A Comprehensive Survey: Ransomware Attacks Prevention, Monitoring and Damage Control

Jinal P. Tailor
Department of Information Technology
Shri S'ad Vidya Mandal Institute of Technology
Bharuch, Gujarat, India

Ashish D. Patel
Department of Information Technology
Shri S'ad Vidya Mandal Institute of Technology
Bharuch, Gujarat, India

***Abstract* – Ransomware is a type of malware that prevents or restricts user from accessing their system, either by locking the system's screen or by locking the users' files in the system unless a ransom is paid. More modern ransomware families, individually categorize as crypto-ransomware, encrypt certain file types on infected systems and forces users to pay the ransom through online payment methods to get a decrypt key. The analysis shows that there has been a significant improvement in encryption techniques used by ransomware. The careful analysis of ransomware behavior can produce an effective detection system that significantly reduces the amount of victim data loss.**

***Index Terms* – Ransomware attack, Security, Detection, Prevention.**

I. Introduction

Ransomware is a type of malware that uses malicious code that infects a computer and spreads rapidly to encrypt the data or to lock the machine. This malware makes the data inaccessible to the users and the attackers demand payment from the user to have their files unencrypted and accessible. The payment is often requested in Bitcoin (is a cryptocurrency and a payment system) or other invisible currency. Businesses and individuals worldwide are currently under attack by ransomware[1]. Ransomware victimize internet users by hijacking user files, encrypting them, and then demanding payment in exchange for the decryption key[2]. Some most common methods used by cybercriminals to spread ransomware are Spam email campaigns that contain malicious links or attachments; Internet traffic redirects to malicious websites; Drive-by downloads, etc.

Some security applications detect ransomware based on its activity such as File System Activities, Registry Activities, Device control Communications, Network Activity, and Locking mechanism[1]. Security firms are consistently developing and releasing anti-ransomware application and decryption tools in response to the threat. However, solutions may not always be present because some encryption is too difficult to break without the decryption key[3]. In the event of an attack, organizations can minimize damage if they can detect the malware early. Business and individuals worldwide are currently under attack by ransomware. The main purpose of ransomware is to maximize the monetization using malware[1]. It has started doing more than just displaying advertisements, blocking service, disable keyboard or spying on user activities. It locks the system or encrypts the data leaving victims unable to help to make a payment and sometimes it also threatens the user to expose sensitive information to the public if payment is not done[1].

In case of windows, from figure 1 it shown that there are some main stages that every crypto family goes through. Each variant gets into victim's machine via any malicious website, email attachment or any malicious link and progress from there.

Fig. 1. Life cycle of Windows based Ransomware

Once the victim's machine gets infected, it contacts Command and Control server. A command and control server is the centralized computer that issues commands to a botnet (a network of private computers infected with malicious software and controlled as a group without the owners' knowledge or zombie army) and receives reports back from the computers. Command and control servers may be either directly controlled by the malware operators, or themselves run on hardware compromised by malware. It sends victim's machine information to the attacker and ultimately obtains a randomly generated symmetric key from the server.

Once it receives the encryption key, then it looks for specific files and folders to encrypt. Some variants look for all disk drives, network share and removable drives as well for encrypting their data. Meanwhile, the malware deletes all the restore points, backup folders, and shadow volume copies[1].

After the entire encryption process, it will display the ransom payment message on victim's machine. In the case of locker ransomware, malware goes throughout all the same phases but it doesn't do encryption of data. Once the victim's machine is infected with locker ransomware, it takes organizational rights and takes control of the keyboard. It locks the user access to the device. It changes the desktop wallpaper or it will show a window which notify about ransomware attack and show the steps to follow in order to get their access back[1].

Ransomware is essentially just an encryption tool that safely packs away your files into an unreadable format. Unfortunately, only the hacker knows the decryption key. As some observers have noted, however, these particular hackers tend to be fairly honorable about giving you the key provided you pay some "fee" for their time and trouble, often in Bitcoin. This business model, as immoral as4 it may be, has a certain logic to it: keep the payments small enough to be worth avoiding the hassles of losing files or trying to resolve the matter through other means, and keep victims reassured that paying up will get them their data back[2].

