Ransomware Deployment and Analysis

T. Nithya[1], K. Vijaya[2], Dharanya Subramanian[3], Elakkiya Balamurugan[4], Kiruthika Shanmugavel[5]

[1, 2] Assistant Professor, Department of Information Technology, Vellalar College of Engineering & Technology, Erode, Tamil Nadu, India. Email: tnithya27@gmail.com[1], Vijaya.krishnamoorthy@gmail.com[2]

[3,4,5]UG Scholar, Department of Information Technology, Vellalar College of Engineering & Technology, Erode, Tamil Nadu, India. Email: dharan.subbu.23@gmail.com[3] elakiyabalamurugan@gmail.com[4] kiruthikavel13@gmail.com[5]

Abstract - Ransomware is a type of computer malware that threatens computer users by locking access to their computers and prohibits the access to its own users or locking access to their files by encrypting them. Cryptoransomware is a type of ransomware that encrypts the important files of the user and demands for ransom to obtain the decryption key. The technological world is facing a rapid increase in ransomware attacks in the past few decades. The signature-based and heuristic detection techniques have considered to be obsolete due to the drastic increase in the number of ransomware variants and dynamic pattern of ransomware attack vectors. In order to survive from ransomware attack, a better understanding on ransomware deployment is needed, along with its characteristics. The major contribution of our project is on addressing this challenge by carrying out an investigation on 19 different variants of ransomware, which leads to develop a model for categorising ransomware types that can be used to improve detection and effective handling of ransomware incidents.

Key words - Crypto-ransomware, encryption, decryption, variants, heuristic detection.

I.INTRODUCTION

Recently, the world is witnessing a high count in ransomware attacks. Ransomware is a malware for data kidnapping. It exploits the user's PC for vulnerability and encrypts the user's (victim's) data. Ransomware prohibits the user from using his/her own PC. Ransomware spreads through e-mail attachments, infected programs and websites which are vulnerable to attacks. Ransomware has miscellaneous characteristic which holds the victim's computer for ransom. The term ransomware can be substituted by similar terms like crypto-virus, crypto-virus, crypto-trojan, crypto-worm.

From the past record, we have seen numerous types of ransomware under various classifications. However, all of them will prevent the user from using his/her own PC normally, and the ransomware creator (attacker) will ask the user (victim) to do something before the user can use his/her own PC. The attackers may target any computer users, which can be a home computer, endpoints in an enterprise network, or servers used by a government agency or healthcare provider. Ransomware always contains a ransom note, which may demand the user either to pay the money demanded or to do certain tasks mentioned in the ransom note that benefits the ransomware creator. Still there is no guarantee that we can get back access to our computer and files by paying ransom or doing tasks mentioned in the ransomware.

II.RANSOMWARE OVERVIEW

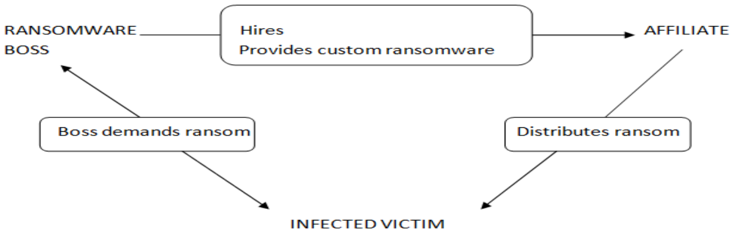

Fig. 1 Ransomware Architecture

The idea of crypto-virology was introduced in 1996 by Young and Yung, who believed and proved that cryptography can be used for offensive purposes, which was later evolved to be ransomware. It is a computer malware for data hijacking. The rapid increase in the ransomware growth was witnessed in the past few years. Ransomware can be categorized into various types under various families. Changing pattern of attack vectors leads to the number of ransomware variants. Some of the common attack vectors are email attachments, exploit kits, phishing, downloader, etc. The ransomware targets the user's (victim's) files through mapping the victim's

© IJRAD.

environment and by looking into recent file history which usually maps to the important files of the user in various folders like my documents, sometimes even recycle bin. The ransom note can be in any form. It may be an application, a text file on the desktop, or any other thing that catches the user's attention. Irrespective of its type, it generally consists of a note from the ransomware creator that demands the victim to do something that benefits the attacker, to gain access to his/her own device.

