CM&CB to detect and prevent damage by the most dangerous ransomware. The key observation for the success of this approach is that the operation of HSRs relies on a key-exchange step. By monitoring and blocking this step, the whole operation of the HSR is thwarted.



Finally ransomware effected badly in 2019 with three prominent ransomware targeting Indian businesses. The global cyber security firm Kaspersky security identified three families as the most notorious such as Ryuk, Purga and Stop.

IV. DISCUSSION

From the survey, I identified some of the gaps, In that first one is there is no detection program for WYSIWYG. Only non-WYSIWYG files are to be protected from ransomware. And all prevention mechanisms are to be done within a system so that it is easier to a attacker to attack the system. Also we can Extend the Connection Monitor & Connection Breaker framework by adding another HSR features to detect new sophisticated HSR's which they will not detect with only key exchange. Till today there is only static protection and removal mechanisms are implemented against ransomware, No dynamic methods are implemented to protect from ransomware attack.

V. FUTURE WORK

In this paper, I review about Ransomware and their types. Ransomware is an active attack. Apart from security mechanisms, prevention and awareness may result in stopping the execution of the ransomware. In future, we can focus on developing a security mechanism which prevents the ransomware attacks dynamically.

IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 8, Issue 6, June 2020

VI. CONCLUSION

This survey focused on the present protection mechanisms of ransomware. I observed that all the protection mechanisms are of static. And there is no dynamic protection mechanism to protect the system from ransomware. Now a day's windows and Kaspersky introduced some anti ransomware software's. But that software's will reside inside the system, so attacker can access that software's too. We can implement a new method using Deterministic random bit generator. And it will dynamically protect the system from ransomware.

REFERENCES

[1] J. Wyke, A. Ajjan, "The current state of ransomware", December 2015, SophosLabs Technical Paper.
[2] K.Savage, P.Coogon, H.Lau,"Security response: The evolution of ransomware", White Paper, 6th August 2015, Syman- tec.
[3] A special report "Ransomware and businesses 2016",2016, Symantec.
[4] [Online] "PHP ransomware attacks blogs, websites, content managers and more…" https://nakedsecurity.sophos.com/2016/03/02/php-ransomware-attacks-blogs-websites-content-managers-and- more/ [last accessed 2018/04/16].
[5] K. Richards, "Recent ransomware attacks: data shows 50% growth in 2016", 2016, SecuritySearch.
[6] J. Crowe, "Ransomware growth by the numbers: ransomware statistics 2017", June 2017, Barkley.
[7] J. Crowe, "Ransomware by the numbers: must-know ransom- ware statistics 2016".
[8] "White paper: ransomware. The virus plumes new depths."9th August 2017, Ethical IT.
[9] "Understanding the depth of theglobal ransomware problem", August 2016, Osterman Research Survey Report.
[10] N. Scaife, H. Carter, P. Traynor, K. Butler, "CryptoLock (and Drop it): stopping ransomware attacks on user data", 2016, IEEE 36th International Conference on Distributed Computing Systems, pp. 303-312.
[11] "Five things you need to know about CryptoLocker", White Paper, Zscaler, 2017.
[12] G. O' Gorman, G. McDonald, "Ransomware: a growing me- nace", White Paper, 8th November 2012, Symantec.
[13] "Ransomware and businesses 2016", White Paper, August 2016, Symantec.
[14] S. Mehmood, "Enterprise survival guide for ransomware at- tacks", White Paper, 30thApril 2016, SANS Institute Reading Room.
[15] "Ransomware and phishing: how to avoid falling victim to these threats", White Paper,19th January 2017,Barracuda.
[16] R. S. Sajjan, V. R. Ghorpade, "Ransomware attacks: radical menace for cloud computing", 2017, International Conference on Wireless Communications, Signal Processing and Net- working (WiSPNET),pp. 1640-1646.
[17] C. L.Gande, R. G. Gutierrez, "Give us this day our daily ran- somware", 2017, IEEE 37th Central America and Panama Convention (CONCAPAN XXXVll). pp. 1-6.
[18] D.Caivano, G.Canfora, A.Cocomazzi, A.Pirozzi, C. A.Visaggio, "Ransomware at X-Rays", 2017, IEEE Interna- tional Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 348-353.
[19] Q. Chen, R. A. Bridges, "Automated behavioral analysis of malware: A case study of WannaCryransomware", 2017,16th IEEE International Conference on Machine Learning and Applications (ICMLA), pp. 454-460.
[20] H. Kim, D. Yoo, J. Kang, Y.Yeom "Dynamic ransomware protection using deterministic random bit generator", 2017, IEEE Conference on Application, Information and Network Security .