Recent Trends in Intensive Computing
M. Rajesh et al. (Eds.)

doi:10.3233/APC210173

A Proposed Methodology to Mitigate the Ransomware Attack

Salunke M. D [a, 1], Kumbharkar P. B [b] and. Dr. Pramod kumar [c]
[a] *Research Scholar, Shri JJT University, India*
[b] *Professor, RSCOE, Pune, India*
[c] *Professor Shri JJT University, India*

Abstract. Now a day's network security becomes more important to organizations, government offices. With the fast advancement of the innovation, assaults throughout the years have turned out to be both progressively various and modern. Ransomware attack becomes one of the most popular weapons for network attackers that ransomware attack is increased rapidly year by year. The study shows that the ransomware attack is one of the top attacks that are most attacked malware by the attackers. In this paper, we focus on mitigation techniques that can be used to recover and mitigate the ransomware attack. The mitigation or recovery approach is very difficult as ransomware is depending upon cryptographic algorithms which are very difficult to crack.

Keywords. Network Security, Attacks, Ransomware, malware, Mitigation, Sniffing.

1. Introduction

Attack is anything which imposes the harm on the system. It can be of two kinds in general. Active Attack: An Attack that may change the information or damage the System. Passive Attack: A type of Attack in which the Attackers goal is to obtain information. The Attack doesn't modify or harm the system. Attack is an assault on system framework security that gets from a keen risk [1].
The Three Goals of Security:
1: Confidentiality: hiding information from unauthorized access.
2: Integrity: preventing information from unauthorized modification.
3: Availability: should be easily available to authorized users.

The four classes of attacks that violate different security properties of the computer Networks are Interruption, Interception, Modification and Fabrication. [2] Ransomware is type of malware used by attacker to attack or locks user's system or data and ask user to pay ransom to gain access to data or system. Ransomware are real threat to systems that attacker can inject to user's system and encrypt the user data or system by using encryption algorithms like AES, RSA or some modern-day ransomware also uses combination of symmetric and asymmetric algorithms for

[1]Mangesh Dilip Salunke, Research Scholar, Shri JJT University,India
Email: salunkemangesh019@gmail.com.

encryption of user data or system and then ask user to pay ransom for accessing system or data by displaying the message about how you can get back your data, files or system [3].

Network defense techniques: The network defense techniques are those tools that can be used to protect network from being attacked or that are used to monitor malicious activities of attacker or process in network. Sometime these techniques allow us to avoid the malicious activities by providing strong security policies for organizations.

Cryptography: It includes protection of data and Data Hiding through the implementation of various algorithms and techniques. While Data Hiding the simple text is converted to a ciphertext, which is a combination of simple text and a certain key. This key is developed through different methods. Basically, there are two types of keys those are Symmetric key and public key. Symmetric key is uses same key for encryption and decryption of data which is kept private. Public key is using a public key known to all to encrypt data and a private key to decrypt data.

Cryptographic attack: Cryptographic attacks are those attacks that are created to evade the current network security systems. These attacks are designed by expertise attacker who knows how to compromise the security systems. These attacks can easily stop actions, productivity and revenue of well expanded business and cost millions of losses. Ransomware attack is one of the types of attack of cryptographic attack that allows digital extortion to the attacker.

2. Ransomware types

There are two types of Ransomware attack, one is Locky Ransomware, and another is Crypto Ransomware. These two classes of ransomware that defines the way of attack, one is Lock Screen Ransomware that simply locks or encrypt the user system or desktop or input system and keeps the user inaccessible by simply showing extortion message is also known as Locker Ransomware. And another is Crypto or Encryption Ransomware that encrypts the user data or files and asks to pay ransom is also known as cryptographic ransomware. Ransomware attacker changes their targets from individuals to organizations such as banking, government offices, and hospitals and may more. Attacker uses different ways to penetrate the user system with ransomware attack that is known as deployment location of attack like spam mails, compromised web sites, Downloading/Opening any malicious file, Log-into any already infected PC, Installing Pirated software are some examples.

