International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-4, February 2020

Ransomware Threat, Attack, Prevention and Cure on Window Platform

Shubham Sharma, Satwinder Singh

Abstract*: With the advancement of digitization in every domain, the dependency of individuals on these digitized softwares has also increased. Although these softwares can perform storage, transfer, and security of digital media easily, the threat of hardware/software failure, data tapping and breaching data has always been there. Most of these threats have been introduced by the development of malicious softwares that can provide unauthorized access of machine's data. This malicious software was termed as malware. The development of any antimalware software to prevent the machine from malware triggers the attacker to generate new malicious operations to infect the machine. Ransomware is, however, a novel and one of the dangerous malware invented recently that restricts the user from accessing their system by locking the operating system files using strong encryption algorithms in the system unless and until a ransom is paid. Seeing the emergence of this ransomware threat and also the increasing usage of digital media, many techniques have been developed to detect the presence of different types of ransomware in different environments. Since the importance of developing techniques to prevent our machines from such attacks is increasing substantially, further research in the respective domain require thorough analysis of all the techniques that have been developed in this regard. This paper introduces the concept of ransomware and how it has been evolved. Along with various methods of handling the ransomware, thorough analysis of techniques that have been developed until now for the prevention and detection of different ransomwares is also performed. The analysis shows that there has been a big improvement in coding techniques utilized by ransomware which will eventually turn out a good detection system that considerably reduces the quantity of victim information loss.

Keywords: Ransomware attack, Security, Detection, Prevention and Cure

I. INTRODUCTION

Malware is a malicious software package or computer code which can infect the computer to destroy or lock your data. Ransomware is a specific type of malware [1] that restricts the access of machine's data to its own user and then demands a ransom to release the restriction.

Revised Manuscript Received on February 28, 2020.
***** Correspondence Author
Shubham Sharma*, Department of Computer Science & Technology (Cyber Security), Central University of Punjab, Bathinda, India. Email: jonusharma59@gmail.com
Satwinder Singh, Department of Computer Science & Technology (Cyber Security), Central University of Punjab, Bathinda, India. Email: satwinder.singh@cup.edu.in

The main difference between ransomware and malware is that, while a malware tries to remain hidden in your pc, laptop, computer just like a hidden file and do their work at backend without knowing the user or client and undetectable to the users, whereas ransomware upon encrypting your whole file which is in system and your PC, laptop and computer too is compromised, and tells the user of its presence [2]. However, the restriction or locking is performed using the encryption mechanism which encrypts the necessary information of the machine, computer, tablets or any kind of other electronic device. However, these encryption mechanisms were primarily developed to encrypt the user information for system security.

Ransomware attacks are rapidly growing in popularity and cybercriminals are earning to a great extent using these attacks. Businesses and individuals worldwide are currently under attack by ransomware [3]. According to the annual cybercrime report, businesses were targeted after every 14 seconds with ransomware in 2019 and this estimate will rise in 2021 by 11 seconds [4]. Usually, the amount of money that the victim pays as a ransom to decrypt or save their data from any kind of stealing canbe$300 to $700 or some time it can be increased $10,000 to $30,000 [5]. This payment is commonly requested in Bitcoin (a cryptocurrency payment system) or any other alternative invisible currency; which mostly depends on the location, local language, the language you are familiar with and your preference and suitability for traveling. However, sometimes even after paying the whole ransom, cybercriminals can break their promises of releasing the original version of data and disappear, leading to bigger losses. These types of attacks happen because of a lack of cyber security knowledge and consciousness of backing up important files by normal users. However, Ransomware-as-a-Service (RaaS) has emerged recently as the worst type of attack that allows nontechnical criminals to make attacks at a very low cost [6].

Ransomware usually operates by locking the desktop of the victim to render the system inaccessible to the user, or by encrypting, overwriting, or deleting the user's files from their storage drive. This is performed by first transferring the parent file of ransomware to perform all operations to the victim's computer either by using e-mail or online advertisements or some external drives. Some commonest ways employed by cybercriminals to unfold ransomware are Spam or fake email campaigns that contain malicious links or attachments; web traffic redirects to compromised websites; Drive-by downloads, infected softwares, contaminated external storage devices like USB drive, memory card, hard drive etc.

