South Asian Journal of Research in Engineering Science and Technology
Volume 4, Issue **3**, **March 2019**

www.sajrest.com
IXplore SAJREST ⓒ2019 ISSN 2455-9261
pp. **21—28**

AUTOMATIC DETECTION AND ANALYSIS OF RANSOMWARE ATTACKS

M.RAJAKUMARAN[1], M.E,(Ph.D), Assistant Prof, Dept of Computer Science and engineering
K.DESIGA[2], Final year B.E Dept of Computer Science and engineering
R.MAHALAKSHMI[3], Final year B.E.Dept of Computer Science and engineering
M.LAVANYA[4], Final year B.E,Dept of Computer Science and engineering
[1234]E.G.S. PILLAY ENGINEERING COLLEGE (AUTONOMOUS), NAGAPATTINAM.

1.ABSTRACT

Ransomware attacks have become a global incidence, with the primary aim of making monetary gains through illicit means. The attack started through e-mails and has expanded through spamming and phishing. Ransomware encrypts targets' files and display notifications, requesting for payment before the data can be unlocked. Ransom demand is usually in form of virtual currency, bitcoin, because it is difficult to track. In this paper, we give a brief overview of the current trend, challenges, and research progress in the bid to finding lasting solutions to the menace of ransomware that currently challenge computer and network security, and data privacy.

Keywords: Master boot record, The Onion Router, Invisible Internet Project, Curve Tor Bit coin, Exploit Kits

2.INTRODUCTION

Ransomware is a particular class of malwares that demands payment in exchange for a stolen functionality, mostly data. This class of malware has been identified as a major threat to computer and network security across the globe. Ransom ware installs covertly on a victim's device to either mount the crypto viral extortion attack from crypto virology that holds the victim's data hostage, or the crypto virology leak ware attack that threatens to publish the victim's data. The real target of this form of attack is critical data that are very important to individuals and enterprises alike. In fact, the attack has spread to mobile

devices and mobile malware detection approaches are not so effective because of the subtle nature of the malicious programs. Therefore, billions of mobile device users are susceptible to this attack. Most of the ransom ware variants depend on file encryption as a strategy for extortion. Data stored on victim's device are encrypted while the hacker demands for ransom before the files can be decrypted. Ransom ware may encrypt the Computer's Master File Table (MFT) or entire hard drive. It is a denial-of-access attack that prevents computer users from accessing files since it is intractable to decrypt the files without the decryption key. Ransom ware attacks are typically carried out using a Trojan that has a payload disguised as a legitimate file. Although advanced encryption algorithms are useful for effective protection of vital enterprise data, they have become tools for malicious attacks in the hand of cyber-criminals. Data protection is, therefore, under serious threat as hackers continue to utilize enhanced algorithms in ransom ware attacks.

3.LITERATURE SURVEY

3.3.1 Hitler Ransomware It claims to have encrypted the victim's files, but in fact simply deletes file extensions for anything found in certain directories. After an hour it crashes the PC and, on reboot, deletes the files. The payment demanded is a cash code for E25 Euro Vodafone Card. Text found in the code suggests it originates in Germany.

3.3.2 Fake Windows 10 Lock Screen It tells the user that their license has expired, turns out to have the decryption key buried in the code. Researchers from Symantec discovered that, while the criminals had gone to considerable effort to set up fake tech support websites for the scam, the phone number they gave out for victims to call was never answered and was soon disconnected. On reverse engineering the code, the researchers found the decryption key (8716098676542789) plainly visible.

3.3.3 'Power Ware' and 'Bart'

They have been cracked by security researchers who found flaws in the malware. A team at Palo Alto Networks found that PowerWare, while trying to emulate the notorious Locky strain, had weak encryption and hardcoded keys.

The company published a decryption tool and AVG created a decryptor for Bart due to the

malware's poor encryption algorithm.

3.3.4 Chimera Ransom ware The decryption keys of the Chimera ransom ware have also been published by a rival ransom ware gang known as Janus. Janus aimed at ensuring there are enough victims available for its own malware, dubbed Mischa, which also uses some of the Chimera source code. The Chimera malware was never especially widespread, being aimed mainly at smaller German businesses.

But it was notable for the threat from its creators that they would publish victims' private documents and login credentials if they didn't pay up. Security firms had yet to write a decryptor using the published keys. Victims are advised to keep the encrypted versions of their files safe for later decryption once the relevant tool is available.

4. EXISTING PROCESS

Since the 50s, the world has seen the merits and the wonders of the Internet and World Wide Web (WWW). Every user today is now being connected to it at an immensely quick pace. The amount of data is now exceeding zettabytes (270 bytes) since last year, and the concerns for its safety are now taking the shape of a major problem. Pernicious content and corrupt programs have been attacking and infecting various devices around the world, and the efforts for their prevention and eradication have also gained pace simultaneously. The software code written especially toward causing damage or stealing information becomes what is known as per-ware (pernicious software) or per-ware in short.