The very first Ransomware attack happened in 1989 known as PC Cyborg also popularly known as AIDS Trojan that demanded $189 or $378 to the 20000 victims that work for AIDS research related journal. For the distribution attack vector used by attacker Dr. Josef Popp is in the form of Floppy disk. After that the attack becomes more popular of attacker as Internet grows the attack grow with it. The use of internet for financial transaction, digital communication, data transfer, and social interaction makes attack more spread and big concern of organizations [3].

3. Literature Review

Authors developed HelDroid a lightweight small emulation system on android platform that is a real time detection system. The system uses the features of natural language processing technique to detect locking mechanisms or encryption detectors with the help of static and dynamic analysis for Android Ransomware samples. The system is tested on a large dataset near about hundreds of thousands APK's that contains scareware, Malware, Good ware, and known ransomware and unknown Ransomware samples. Result shows that the system has near about zero false positive rate and 99% capability of recognizing new Ransomware samples on Android platform [4].

Ransomware attacks and mitigation or awareness strategies of attack with conducting interview and survey of victimized and non-victimized people and the result of survey were analyzed by using statistical analysis by using different factors such as age, education, awareness that are dependable upon causes of ransomware attack. And the result shows that it is irresponsibility and dependency for attack on the IT department of other employee to make the attack happen [5].

Author creates a novel solution in the form of an easy to use script that runs on Windows 7 platform to recover from Crypto ransomware. They executed their system on a secure platform such as Virtual machine and tested by attacking that virtual machine by renaming vssadmin.exe file which is used for backup purpose in virtual machines to prevent encryption of backup with theses crypto ransomware attack. The system shows that by using proper preventive measures such as updated antivirus, updated operating system and software, proper backup and well configured firewall one can easily restore the system to the normal state as it was before the encrypted state. The analysis is done on most recent and common 4 crypto Ransomware samples at that time [6].

In this authors implement a technique that monitors suspicious activity over a locally virtualized environment for a file system that is dynamic system name as POSTER. Their solution is based on the behavior of Ransomware on Windows 7 Platform to mitigate the effect of ransomware with four modules. The result shows the possibility to detect old as well as new variants of the Ransomware family. To analyze the gap of previous existing systems they have developed three new variants of ransomware such as Zero replacement, Friend indeed behavior, Ledger Manager Behavior based on their behavior [7].

Author studied and describes the crypto ransomware attack in terms of history and timeline of some popular ransomware attack that describes the journey of attack for making awareness among internet users about the attack and potential harm of attack. Static analysis is done on captured packets of ransomware from various sources to understand the working of ransomware attack, C&C server and contribution of crypto currency to ransomware attack. They have performed their static analysis on virtual machine environments. For that they have used two VMware machines one is for a fake DNS server as REMnux operating system and another is victim's machine that is a Windows 7 machine. Sample of Cerber ransomware was used to analyze a Wireshark traffic analysis tool [8].

Authors discussed crypto virology, the technique in which an attacker merges the cryptography with malware such as ransomware attack. They have discussed the symmetric and asymmetric key cryptography technique. The attacker uses the asymmetric key to launch the ransomware attack and how the public key of the attacker