III.RELATED WORK

A. Ransomware Early Detection by the Analysis of File Sharing Traffic.

Mikel, Izal in the Journal of Network and Computer Applications by ELSEVIER (2018). This paper shows the life cycle & analysis of Crypto-ransomware[1]. Crypto-ransomware is a type of malware that locks access to user files by encrypting them and demands a ransom in order to obtain the decryption key. This type of malware has become a serious threat for most enterprises. In those cases where the infected computer has access to documents in network shared volumes, a single host can lock access to documents across several departments in the company. Proposed an algorithm called REDFISH based on the analysis of passively monitored network traffic. Some of the positive aspects of this paper includes: It can detect the ransomware activity in less than 20s and before more than 10 files are lost. It offers analytical model for the probability of early detection & false alarms. It also suffers from serious disadvantages like for preventing the user's data from getting into unrecoverable state, API calls, canary file or binary analysis must be discarded. Probability for False positives (triggering the alarm without real ransomware action).

A. CryptoLock (& Drop it): Stopping Ransomware attacks on User Data.

This paper was an IEEE paper contributed by Nolen Scaife, Henry Carter, Patrick Traynor, Kevin R.B. Bulter (2016). In this paper some of the important types of ransomware like Teslacrypt, CTB-Locker, GP code has been examined and used for CryptoDrop detection. Ransomware is a nuisance which can be remediated by wiping the system or removing the disk & extracting the user's important data. CryptoDrop[3] reduces the need for the victim to pay the ransom and made the malware ineffective. Using a set of behavior indicators, CryptoDrop can halt a process that appears to be tampering with a large amount of the user's data. While CryptoDrop is effective at quickly detecting ransomware, we note that any evaluation of its real-world utility must also include a discussion on incorrect detection of benign activity. False positive for CryptoDrop is challenging, since its analysis requires changes to be made to a user's protected documents. CryptoDrop is unable to determine the intent of the changes it inspects.

B. Unknown Malware Detection Using Network Traffic Classification.

This IEEE paper was the major contribution of Nolen Dmitri Bekerman, Bracha Shapira, Lior Rokach, Ariel Bar (2015). The paper presents an End-to-end supervised system for detecting malware by analyzing the network traffic. For this, Network classification method is used. It analyzes DNS, HTTP, & SSL protocols, & combines different network classification methods in different resolutions of network. The data that can pass through firewalls is recorded and relayed further to the global network. The system analyzes the collected data in order to detect malicious activities and issue alerts when such activities are detected. One major shortcoming of the approaches that aimed at specific use cases was that they could not detect previously unseen malware. A major advantage of this paper is the ability to detect unknown [6] (new) malware or malware families that were not previously investigated. Meanwhile, it evaluates the effect of the environment on the performance. A feature selection method is used to identify the most meaningful features and to reduce the data dimensionality to a tractable size. Finally, various supervised methods are evaluated to indicate whether traffic in the network is malicious, to attribute it to known malware families and to discover new threats.

C. Experimental Analysis of Ransomware on Windows and Android Platforms.

It was an IEEE paper published by Monika, Pavol Zavarsky, Dale Lindskog (2016). The paper focuses on providing insights on how ransomware have evolved from its starting till March 2016 by analyzing samples of selected ransomware variants from existing ransomware families in Windows and Android environments[5]. Seventeen Windows and eight Android ransomware families were analyzed. For each ransomware family, at least, three variants belonging to the same family were compared. The analysis revealed that ransomware variants behave in a very similar manner, but use different payloads. The analysis shows that there has been a significant improvement in encryption techniques used by ransomware. The experimental results in Windows environment demonstrate that detection of ransomware is possible by monitoring abnormal file system and registry activities. In Android environment, analysis reveals that likelihood of ransomware attacks can be reduced by paying a closer attention to permissions requested by the Android applications. All the inbuilt defense mechanisms and above detection tools should be kept up and running all the time. Ransomware can spread on various platforms like Linux and Mac operating systems1. So, analysis of ransomware should be done on these platforms too.