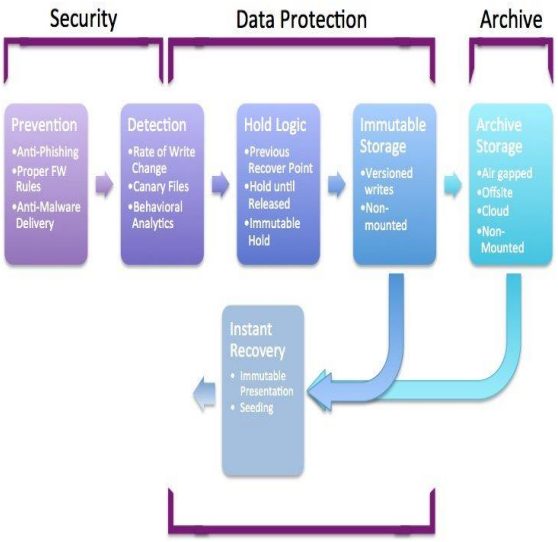
5. PROPOSED METHODOLOGY

We provide a brief overview of the current trend, challenges, and research progress in the bid to finding lasting solutions to the menace of ransom ware that currently challenge computer and network security, and data privacy Ransom ware are now delivered as Word macros and Power Shell scripts. ‘Petya’ encrypted hard drive master boot record (MBR), as well as files, rendering computers completely unusable. The MBR is replaced with the malware’s own boot loader so that the ransom note can be displayed. The most common method of delivering ransom ware is the phishing attack and it is not easily recoverable.

6. DETECTION TECHNIQUE:

Now a day‟s healthcare, government, university, Manufacturing, technology, and banking sector etc. like everywhere security of data is the main concern [6]. Everyone is maintaining our data in digital form like on a cloud or on a hard disk. So cyber security is required to secure data from an intruder. The present portion deals with the experiment made by the researcher in the area of the variant of ransomware and its detection techniques. Chris Moore 2016, in which author creates a honeypot to identify ransomware activity. There are two select point options in which Microsoft File Server Resource manager using File Screening service and for controlling the security logs of window EventSentry are used. The research developed a staged response to attack to the system along with thresholds when there were triggered. There were no agreements that malware would attempt to occupy these areas and the disadvantage of honeypot technique is restricted system view. In which a message from attack free honeypot is not specifying that this will not targeted other area.

7.ARCHITECTURE:



8. IMPLEMENTATION RESULTS

Configuration Module. The configuration module is the basic setup to be applied when the proposed technique detects a ransomware. In this paper, default setting values that are information about the process or application installed by default on the Android platform are saved in a database. The foremost role of the configuration module is to specify the location of the files needed to be protected from the attacks of the ransomware. An area of these important files is called priority protection area (hereinafter PPA).

If the proposed technique is run correctly, it will collect the information of PPA, register them to the watch list table for the monitoring module, and protect the corresponding files in real time. The second role is to register user's handling for the suspected process detected by the monitoring module into the database and maintain the handling. If the user finally determines the process as a ransomware, it stores the information of the corresponding process. It will automatically detect and delete the process depending on the user's feedback. If the user determines the process as normal, it records the information of the process and forces the system to maintain the process without terminating the process even if the process is redetected.

Monitoring Module. The monitoring module is responsible for detecting the ransom ware by monitoring the PPA area and the process. The monitoring module is largely composed of two modules (file monitoring and process monitoring) based on the roles.

(i) File Monitoring Module. It continuously monitors the status of the input/output events such as reading, writing, copying, and deleting of a file belonging to a PPA set in the configuration module and detects the attacks of the ransomware. Algorithm 2 shows the operation flow of the file monitoring module proposed in this paper.

(ii) Process Monitoring Module. It continuously monitors Processor share by Process, Memory usage, I/O count, Storage I/O count, and so forth and detects the ransomware. Algorithm shows the operation flow of the process monitoring module proposed in this paper. Upon detecting the suspected process, it also handles malicious or exceptional processes in the database applied in the configuration module. For the process registered as a malicious process, the monitoring module will stop the process at the moment of detection and automatically delete the process. For the process registered as an exceptional

process, it will allow the normal execution because it is specified as safe by the user.

Processing Module. The processing module forcibly stops the process suspicious of ransom ware in the monitoring module and inquires users about the appropriate handling of the process. Once the handling is determined, the information of the corresponding process will be stored in the database and used in the configuration module subsequently.

ID is used to place the number of each tuple. PackageName is the name of an application. RiskType is a flag to determine whether it is safe/unsafe. Comment is prepared in case a separate explanation is needed.