Sometimes, attacks also use remote desktop protocols like approaches that don't have confidence in any kind of user interaction. This parent file first creates a connection with the C&C server which provides keys for encrypting the stored data of the victim's computer. Once it receives the encryption key, 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. In addition to that, this malware deletes all the restore points, backup folders, and shadow volume copies from the victim's machine to fully hijack the PC and removing all ways of recovery. Once the victim's machine gets infected with ransomware and keys are transferred, theC&C server gains full control of the victim's machine. After that, the restriction is applied to the access of encrypted files to their original users followed by changing the desktop wallpaper notifying the user about ransomware attack along with steps to follow in order to get their access back[5].

Some security applications had already been employed on computing machines to prevent the machine from such malware which is based on the occurrence of suspicious activities occurring on the machine. Some of these suspicious activities, such as File System Activities (creation of too many shortcuts),Registry Activities (Servicing & process monitoring), Device control Communications (unnecessary communication with I/O device), Network Activity (random opening of new tabs), Locking mechanism (problem in data synchronization and backup), are demonstrated in Some of these methods were proposed to against ransomware, in Figure 1 will show you how and what security step can we take to sure our PC and Machine from a high-level ransomware attack in the future. However, this solution is only applied to the detected environment instead of a real situation. This paper summarized and classified the behavior of ransomware while doing file operation as indicators, and detected ransomware by monitoring and tracking those indicators. Even though these methods are advanced, but they cannot prevent loss completely.

These security features detect a ransomware attack and intimate that a machine is being infected with ransomware. These security features must keep on updating with respect to the new signatures of ransomware generated making it a necessity to develop new techniques for ransomware detection.

A. Evolution of Ransomware:-

Many variants of ransomware have created destruction in machines and caused a great loss of data till now. The evolution of malware or ransomware provides information about the different variants of ransomware created till now from the very beginning [5]. The beginning of network-based ransomware, crypto worm, purged the need for the human element in launching ransomware campaigns. The earliest windows ransomware which started to spread from days of their lease of first ransomware is performing destruction till now. After that, the second ransomware was introduced after a huge gap and then the generation of ransomware started with an approximate of one in a year. There is no reason to believe now that the evolution of ransomware is complete; its creators are continuously looking for new ways to enhance it.

ble1., however, demonstrates the annual growth of ransomware

Malware tends to evolve, with crooks adding new functions and techniques to assist it to avoid detection by antivirus programs. Evolution is rather rapid sometimes.

This ransomware timeline in

Table1.,indicates that the ransomware was not only for PCs and mobile devices targeted by ransomware attacks, but there are other devices that can also be attacked by ransomware. These devices might be directly or indirectly connected with the cyber web or the network like smart TVs, IoT devices (smart cities, smart phones, etc). An IoT device is still a major target for any kind of cyber attack due to its interconnection with the insecure networks which can be compromised easily. Some of the targeted IoT devices are wearable devices like fitness watches, and cloud-based systems like Dropbox, google drive one drive. Likewise, almost all of the operating systems have become vulnerable to these attacks, including Mac OS and Linux, Windows, Android. Such systems are vulnerable to both crypto-ransomware, and locker-ransomware attacks [8]. The categorization of ransomware with respect to its platform has been given here.