IV.LITERATURE SURVEY

S.No	Author	Title	Overview	Positive Aspects	Limitations
1	Daniel Morato , Eduardo Berrueta, Eduardo Magana, Mikel, Izal	Ransomware Early Detection by the Analysis of File Sharing Traffic (2018).	This paper shows the life cycle & analysis of Crypto ransomware. Proposed an algorithm called REDFISH based on the analysis of passively monitored network traffic.	It can detect the ransomware activity in less than 20s and before more than 10 files are lost. Offers analytical model for the probability of early detection & false alarms.	To prevent the user's data from getting into un-recoverable state, API calls, canary file or binary analysis must be discarded. Probability for False positives (triggering the alarm without real ransomware action).
2	Nolen Scaife, Henry Carter, Patrick Traynor, Kevin R.B. Bulter	CryptoLock (& Drop it): Stopping Ransomware attacks on User Data (2016).	Teslacrypt, CTB-Locker, GP code are used for CryptoDrop detection. Remediated by wiping the system or removing the disk & extracting the user's important data.	CryptoDrop reduces the need for the victim to pay the ransom and made the malware ineffective.	CryptoDrop stops ransomware from executing with the median loss of only 10 files.
3	Dmitri Bekerman, Bracha Shapira, Lior Rokach, Ariel Bar	Unknown Malware Detection Using Network Traffic Classification (2015)	End-to-end supervised system for detecting malware by analyzing network traffic. Network classification method is used.	Analyzes DNS, HTTP, & SSL protocols, & combines different network classification methods in different resolutions of network.	Evaluated the effect of the environment on the performance.

V.PROPOSED SYSTEM

Till now, the technological world has witnessed various models for detecting ransomware. All of them dealt with detecting the ransomware when it encrypts the file that resides in the user's computer. However, the concept of centralization offers a better utilization of resources in terms of storage, group sharing capabilities, disk quality, maintenance and periodic backups. Due to this, most of the users like to use the centralized and shared resources, which serve as a gateway for ransomware and similar malware attacks.

Hence we've developed a ransomware detection tool by analysing 19 variants of ransomware, which is capable of detecting ransomware infections without any software installation at end-hosts. The ransomware

© IJRAD.

deployment and analysis tool we have developed using pure java, can detect ransomware in an efficient way, meeting up the time and resource constraints. The tool provides a quick recovery from the ransomware attack.

A. Ideology

Among various kinds of ransomware families that have been identified and analysed till now, most of the ransomware types uses AES-256, a Strong Encryption Algorithm, to encrypt the victim's data in the background. AES-256 algorithm uses RSA Public Key. AES is a symmetric encryption algorithm. It has the block length of 128 bits and key length of 128, 192, 256 bits. RSA uses public key for both encryption and decryption process. The AES Symmetric key thus obtained, can be secured and it can be stored in an embedded database and thus it can be decrypted using the same when it asks for ransom. By implementing this, we can able to provide a better solution to the ransomware issue.

B. Classification of Ransomware Samples

From the detailed analysis of our ransomware samples, we have recognized 3 types of general behaviours in the samples:

- Type I - The malware reads the original file, creates a new file with a different name or extension and it writes in the new file the encrypted content from the original one. Finally, it deletes the original file and proceeds to the next one.
- Type II - It is similar to type I but the encrypted content is written over the original file, not in a new one.
- Type III - It is similar to type II but after overwriting the content it renames the file, adding an extension specific to the ransomware strain.

Further, the testing process can be done with the help of detailed analysis of more than 50 ransomware samples obtained from 19 variants which are listed below in table 1.