The reminder of this paper is organized as follows: in section II related work is included with literature survey and section III consists of detection and prevention of ransomware and section IV consist final conclusion of paper.

II. Related Work

A. Ransomware Evolution

In this section includes the year vise evolution of the ransomware attacks. The earliest Windows ransomware started to spread in 1989 and since then it has been present till now but has changed notably since then. The first ransomware attack was PC Cyborg attack, which was seen in December 1989. Its payload hides the files on the hard drive and encrypted their names, and displayed a message claiming that the user's license to use a certain piece of software had expired. The user was asked to pay US$189 to "PC Cyborg Corporation" in order to obtain a repair tool. It was the first crypto form ransomware as it used the combination of a symmetric key and an initialization vector to encrypt the files present in the computer drives[1].

The first fake antivirus ransomware appear in 2004 and then in 2005 the series of fake antivirus ransomware types seen. Some of these were named as Spysherriff, Performance Optimizer, and Registry care[1]. In 2005, the PGPcoder family started growing and this visibly indicates the era of crypto ransomware. Gpcode used custom encryption method for encryption of data. PGPcoder spread wildly till 2008 as we can see many variants. In 2006, two other families started spreading, these are Cryzip and Archiveus. Cryzip searched for files with selected extensions, and then located these encrypted files in a zipped folder. Archiveus placed all the files in a password protected folder[1].

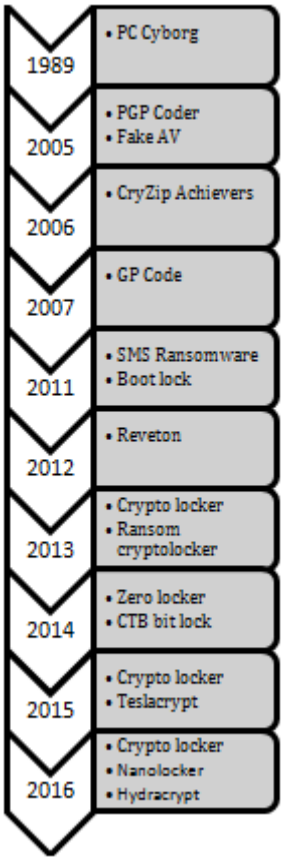

Fig. 2. Timeline for Windows based ransomware

MBR (Master Boot Record is the information in the first segment of any hard disk that identifies how and where an operating system is placed so that it can be loaded into the computer's main storage or random access memory). Ransomware came into continuation in 2010, the first variant that we came across was Trojan- Ransom.Boot.Seftad.a, and in 2011 bootlock B out. This type of ransomware replaces the original MBR with its own code and then locks the user from

accessing its services. It not at all encrypts file and displays the ransom message at computer boot-up time[1].

Fake Antivirus (Fake AV is detection for Trojan horse programs that intentionally misrepresent the security status of a computer) was increase in the natural in 2004. It became significant in 2005 when it tried to take the form of Fake Antivirus solution, Performance Optimizer software and Registry care software, which tried to offer paid solutions for your machine problems which didn't even existed. It was surfaced over the internet till 2008[1].

Fake FBI(Federal Bureau of Investigation) ransomware out in 2011 with the Ransom lock family. Later in 2012, families like Reveton and ACCDFISA started spreading in-the-wild. These families display the fine payment notice from official looking local law enforcement agencies. Later, many variants of Ransom lock and Reveton came in 2013. In 2014, new locker families like Virlock, Kovter and few new variants of Ransom lock arrived[1].

Crypto ransomware became a vast problem in 2013, it came back with Cryptolocker, Cryptolocker 2, Ransomcrypt, Crilock and Dirty Decrypt. Later in 2015, a new variants of Ransomcrypt, Crypto locker, Vaultcrypt, Crypto Fortress,Troldesh, TelsaCrypt, CryptoTor Locker, Cryptowall 4. Cryptowall 3 uses Tor anonymity network for C & C communication. Nearly all recent crypto ransomware families are using very sophisticated encryption techniques.

Ransomweb, Pclock, Cryptowall 3, Crypto blocker and Recently in 2016, new families of crypto like PHPRansm.B, Locky, Ransom32, HydraCrypt, Crypto locker.N andCerber have started to spread [1].