is of no use to the victim and also how randomly generated symmetric key received to victim is unused to others [9].
They analyzed ransomware attack and provided a report of their analysis and study of ransomware attack with the help of history and evolution of ransomware attack and provide some prevention techniques that are necessary to counter the ransomware attack for different organizations. To understand and to analyse the working of attack they have created a sample model of attack as a demo ransomware in a controlled environment. Their demo model starts encrypting files with AES encryption algorithm after searching to only some specific types of files such as *.cpp extension files that they used for the target file in their model. In their result they state that the CPU usage increased from 3% to 28 % after execution of attack [10].
Author discussed the types of ransomwares such as Goldeneye, WannaCry, RAA ransomware, Cerber, Crysis, petya, Locky, CryptoWall, PowerWare with the help of case study of attack with most popular cyber-attack such as Google China, WannaCry, Heart bleed and PlayStation server. Author stated that the ransomware attack for encryption of files it generally use RSA 2048 encryption algorithm and because of security loophole of SMB that is samba server vulnerability which uses EternalBlue protocol which used by attacker as a exploit kit which mostly affect the windows operating systems such as windows 7, windows xp, windows 8, windows 10 and windows server which use AES-128 encryption algorithm for encryption process. Lastly the author described some prevention tips and security tips to users to avoid the ransomware attack [11].
Author discussed previous ransomware detection systems with the help of literature survey. Author also evaluates both stated and implicit assumptions on each and every detection system they have surveyed as their literature study. They gave name to working of attack as ransomware attack kill chain as a Identify and recon, Initial Attack, Command & Control, Discover & Spread and Extract & Exfiltrate are the phases of ransomware attacks on Android system [12].

4. Mitigation Approach

As ransomware attack is based on cryptographic algorithm such as AES, RSA and other algorithmic techniques are used to create this most effective attack. In cryptography the plain text is converted into unreadable cipher text format with the help of Cryptographic key. The key is required to convert this cipher text to again into plain text that is readable by humans. Attackers' usage these approach to attack systems or files to encrypt the users system or files. As the key is required to convert the files or system back to working stage attacker ask the user to pay for that key. Also these cryptographic algorithms are very strong in nature one cannot crack the key for decrypting the files which are locked due to ransomware attack.

Figure 1 describes the architecture of proposed systems mitigation module, in which it describes the process of mitigation or recovery from ransomware attack. In this left part shows the working of mitigation module and right part shows the working of decryption process of mitigation module.

(i) Packet Capturing: Packet capturing is the process of capturing the network packets for monitoring and detecting the possibilities of malicious code or attachments. There are various packet capturing techniques are available for analyzing and detecting the

packets for possible attack. Wireshark, Pcap and TCPDUMP are some examples of packet capturing and analyzing tools.

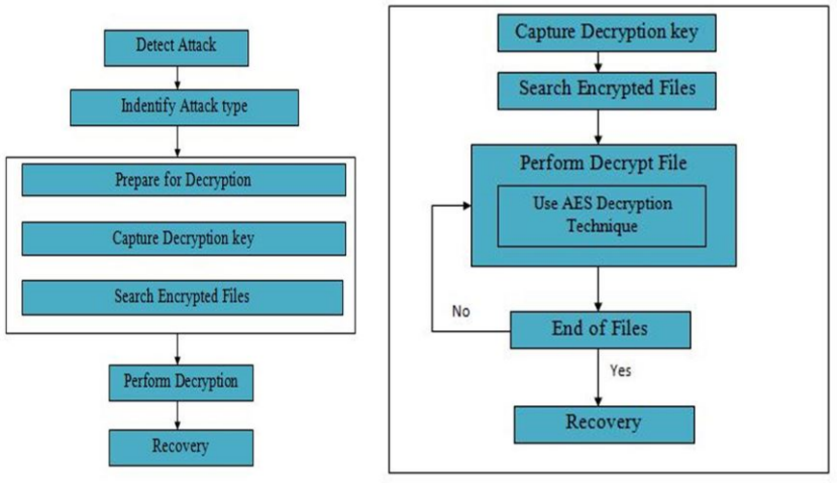

Figure 1. Architecture of proposed system mitigation module.

Wireshark: It is one of the most popular and widely used network packet analyzer tools for monitoring and analyzing the computer network for checking the possibilities of network attack in Figure 1.

PCAP: It is nothing but a Packet Capture. A tool for capturing the network traffic with the help of Application programming interface (API).

(ii) Sniffing: Sniffing or sniffer used to sniff the network packets with the help of packet capturing and analyzing tools. The tools are also known as Packet Sniffer. It is also known as Network Analyzer or Packet Analyzer which is useful for monitoring the computer network for network attack.