TABLE 1: LIST OF RANSOMWARE SAMPLES

Name of the Variant	Versions Released	Date of Appearance	Behaviour Type	Characteristics	No. of. Samples
TorrentLocker	CryptoFortress	February 2014	III	Ransomware Trojan	1
CTB Locker	CTB Locker v4.0	July 2014	I	Encrypts victim's hard disk	3
VirLock	VirLock	December 2014	I	Infects binary files	1
Teslacrypt	Teslacrypt v3.0	February 2015	III	Ransomware Trojan	1
DMA Locker	DMA Locker	December 2015	III	Targets Windows OS	1
Locky	Locky v1.0, Aesir, Odin, Osiris, Diablo6	February 2016	III	Ransomware Trojan Vector: e-mail attachments	10
Cerber	Cerber v2.0, v4.0, v4.1.6, v5.0, v4.1, Red Cerber	March 2016	III	Ransomware-as-a-Service (RaaS) application	15
CryptXXX	CryptMIC v5.001	April 2016	II	Ransomware Trojan Targets Windows	1
Bart	Bart v2.0	June 2016	I	Victim: zip attachments through email	1
CryptoMix	CryptFile2	June 2016	I	Single link spent via spam email	10
Crysis	Crysis, Dharma	November 2016	III	Targets Windows Systems	1
Sage	Sage v2.0	December 2016	III	Appends .sage extension to the encrypted files	1
MRCR	MRCR1	December 2016	III	Uses custom encryption algorithm	1

Spora	Spora	January 2017	II	Uses RSA cryptography	1
WannaCry	WannaCry v2.0	February 2017	I	Ransomware Cryptoworm	2
BTC Ware	Aleta	March 2017	III	Installed manually	1
Jaff	Jaff	May 2017	III	Encrypted files are appended with .jaff extension	1
Globe	GlobeImposter v2.0	June 2017	III	Ransomware Trojan	1
Zeus	Zeus	May 2018	I	Trojan Horse package used to steal banking information	1

VI.CONCLUSION & FUTURE SCOPE

The characterization of ransomware families is based on ransomware samples from 19 variants that have been found over the last few years. Results shows that a significant number of ransomware families exhibits very similar characteristics. Best practices to prevent the user's data from getting into unrecoverable state, a user should have incremental online and offline backups of all the important data and images. The most recent ransomware attacks like STOP (DJVU), Dharma, Phobos, GlobeImposter, etc have been witnessed in the year 2019. The Baltimore ransomware attack was occurred in May 2019 by a new strain of ransomware called RobbinHood. The current project aims at detecting and recovering from the classified species of ransomware. So, analysis of ransomware can be extended for classification and detection of new strands of ransomware and its recovery can be done for future research work.

REFERENCES

[1] Daniel Morato, Eduardo Berrueta, Eduardo Magaña, Mikel Izal, "Ransomware Early Detection by the Analysis of File Sharing Traffic," Journal of Network and computer Applications, vol.124, no. 15, pp. 14-32, December 2018.

[2] S.Mahmudha Fasheem, P.Kanimozhi, B.AkoraMurthy, Detection and Avoidance of Ransomware, International Journal of Engineering Development and Research , Volume 5, Issue 1, pp. 590-595, 2017.

[3] Nolen Scaife, Henry Carter, Patrick Traynor, Kevin R.B. Bulter, CryptoLock (& Drop it): Stopping Ransomware attacks on User Data. IEEE 36th International Conference on Distributed Computing Systems (ICDCS), 2016.

[4] Sangguen Song, Bongjoon Kim, and Sangjun Lee, The Effective Ransomware Prevention Technique using Process Monitoring on Android Platform: Hindawi, Mobile Information Systems, vol. 1, pp. 1-9, 2016.

[5] Monika, Pavol Zavarsky, Dale Lindskog, Experimental Analysis of Ransomware on Windows & Android Platform. ELSEVIER. *in* Procedia Computer Science, vol. 94, pp. 465-472, December 2016.

[6] Dmitri Bekerman, Bracha Shapira, Lior Rokach, Ariel Bar, 2015. Unknown Malware Detection Using Network Traffic Classification. 2015 IEEE Conference on Communications and Network Security (CNS)

[7] Kai Zhao, Dafang Zhang, Xin Su, WenjianLi, 2015. A Feature extraction and Selection tool for Android Malware Detection. 2015 IEEE Symposium on Computers and Communication (ISCC)