B. Literature Survey

The following table 1 contains study of 20 most important papers on the ransomware attack which helps to identify the effects, amount that to pay for ransom when it gets the attack to the system. It also includes the overview of each paper with their positive and negative aspects. Publishers and publication year are also included in the table

. TABLE 1: Literature Survey on Ransomware Attack

Publication/Year	Title	Overview	Positive Aspects	Limitations
ELSEVIER/2016	Experimental Analysis of Ransomware on Windows and Android Platforms: Evolution and Characterization[1]	-This paper shows the life cycle and analysis of windows based Ransomware. -Also it presents evolution of ransomware for windows. -MD5 method, Cuckoo Sandbox used for malware analysis system. -RSA and AES used for encryption.	-The main purpose is to detect the ransomware by monitoring abnormal file system registry activities. - PEid tool is used for windows ransomware detection.	- To prevent the user's data from getting into un-recoverable state, a user should have incremental online and offline backups of all the important data and images.
IEEE/2016	CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data[2]	-Teslacrypt, CTB-Locker, GP code are used for CryptoDrop detection. - Ransomware is a nuisance which can be remedied by wiping the system or removing the disk and extracting the user's important data.	-CryptoDrop reduces the need for the victim to pay the ransom and represents the malware ineffective.	- CryptoDrop stops ransomware from executing with a median loss of only 10 files.
Hindawi/ 2016	The Effective Ransomware Prevention Technique Using Process Monitoring on Android Platform[4]	-Ransomware prevention technique on Android platform is proposed. - The proposed technique is designed with three modules: Configuration, Monitoring, and Processing.	- The proposed method can monitor file events that occurred when the ransomware accesses and copies files. -Ransomware classified into three types: Scareware, Lock-Screen, and Encrypting.	- It does not need to install an application such as existing prevention and reduce damage caused by unknown ransomware attacks.
IEEE/2015	Unknown Malware Detection Using Network Traffic Classification[5]	- It presents an end-to-end supervised based system for detecting malware by analyzing network traffic. -Network classification method is used.	- The proposed method analyzes DNS, HTTP, and SSL protocols, and combines different network classification methods in different resolutions of network.	- Evaluated the effect of the environment on the performance.
IEEE/2015	Fest: A Feature Extraction and Selection Tool for Android Malware Detection[6]	- FEST contains three components: AppExtractor, FrequenSel and Classifier. -FEST generally aims with detecting malware using both of high efficiency and accuracy. -AppExtractor, FrequenSel is used as the method.	- FEST only takes 6.5s to analyze an app on a common PC, which is very time-efficient for malware detection in Android markets.	-FrequenSel is definitely more suitable for feature dataset.