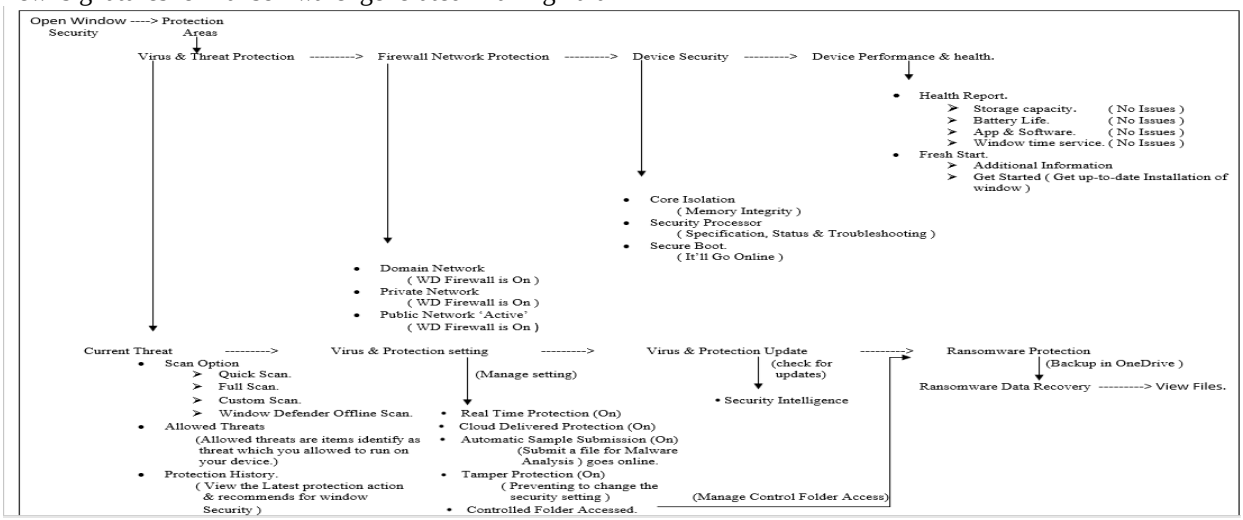

Figure 1 Steps to secure PC from ransomware (Folder(---->),Result (()),Window Defender (WD))

Table 1 Evolution of ransomware

Sr.No.	Year	Name Of Ransomware	Details
1).	1989	AIDS Trojan	Used symmetric cryptography; Infected 20,000 diskettes distributed at AIDS conference; Set in motion three decades of a ransomware attack
2).	2005	Archievus	Use asymmetric encryption; Encrypt everything in victim PC; Password is required to obtain a password to decrypt all files; Get password after paying the ransom
3).	2006	GPCode	Used a 660-bit RSA public key; An encrypted trojan spread via an email attachment asserting to be a job application
4).	2007	GPCode with multiple variants	Did not involve encryption, but simply locked out users andWinlock showed pornographic images until the users payto receive the unlocking code
5).	2008	Initially, GPCode virus created	A key was unleashed on the public using a 1,024-bit RSA key
6).	2011	Unnamed Trojan	Adoption of anonymous payment services
7).	2012	Reveton	Police-based Ransomware; Trojans show up; Responsible for scams that spread throughout
8).	2013	Cryptolocker	Cryptography malware spread by downloads from compromised links or show it professionally in the form of fake email attachments
9).	2014	CryptoDefense.	Used window in-built encryption; RSA encryption
		CryptoWall.	An improvised version of cryptoDefense; Uses Java vulnerability
		Sypeng.	Android-based Ransomware
		Koler	First ‘LockerWarm’
		CTB-Locker	Communicate directly with a C2 server through tor browser; Delete the shadow copies in Windows O.S.
		SimplLocker	Crypto based ransomware for android Devices that encrypt files; Phone is locked
Common Details	*At the End of 2014 — TorrentLocker, a new replacement of ransomware,wasintroducedwhich used the mechanisms of CryptoLocker and CryptoWall but with completely different source code from these. Concept of C-&C or C2- Command & Control came here.* *Early 2015 —CryptoWalloutreplacesCryptoLocker*		
10).	2015	LockerPin	Able to reset pin in Android phones
		TeslaCrypt	Allow persistence on the victim machine