(iii) HTTP Traffic analysis: It is the process in which HTTP traffic from any network can be analyse, that is it capture the HTTP packets that are transfer from one end to another end of network and these packets are then analyzed for checking the possibility of malicious activity. Several tools can be used to capture and analyze the HTTP traffic.

5. Result and discussion

In proposed approach of ransomware mitigation technique, it is not even possible to crack or perform dictionary attack on AES or RSA to get the encryption key. So only way to get back data or files that are encrypted with ransomware attack is either pay the ransom or sniff the packets that are going outside into the direction of command-and-control server. With the help of this sniffing technique, we can able to capture and analyze the packet data that is going towards the command-and-control server after encryption process and that key of decryption is send to that server.

The proposed methodology for mitigation or recovery of ransomware attack data shall be implemented on Virtual machine and Windows 10 Machine. AES

cryptographic algorithm is used for encryption and decryption process of data in attack. For analyzing and monitoring the network packets Wireshark tool is best used.

6. Conclusion

The ransomware attack is very vital and most dangerous attack for computer users and organizations, so it is very important to counter such kind of attack. The biggest concern while designing the countermeasure system for countering the ransomware attack is the mitigation part as it allows users to recover from attack and get back data or system of users. One has to take care about recovery or mitigation module while building the ransomware countermeasure systems. Because of which in proposed system this countermeasure technique is includes mitigation as a one of the modules which is an important part of proposed system and works as a defending the most popular and powerful weapon of attacker that is ransomware attack.

References

[1] Saiyed Kashif Shaukat, Vinay J. Ribeiro," RansomWall: A Layered Defense System against Cryptographic Ransomware Attacks using Machine Learning", 2018 10th International Conference on Communication Systems & Networks

[2] Ibrahim Nadir, Taimur Bakhshi, “Contemporary Cybercrime: A Taxonomy of Ransomware Threats & Mitigation Techniques”, 2018 International Conference on Computing, Mathematics and Engineering Technologies – iCoMET 2018, 978-1-5386-1370-2/18/$31.00 ©2018 IEEE.

[3] Kul Prasad Subedi, Daya Ram Budhathoki, Dipankar Dasgupta, “Forensic Analysis of Ransomware Families using Static and Dynamic Analysis”, 2018 IEEE Symposium on Security and Privacy Workshops, DOI 10.1109/SPW.2018.00033

[4] Nicol´o Andronio, Stefano Zanero, and Federico Maggi, “HELDROID: Dissecting and Detecting Mobile Ransomware”, Springer International Publishing Switzerland 2015, RAID 2015, LNCS 9404, pp. 382–404, 2015. DOI: 10.1007/978-3-319-26362-5 18

[5] Rhythima Shinde, Pieter Van der Veeken, Stijn Van Schooten, Jan van den Berg,” Ransomware: Studying Transfer and Mitigation”, 2016 International Conference on Computing, Analytics and Security Trends (CAST) College of Engineering Pune, India- 2016 IEEE

[6] Mattias Wecksten, Jan Frick, Andreas Sjostrom, Eric Jarpe,“Novel Method for Recovery from Crypto Ransomware Infections”,2016 2nd IEEE International Conference on Computer and Communications

[7] Manish Shukla, Sutapa Mondal ,Sachin Lodha, “POSTER: Locally Virtualized Environment for Mitigating Ransomware Threat”, ACM ISBN 978-1-4503-4139-4/16/10. DOI: http://dx.doi.org/10.1145/2976749.2989051

[8] Shaunak Sanjay Ganorkar and Kamalanathan Kandasamy, “UNDERSTANDING AND DEFENDING CRYPTO-RANSOMWARE”, ARPN Journal of Engineering and Applied Sciences, VOL. 12, NO. 12, JUNE 2017

[9] Adam L. Young and Moti Yung, “Cryptovirology: The Birth, Neglect, and Explosion of Ransomware”, COMMUNICATIONS OF THE ACM JULY 2017, VOL. 60