IEEE/2015	Validation of Network Simulation Model with Emulation using Example Malware[7]	-Cyber Army Modeling and Simulation (CyAMS) model is to provide an accurate representation of malware propagation over a behavioral model network.	- National Cyber Range (NCR) is utilized to generate data and provide results for a number of different test cases on networks of varying sizes.	-Results demonstrated that several orders of magnitude of less computing resources are required for a simulation compared to emulation for particular test case.
2016	Protecting Your Networks from Ransomware[8]	-The method Remote Desktop protocol (RDP) and Software Restriction Policies (SRP) is used. - Configure firewalls to block access to known malicious IP addresses.	-Ransomware targets home users, businesses, and government networks and can lead to temporary or permanent loss of sensitive or corrective information.	-The prevention measures are to set anti-virus and anti-malware programs to conduct regular scans automatically. -Back up data regularly and keep it secure.
ELSEVIER/2016	Grouping the executables to detect malwares with high accuracy[9]	- K-Means Clustering algorithm is used to obtain groups to select promising features for training classifiers to detect variants of malwares or unknown malwares. -Metamorphic malware represent the next group of virus that can create an entirely new variant after reproduction.	- The study of malwares and generous executables in groups to detect unknown malwares with high accuracy.	-Detection of malwares on the basis of classifiers, file sizes gives accuracy up to 99.11%.
Springer/ 2015	HELDROID: Dissecting and Detecting Mobile Ransomware[10]	-HelDroid, a fast, efficient and fully automated approach that recognizes known and unknown scareware and ransomware samples. -The main approach is to determine whether a mobile application attempts to threaten the user, to lock the device and to encrypt data.	-.The classifier based Natural Language Processing (NLP) features, a lightweight emulation technique to detect locking strategies, and the application of ruin tracking for detecting file-encrypting flows. -HelDroid performs well against unknown ransomware samples.	-Ransomware, before or after the threatening phase the malware actually locks the device and/or encrypts sensitive content until the ransom is paid, usually through money transfer.
Springer/ 2011	Study of Malware Threats Faced by the Typical Email User[11]	-The main objective of this paper is the behavioral characteristics of different malware types affecting the Internet and other enterprise email systems.	-A sandbox test environment platform using virtual machines was built to perform research and simulate real-life malware behavior and determine its signature at the point of execution for proper analysis.	-The future work is to expand the malware data coverage to a maximum of one year period to record a complete picture of the malware behavior over an extended period of time.
IEEE/2011	An Experimental Analysis For Malware Detection Using Extrusion[12]	-Method such as Inbound traffic approach, distributed denial-of-service (DDoS) activities and direct attacks and tool such as Snort software is used. - For the detection of malware, it will use two sniffers which will be implemented using an open source snort.	-The main goal of this paper is to work out a realistic solution to protect the network from the malware by exploring the feasibility of the concept of analysis of outbound traffic.	- The sniffer-2 takes more time to search through a database containing more number of rules than sniffer-1.
IEEE/2011	A Virus Detection Scheme Based on Features of Control Flow Graph[13]	- Paper present a graph features based method, which can be used in the method of machine learning, and design a virus detection model based on feature method.	- It present a novel feature chooses method that extract structural features from the Control Flow Graph of PE files.	- This paper is not providing better convinced data of detection results.
Springer/ 2010	Monitoring Malware Activity on the LAN Network[14]	-Honeypot operation is to make available some resources or illusion of resources as a trap for malware program and monitor program behavior in its attempts of resource usage.	- Access router works also as DHCP server, assigning IP addresses to systems on research network and as a DNS server.	- Assigned IP addresses do not generate much address resolution protocol (ARP) traffic.
Springer/ 2014	Research on Classification of Malware Source Code[15]	-In the proposed system, file structure and file content are extracted as features for classification system.	-This paper presents a novel classification approach, based on content similarity and directory structure similarity.	-The proposed approach is not to replace classification of binary malware.
2016	Ransomware attacks: detection, prevention	-The five phases of ransomware are Exploitation and infection,	-The main objective is defending against a	-Organizations can suffer the effects of lost productivity, loss of business, problem

	and cure[16]	Delivery and execution, Back-up spoliation, File encryption and User notification and clean-up.	ransomware attack is largely dependent on the level of preparation and the ability to detect, shut down and contain suspicious activity.	to customers and potentially the permanent loss of data.
Springer/ 2014	Feature-Distributed Malware Attack: Risk and Defence[17]	-The main objective is to propose the new method of feature-distributed malware that dynamically distributes its features to various software components.	-In particular, malware can perform its functionalities by dynamically distributing them to user-approved or system approved applications.	-C&C communication of the current implementation is based on sbd(Automotive technology consultancy and research) that is a Netcat-clone, designed to be portable and offer strong encryption.
Springer/ 2015	A comparison of static, dynamic, and hybrid analysis for malware detection[18]	-Used malware detection method is signature scanning. There are many approaches to the malware detection problem such as signature-based, behavior based, and statistical-based detection.	-The main purpose of this paper is to compare malware detection techniques based on static, dynamic, and hybrid analysis.	-Future work could include a similar analysis involving additional features beyond API calls and opcodes.
Springer/ 2010	Analyzing and Exploiting Network Behaviors of Malware[19]	-Clustering and Classification algorithms are comprehensively used in the literature to evaluate proposed host, network and hybrid detection approaches.	-The goal of the research is a real time behavior based malware detection system incorporating several perspectives capable of detecting known and unknown malware on host machines.	- The reports do not include sufficient detailed information to identify malware's precise implementation.
Springer/ 2011	A Framework for Defining Malware Behavior Using Run Time Analysis and Resource Monitoring[20]	-It proposes a framework for dynamic malware analysis using real time analysis and resource monitoring. Two common techniques that can be used to analyze malware are static analysis and dynamic analysis.	-The proposed framework has three major processes such as run time analysis, resource monitoring and behavior definition.	-The main problem of approach is the technique to disassemble the program because most of the malware codes are blur by great variety of packers.
IEEE/2012	Automatic Signature Analysis and Generation for Large-Scale Network Malware[21]	-It presents a technique for large-scale malware analysis with feature extraction based on hashed matrix. -It proposes the automatic signature generation using the Bayesian signature selection within clusters.	-Feature hashing is to get the bit-vector representation of the malware in each cluster. -Bayesian selection method achieves good performance in speed and accuracy, and can also be efficient in presence of noise.	- Feature hashing is a fast and space efficient way of vectorizing features. - Bayesian selection method provides a way to ensure the low false negative and low false positive of the signature.