		Chimera	Threatened to publish sensitive or private information & file or data online
		LowLevel04	Remote access, deleting the application, and all security & system logs
11).	2016	7ev3n	Demanded the highest ransom; Window system is destroyed in case of payment failure
		Ransomware32	First ransomware is written in javascript to work on multiple operating systems including window, Linux &macOS X
		SamSam (SAMAS)	Target JBoss server & include attacker communication in real-time with the victim via tor browser or onion website
		Locky	Spread through aggressive phishing &dridex infrastructure; used to target hospitals & other healthcare centers
		Petya	Delivered through dropbox; overwrite Master Boot Record (MBR) of victim Computer and encrypt the whole physical drive; If the ransom is not paid within a given time period it will get double
		KeRanger	First MacOSX ransomware signed via Mac development; allow to bypass or damage the Apple GateKeeper security parameters
		Jigsaw	First ransomware that deletes the file in every hour if ransom not paid; Automatic restart of PC results in deletion of all files
		Maktub	Use Crypter to hide & encrypt the source code of Malware
		CyrptXXX	Advice to Connect with Reveton ransomware variants; typically observed aftetbedep infection
		PowerWare	Introduce Power shell on OS discovered by Cb threat research (the main work in current window System to do the dirty work, attempts to write new files in disks & tries to stop or blend computer activities)
		ZCryptor	One of the first crypto-warm which infects the external devices & other systems over the network by encrypting all connected machines
Common Details		*Early 2016* —The first JavaScript-only Ransomware-As-A-Service (RaaS) was discovered. A new strain referred to as Ransom32 integrates a twist, having been completely developed in JavaScript, HTML, and CSS, that probably permits for multi-platform infections once repackaging for UNIX and Mac OS X. JavaScript made 'write-once-infect-all' threat*(Cb Threat- Cloud-based hunting threat)*possible	
		WannaCry	A worm is also known as WannaCrypt, Wana Decrypt0r 2.0, WanaCrypt0r 2.0, and WannaDecryptor; Network worm conjointly includes a "transport" mechanism to automatically spread itself.

12).	2017 [7]	ExPetr	Used encryption code that stops any decryption key from working; can notrecover encrypted data
Common Details	*Pre 2017* —Two large-scale epidemics triggering damage in the millions showed that ransomware could be used for purposes other than extortion		
13).	2018 [7]	SynAck	Applying a process duplication method known as Process Doppelganging; contain complex mechanisms to counter protection technologies; Avoids detection with unprecedented effectiveness
11).	2016	7ev3n	Demanded the highest ransom; Window system is destroyed in case of payment failure
		Ransomware32	First ransomware is written in javascript to work on multiple operating systems including window, Linux &macOS X
		SamSam (SAMAS)	Target JBoss server & include attacker communication in real-time with the victim via tor browser or onion website
		Locky	Spread through aggressive phishing &dridex infrastructure; used to target hospitals & other healthcare centers
		Petya	Delivered through dropbox; overwrite Master Boot Record (MBR) of victim Computer and encrypt the whole physical drive; If the ransom is not paid within a given time period it will get double
		KeRanger	First MacOSX ransomware signed via Mac development; allow to bypass or damage the Apple GateKeeper security parameters
		Jigsaw	First ransomware that deletes the file in every hour if ransom not paid; Automatic restart of PC results in deletion of all files
		Maktub	Use Crypter to hide & encrypt the source code of Malware
		CyrptXXX	Advice to Connect with Reveton ransomware variants; typically observed after the infection
		PowerWare	Introduce Power shell on OS discovered by Cb threat research (the main work in current window System to do the dirty work, attempts to write new files in disks & tries to stop or blend computer activities)
		ZCryptor	One of the first crypto-warm which infects the external devices & other systems over the network by encrypting all connected machines
Common Details	*Early 2016 —The first JavaScript-only Ransomware-As-A-Service (RaaS) was discovered.* *A new strain referred to as Ransom32 integrates a twist, having been completely developed in JavaScript, HTML, and CSS, that probably permits for multi-platform infections once repackaging for UNIX and Mac OS X. JavaScript made 'write-once-infect-all' threat(Cb Threat- Cloud-based hunting threat)*possible		

		WannaCry	A worm is also known as WannaCrypt, Wana Decrypt0r 2.0, WanaCrypt0r 2.0, and WannaDecryptor; Network worm conjointly includes a "transport" mechanism to automatically spread itself.
12).	2017 [7]	ExPetr	Used encryption code that stops any decryption key from working; can notrecover encrypted data
Common Details	*Pre 2017* —Two large-scale epidemics triggering damage in the millions showed that ransomware could be used for purposes other than extortion		
13).	2018 [7]	SynAck	Applying a process duplication method known as Process Doppelganging; contain complex mechanisms to counter protection technologies; Avoids detection with unprecedented effectiveness

- PC ransomware.
  - Window ransomware.
  - macOS ransomware.
  - Linux ransomware.
- Mobile ransomware.
  - Android ransomware.
  - IOS ransomware.
  - Window ransomware too.
- IoT based ransomware.
  - Smart Watches
  - Smart TVs
  - Smart Cities.
- Cloud-based ransomware.
  - Google drive
  - Dropbox
  - One drive.