The processing module also warns users about the risk of the ransomware through Android permission analysis.

(i) System Permission.The ransomware has permissions of the system. It seizes permissions of the device's administrator and prevents users from manipulating the device. This permission involves the risk of ransomware browsing the user's personal files stored in the device without user's permission. It uses administrator's permission.

(ii) SMS Permission. While a normal application provides convenience to users with SMS permission, the ransomware intercepts received messages to use them for illegal purposes by using SMS permission.

(iii) Contract Permission. Permission to access contacts is stored in the device. Typical examples of making ill use of this permission are phishing and smishing.

(iv) Network Permission. Permission to automatically find network connected to the device and allow the ransomware to operate. Ransomware seizes permission of the device so that users cannot operate the device. It has the risk of intercepting user's personal information stored in the device.

The processing module inquires of users about whether to keep or delete the corresponding program after stopping the process suspicious of ransom ware.

If the user shows his intention to delete the application, when the same process appears later, it is automatically removed without asking about user's thoughts because the user recognizes the corresponding application as ransom ware.

If he determines the process as normal, its safety is guaranteed so the process will not be forcibly stopped by the proposed technique. In addition, the proposed technique will let the

user know if any part of the process is vulnerable

User Interface. User Interface provides users with easy access to the proposed method. UI is equipped with a basic format of the Android. It provides an interface of the configuration module. The proposed system functions can be turned on and off at any time using the corresponding interfaces.

9. CONCLUSION

In this paper, a technique is proposed to reduce damage caused by unknown ransomware attacks on Android devices. The proposed method can effectively reduce damage caused by ransomware with modified or new patterns without obtaining information on the ransomware.

It uses file input/output events and Processor status information based on the behavior of ransomware, unlike existing techniques that need information about the ransomware.

It can automatically prevent damage caused by such ransomware attacks later based on information collected on the detected ransomware.

10. FUTURE ENHANCEMENT

It is possible to use the future in all Android-based smart phones because this technique is added to the open source of Android source file. This technique is expected to allow users to minimize damage caused by attacks of ransomware that existing vaccine systems fail to detect.

Ransomware variants are increasing day by day. They usually target user wise (Average user, Business, Emergency service, Banking) and system wise (Personal Computer, Mobile Device, server).The main aim of ransomware is totake currency from the victim. Detecting this attack researcher used various techniques like V-detector negative selection algorithm, creating a safe zone to secure data, heldroid, honeypot, Cryptolock, and sand-box etc.

There is distinct model invented by the researcher to protect from malicious activities like ATPG model collect a nominal set of test packet, protect MFT file, patched software, backup important data regularly and ignore spam emails. Researchers discuss some fact about to secure system from attack and set some parameters to save data from attack in future. Just because of Ransomware are Malware and Trojan type attack so Anomaly-based IDS may be used in future for detecting abnormal behaviour of the network.

11. REFERENCES

[1] X. Luo and Q. Liao, “Ransomware : a new cyber hijacking threat to enterprises,” in Handbook of Research on Information Security and Assurance, IGI Global, 2009.

[2] “Worldwide Quarterly Mobile Phone Tracker,” IDC, August 2015, http://www.idc.com/tracker/showproductinfo.jsp?prod id=37.

[3] TREND Micro, Ransomware Definition—Security Intelligence, TREND Micro, Irving, Tex, USA, 2015, http://www.trendmicro .com/.

[4] D. Kim and S. Kim, “Design of quantification model for ransom ware prevent,” World Journal of Engineering and Technology, vol. 3, no. 3, pp. 203–207, 2015.

[5] D. Lim, “Treats and countermeasures of malware,” Journal of IT Convergence Society for SMB, vol. 5, no. 1, pp. 13–18, 2015.

[6] N. Andronio, S. Zanero, and F. Maggi, “HelDroid: dissecting and detecting mobile ransomware,” in Research in Attacks, Intrusions, and Defenses, vol. 9404 of Lecture Notes in Computer Science, pp. 382–404, Springer, 2015.

[7] A. Beuhring and K. Salous, “Beyond blacklisting: cyberdefense in the era of advanced persistent threats,” IEEE Security & Privacy, vol. 12, no. 5, pp. 90–93, 2014.

[8] P. Ducklin, “Reveton/FBI ransomware-exposed, explained and eliminated,” NakedSecurity, August 2012, https://nakedsecurity.sophos.com/.

[9] J. Milletary, Citadel Trojan Malware Analysis,” Dell Secure Works Counter Threat Unit Intelligence Services, Dell Secure Works, September 2012.

[10] T. M. Marengereke and K. Sornalakshmi, “Cloud based security solution for android smartphones,” in Proceedings of the IEEE International Conference on Circuit, Power and Computing Technologies (ICCPCT ‘15), pp. 1-6, Nagercoil, India, March 2015.