III. Detection and prevention of Ransomware

A. Detection of Ransomware

Ransomware is an increasing criminal activity involving numerous variants. Since 2012 when police locker ransomware (The malware is known as "policeware" or a "police locker," and it takes over your Windows with a warning that claims you are under observation by centralized agents for alleged criminal activity)[1]. Various variants encrypt not just the files on the infected device, but also the contents of shared or networked drives, externally attached storage media devices, and cloud storage services that are mapped to infected computers[4]. The first variants of Ransomware used a small number of very specific file extensions like .crypt. However, each new variant seems to use different extensions and some even keep the file name intact. There are many ways to detect the presence of ransomware on the network[24]. They are as follows:

a. *Watch out for known file extensions*:

Even though the list of known Ransomware file extensions is growing rapidly, it is still a useful method for detecting suspicious activity. Before you do anything

you need to get file activity monitoring in place so that you have both a real time and historical record of all file and folder activity on your network file shares[24].

b. *Watch out for an increase in file renames:*

File renames are not a common action when it comes to activity on network file shares. Over the course of a normal day, you may end up with just a handful of renames even if you have hundreds of users on your network. When Ransomware strikes, it will result in a massive increase in file renames as your data gets encrypted. However, if the number of renames goes above a certain threshold, then you have a potential Ransomware issue[24].

c. *Create a sacrificial network share:*

When Ransomware strikes, it typically looks for local files first and then moves onto network shares. Most of the variants go through the network shares in alphabetical

order G: drive then H: drive etc. A sacrificial network share can act as an early warning system and also delay the Ransomware from getting to your critical data[24].

d. Use client based anti-ransomware agents:

Anti-ransomware software applications are designed to run in the background and block attempts by Ransomware to encrypt data. They also monitor the Windows registry for text strings known to be associated with Ransomware[24].

B. Prevention of Ransomware

i. Back up your files regularly and keep a current backup off-site. Backups can protect your data against more than ransomware. Make sure you encrypt the backed up data so only you can restore it[8].
ii. Be very careful about opening unsolicited attachments[22].
iii. Don't give yourself more login power than necessary. Don't stay logged in as an administrator any longer than needed[8].
iv. Avoid browsing, opening documents or other regular work activities while logged in as administrator[8].
v. Think twice before clicking. Dangerous hyperlinks can be expected via social networks or instant messengers, and the senders are likely to be people you trust, including your friends or colleagues.
vi. For Ransomware attack to be deploy, cybercriminals compromise their accounts and submit fake links to as many people as possible[23].
vii. Keep the Windows Firewall turned on and properly configured at all times. Enhance your protection more by setting up additional Firewall protection. Configure firewalls to block access to known malicious IP addresses[22].
viii. Place anti-virus and anti-malware programs to conduct regular scans[8].

IV. CONCLUSION

Ransomware families mostly focus on their evolution and characterization. The characterization of ransomware families is based on ransomware samples from ransomware families that have emerged over the last few years. Results show that a significant number of ransomware families exhibits very similar characteristics. With occurrences of ransomware on the rise, the encryption algorithms employed are becoming increasingly sophisticated. Ransomware will certainly continue to be a serious challenge for both information security professionals and researchers. CryptoDrop is an early-warning detection system that alerts a user during suspicious file activity. Windows, implementing practical defense mechanisms is possible, by continuously monitoring the file system activity and registry activity, so if these registry values are put under continuous observation then, detection of ransomware is possible.