Some of the ransomware is Location-based ransomware that targets the computer through Google adds on, online fake advertisement and so on. Ransomware could be a variety of malware that restricts access to the infected (ADPS) automatic data processing system which means it can be processed your data without your permission or without providing any kind of executive command by the user, client to run & execute their data. It can be processed unwantedly without knowing anything that what actually is happening or happened to your PC or any electronic devices. This is a form of technological or technical blackmail that exploits software and hardware vulnerabilities, sometimes, in your devices via drive-by attacks on maliciously crafted web pages. It comes in the form of a Crypto locker or CryptoWall. They employed strong encryption algorithms to scramble nearly every files they targeted, mostly in document storage formats such as office, PDF and all other data like- image personal documents, bank detail documents, etc making them impossible to recover without the unique, or private key used to encrypt them. The cracker then puts up a show note on your Victim Computer screen explaining the processes to follow to recover the decrypted all files when payment which is able to mark the top.

B. Phases of Ransomware Attack:-

There are distinct phases of a ransomware attack, whether it is a mass distribution or a targeted attack. Understanding each action performed by ransomware on targeted machine and knowing the indications of compromise (IOCs) to appear for, will increase the ability to successfully defend against the attack or at least mitigate the effects of an attack. These events occurring in the machine due to ransomware are categorized into five different phases as given below:-

Phase 1:-Exploitation & Infection
Phase 2:- Delivery & Execution.
Phase 3:-Back-up Spoliation.
Phase 4:-File Encryption.
Phase 5:-User Notification & clean-up.

II. METHODOLOGY OF HANDLING RANSOMWARE ATTACKS

Ransomware kits on the deep network have allowed cybercriminals to use a software package tool to form ransomware with some specific capabilities. Attackers can then generate a very dangerous type of malware for their own distribution with ransoms paid to their bitcoin accounts. As with a lot of the remainder of the IT world, it's currently potential for those with very little or no technical background knowledge and experience to order up cheap ransomware-as-a-service (RaaS) and launch attacks with minimal effort. In one RaaS situation, the supplier collects the demanded extortion money and takes a share before distributing the return to the service user by providing a decryption key to take full access again. Some examples of attacks performed by ransomware include:-

- Email Attachments:- A fake e-mail is sent to the victim with an offer of some kind of money price etc.
- Social media messages:- Malware file is sent to victim through some pictures, images or other media attachments.
- Pop-ups:- The malware file can be downloaded into the machine through the fake information, usually related to new software, spread through different popups.

A. Operation of ransomware attacks

Ransomware attacks are usually administered by employing a Trojan, coming into a system through, for instance, a malicious attachment, embedded link during a Phishing email, or a vulnerability in an exceedingly network service. The program then runs a payload, which locks the system in some fashion or claims to lock the system. The attackers, however, get a ransom or extortion money by using one of the three ways or protocols discussed here.

- Attacker to Victim:- Attacker performs the attack on victim's machine& encrypt the whole data of the same& ask the victim to pay some ransom in form of crypto currency or bitcoins accounts to decrypt data again
- Victim to Attacker:- If the data is important or discrete then the victim definitely pays the ransom or extortion money to attacker in the form they want.
- Attacker to Victim:- After payment of demanded ransom or extortion, it is expected from the attacker that he/she will provide a decryption key but sometimes the attacker does not keep the promise.

B. Prevention of ransomware attacks

A variety of procedures and policies have been adopted to address and identify the problem of ransomware to prevent the introduction of ransomware into the machine. These different prevention approaches have been proposed in several studies to protect the machine and its data from being victimized and blackmailed via ransomware [5, 8].