REFERENCES

[1] P. Zavarsky and D. Lindskog, "Experimental Analysis of Ransomware on Windows and Android Platforms : Evolution and Characterization," vol. 94, pp. 465–472, 2016.
[2] H. Carter, P. Traynor, and K. R. B. Butler, "CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data," 2016.
[3] J. Scott and D. Spaniel, "ICIT Ransomware Report," 2016.
[4] S. Song, B. Kim, and S. Lee, "The Effective Ransomware Prevention Technique Using Process Monitoring on Android Platform," vol. 2016, 2016.
[5] D. Bekerman, B. Shapira, L. Rokach, A. Bar, and B. Sheva, "Unknown Malware Detection Using Network Traffic Classification," pp. 134–142, 2015.
[6] K. Zhao, D. Zhang, X. Su, W. Li, and E. Engineering, "Fest : A Feature Extraction and Selection Tool for Android Malware Detection," pp. 714–720, 2015.
[7] S. Brown, B. Henz, H. Brown, M. Edwards, M. Russell, and J. Mercurio, "Validation of Network Simulation Model with Emulation using Example Malware," pp. 1264–1269, 2015.
[8] P.Y. Networks, "Protecting Your Networks from Ransomware", U.S Government interagency technical guidance document aimed to inform chief information officres and chief information security officers at critical infrastructure entities.,2016.
[9] S. K. Sahay and A. Sharma, "Grouping the executables to detect malwares with high accuracy," *Procedia - Procedia Comput. Sci.*, vol. 78, no. December 2015, pp. 667–674, 2016.
[10] S. Zanero and F. M. B, "H EL D ROID : Dissecting and Detecting Mobile Ransomware," pp. 382–404, 2015.
[11] Anthony Ayodele, James Henrydoss, Walter Schrier, and T.E. Boult, "Study of Malware Threats Faced by the Typical Email User", Springer, 2011.
[12] Sunny Behal, Krishan Kumar, "An Experimental Analysis For Malware Detection Using Extrusions", International Conference on Computer & Communication Technology (ICCCT), IEEE, 2011.
[13] Zongqu Zhao, "A Virus Detection Scheme Based on Features of Control Flow Graph", IEEE, 2011.
[14] Mirosław Skrzewski, "Monitoring Malware Activity on the LAN Network", Springer, 2010.
[15] CHEN Chia-mei, LAI Gu-hsin, "Research on Classification of Malware Source Code", Springer, 2014.
[16] Ross Brewer, LogRhythm, "Ransomware attacks: detection, prevention and cure", September 2016.
[17] Byungho Min and Vijay Varadharajan, "Feature-Distributed Malware Attack:Risk and Defence", Springer, 2014.
[18] Anusha Damodaran, Fabio Di Troia, Corrado Aaron Visaggio, Thomas H. Austin, Mark Stamp, "A comparison of static, dynamic, and hybrid analysis for malware detection",Springer, 2015.
[19] Jose Andre Morales, Areej Al-Bataineh, Shouhuai Xu, and Ravi Sandhu, "Analyzing and Exploiting Network Behaviors of Malware", Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Springer, 2010.
[20] Mohamad Fadli Zolkipli and Aman Jantan, "A Framework for Defining Malware Behavior Using Run Time Analysis and Resource Monitoring", International Conference on Software Engineering and Computer Systems (ICSECS), Springer, 2011.
[21] Wen Wang, Xiaofeng Wang, Huabiao Lu, Jinshu Su, "Automatic Signature Analysis and Generation for Large-Scale Network Malware", IET International Conference on Information Science and Control Engineering 2012 (ICISCE), IEEE, 2012.
[22] Link: https://nakedsecurity.sophos.com/2016/03/24/8-tips-for-preventing-ransomware, visited on: 5 November 2016.
[23] Link: https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/22-ransomware-prevention-tips, visited on: 5 November 2016.
[24] Link: https://www.netfort.com/blog/methods-for-detecting-ransomware-activity/, visited on: 7 November, 2016.