Authors in [9, 10] provided several preventive measures to avoid the introduction of ransomware into the machine. Some of the ways demonstrated in Figure 1states several ways of securing the machine or protecting the data from a ransomware attack by keeping windows firewall on or some other means. Some common precautionary measures are discussed in some points given here.

- Back up your data regularly and keep one of those backup copies off-site. Backups will defend your data, information against ransomware or any other kind of other malicious attack. Make sure to encode your backed-up data or information so that only you will be able to restore it.
- Be very careful about opening unsolicited attachments received through e-mail.
- Keep the windows firewall or window defender firewall always turned on and properly organized.
- Enhance the protection level of the machine by employing trustworthy antivirus software and third-party Firewall protection.
- Configure firewalls to restrict access to well-known malicious IP addresses.
- Place strong antivirus and antimalware programs to conduct regular scans.
- Update software and operating systems with the latest patches.
- Never click on links or open attachments in uninvited emails.
- Follow safe practices when browsing the internet over the network.
- Prevention is essential because it will keep your machine safe. It is recommended for every user to stay on reliable multilayer protection security solutions.

C. Detection of Ransomware

Numerous techniques have been proposed in the literature since its origin for the detection of ransomware and have also been surveyed in [5], [11] and more. This paper provides a detailed overview of all these techniques along with the datasets used to evaluate those techniques and their evaluation performance too. Unlike previous papers, this paper classified all these techniques corresponding to the type of features examined as explained in this section for analyzing file type/content and connection respectively. Summarization of respective techniques is provided in tabular form also.

1. File Type and Content Monitoring for Detection:

The foremost technique to detect ransomware was proposed in [12] where the author monitors abnormal file system activities. While examining file system activities for a variety of ransomware samples, the author found that monitoring of I/O requests makes the prevention and detection of ransomware attacks possible by protecting Master File Table (MFT) in NTFS file system. The majority of ransomware attacks observed during the period 2006 to 2014 were observed in the respective paper. From 15 different families, 1359 different ransomware were selected from Anubis and other different repositories. Moreover, the technique also analyzed charging methods through which a victim was supposed to pay a ransom amount. Generally, bitcoins are adopted as a charging method due to its efficient privacy mechanism. However, the author did not provide any numerical results.

Since JPEG files are supposed to represent the most valuable data from the computing machine, the main focus in [13] was given to JPEG files. The author, here, distinguish between the original and encrypted version of JPEG files with high entropy using some differentiation measures to detect TorrentLocker ransomware. These adopted measures were Shannon entropy and Kullback-Leibler (KBL) divergence; KBL divergence is also known as relative entropy. While Shannon entropy measures the uncertainty associated with a variable, the KBL divergence measures the distance between two probability distributions over a random variable. The author found, from experimentation, that Shannon entropy could not efficiently distinguish between original JPEG and encrypted JPEG files as JPEG files are already compressed and have some compression artifacts. KBL divergence was thereby used for the said objective and threshold for the same was selected based on the accuracy rate. The dataset utilized by the author was composed of a total of 4000 files, out of which 2000 are original JPEG and rest are encrypted using the AES-256 algorithm. However, the maximum detection accuracy of the proposed technique was found to be 99.95%.

In [6], the authors developed a new technique named 'POSTER' in 2017 to detect crypto-ransomware.

Since crypto-ransomware use to find files in the system and then encrypt those files in the same search order, this approach was designed with respect to the behavior of file traversal.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

In this method, two window APIs, FindFirstFile and FindNextFile are invoked in sequence; FindFirstFile starts the search of a specific file and FindNextFile continues the search of that file afterward. In this search path, some decoy files are created having file extensions that are easily targeted by ransomware. However, the two API's used here returns the name of only decoy files on the path which are then analyzed using decoy file monitor by comparing Shannon entropy between original and manipulated file. This approach was found to generate no loss and that too with less cost because only decoy files are monitored first instead of real files. Moreover, these operations did not consume much time. This approach was tested on Locky ransomware, however, the author did not provide any numerical results.

Crypto-drop, an early warning system, was proposed by authors in [14], that can halt a process and alerts a user after any suspicious file operation is found to occur in the system. Instead of searching for a program that is making changes in the system, this technique monitors all the changes in the data to detect suspicious transformation. One such transformation is the bulk modification of file types. Another suspicious modification monitored in this technique is similarity between the original file and ransomware encrypted version of that file using hash value. Shannon entropy is the third primary indicator for the early detection of ransomware. However, the number of files created by injecting a specific file or application and bulk deletion of files are also used as secondary indicators for the same. The union of these primary indicators generates a reputation score which is then compared with the threshold to ensure the existence of malware. This technique provided 100% accuracy after testing on 492 real-world ransomware samples. However, the author in this paper stated the limitation that this technique can't specify whether these suspicious transformations are performed because of ransomware or by the user only.

The technique proposed in [15], 'RDware' (Ran-Detect-Ware), is based on the idea that encryption of host files using ransomware changes the type of file extensions. This hybrid approach utilized a set of behavioral indicators for analyzing manipulations in a file type. This technique also analyzedthepattern of the Windows API call sequence to classify ransomware infected pattern from a benign file pattern. Here, changes in file type and file content of the original and encrypted version are tested using AnalyzeIT [1] and Win-Merge [2] software's available on the internet. Moreover, the Windows API call sequence is analyzed using Detours libraries [16], which is also available on the internet. This technique was tested using 300 ransomware samples collected from four different websites, type and authenticity of which were first analyzed in VirusTotal. However, the author in this paper created his own ransomware too to analyze the working which was tested in VirusTotal and Windows Defender and classified as ransomware. The technique can be further extended by analyzing more indicators like entropy change and by analyzing dynamic malware at the kernel level.

Honey-pot Based Approach

In [17], the author deployed a honeypot folder containing tripwire files that are supposed to be more likely infected by ransomware. The aim of the honeypot based technique is to attract the attention of ransomware towards a specific location so that monitoring of any change would be constrained to that location only. So, the authors in this paper used the file screening service of Microsoft File Server Resource Manager (FSRM) to monitor changes in the honeypot folder. After that, EventSentry was used further to monitor windows security logs. Moreover, a particular action was performed by this proposed technique to alert the user and protect the machine based on the severity of attack ransomware has incurred. Since ransomware or any malware can attack any folder in the machine, this technique was not proved to be much effective because of monitoring manipulations in a limited area i.e. in a honeypot created folder only.

Machine-Learning Based Approach

As compared to analyze files using a few features, machine-learning-based classification has started been using to detect ransomware where a large and effective set of features is selected to classify ransomware infected and benign files.

In 2016, authors in [2] proposed a machine learning-based approach for ransomware detection by training the machine using different API call sequences, registry keys, file or directory operations. In the meantime, another author [18] utilized features based on file characteristic operations to train a machine for the detection of ransomware.

However, a deep learning-based ransomware detection scheme proposed in [2] by authors utilized MultiLayer Perceptron (MLP) for classification with a learning rate of 0.1. Different architectures of MLP were proposed here with one, two or three layers for determining the best one to detect ransomware. However, these different architectures were trained with the frequency of API calls, which was estimated using Cuckoo Sandbox logs. To prove the effectiveness of this technique, other shallow networks are also trained with the same feature set and are then compared with the proposed deep network MLP. A thorough analysis performed by authors proved SVM and MLP to be the most accurate having AUC of 1.0. Moreover, it was found that the MLP network with three layers provides more information with the inference that Cryptolocker and Cryptowall ransomware have similar behaviors and therefore, difficult to be distinguished. These results can be enhanced using more complex architecture.

Afterward, a machine learning-based approach was proposed by authors in 2018 in [19]. This technique utilized SVM classifier for the classification of ransomware infected files from benign software. However, learning of classifiers was done using API calls history as a feature. The author, in [18], stated the limitation of previously proposed API call based technique that execution of two different programs may result in the same API log sequence and hence, difficult to be classified. Rather than the presence of a possible combination of API call sequence for a particular program,

The technique proposed here compute the number of times a particular combination of API calls appears in the sequence. This count, however, was then represented in the form of vector. These vectors were then converted to a standardized vector representation using mean and variance.

[1]AnalyzeIT. http://www.shockingsoft.com/AnalyzeIt.html
[2]WinMerge. http://winmerge.org/

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

However, SVM was trained using these standardized vectors for each program either malicious or uninfected. This technique was tested using 312 goodware and 276 ransomware samples which are targeted on windows platform, out of which 294 logs are used for training and 294 for testing. After performing a number of experiments, the highest accuracy of the proposed technique was found to be 97.48%.

In the meantime, another approach was proposed with the name 'DRTHIS' (Deep Ransomware Threat Hunting and Intelligence System) [20] which utilizes two deep learning networks, Convolutional Neural Network (CNN) and Long Short Term Memory (LSTM)) for classification of infected files from benign ones. The proposed technique was tested using Locky, Cerber and TeslaCrypt ransomware samples where 220 samples are included for each category. In this technique, the frequency of occurrence of a sequence of events with respect to a particular execution was represented as a feature vector and these two networks were trained using these networks. However, the F-measure and True Positive Rate of the proposed technique, after testing, was found to be 99.6% and 97.2% respectively. Moreover, the proposed technique correctly classifies unknown ransomware samples also i.e. 99% of Crypto Wall samples, 75% of Torrent Locker samples and 92% of Sage Samples.

Furthermore, an early detection system was proposed by authors in [21] to detect crypto-ransomware. Here, API calls were analyzed from the pre-encryption data from the runtime code of malicious code for early detection. The next phase categorizes the API calls based on the resource on which they are working and puts the API calls working on the same resource into the same groups. However, the classifying feature is obtained by calculating the frequency of these API's. The author, here, did not provide any experimental details.

Table 2 File type and content monitoring detection techniques

Paper	Technique	Features	Ransomware detected	Result
[12] (2015)	Monitoring I/O requests	Abnormal file system activities	1359 ransomware from 15 different families	No numerical results
[13] (2016)	KBL Divergence	Original and encrypted JPEG files	TorrentLocker	99.95%
[6] POSTER (2017)	API's FindFirstFile and FindNextFile to find decoy files	File extension based analysis	Crypto-ransomware (Locky)	No numerical results
[14] Crypto-drop (2016)	Reputation score computed using the union of primary indicators	File type modification, different encrypted version, Shannon entropy	492 samples from 14 families	Accuracy-100%
[15] (2019) RDWare	AnalyzeIT&WinMergeSoftwares Detours Libraries	File type manipulation and Windows API call sequence	300 ransomware samples from 4 different sites Author's own created ransomware	No results are given
[17] (2016)	Honeypot based approach	FSRM to monitor file change EventSentry	No information	No analysis
[2] (2016)	Machine learning using SVM and MLP	API call sequence, registry keys, file operations	7 different ransomware families	Accuracy: 1.0 (MLP) Accuracy: 0.98 (SVM)
[18] (2016)	Machine learning	File characteristic operations	582 ransomware and 942 goodware samples from 11 families	AUC (Area Under ROC): 0.995
[19] (2018)	SVM Classifier	Windows API call sequence	312 goodware and 276 ransomware samples	Accuracy-97.48%
[20] (2019) DRTHIS	LSTM and CNN classifier	Frequency of occurrence of each event	Locky, CerberandTeslaCrypt ransomware samples	F-measure- 99.6% TPR- 97.2%
[21] (2018)	Classifier	Similar API's and frequency of each	Crypto ransomware	No quantitative analysis

[22] (2019)	Classification using different behavioral indicators	Prevention using BitLocker encryption	DARPA IDS assessment dataset	76.6% accuracy
[23] (2018) RansomWall	Honeypot approach Classification	Static and dynamic features	574 samples from 12 ransomware families (VirusShare)	98.25% TPR with Gradient Tree Boosting Classifier

Recently, in 2019, authors in [22] analyzed the performance of five different machine learning classifiers by training them with the same set of behavioral indicators. However, different classifiers analyzed were Linear Regression, Adaboost, Random Forest, Extra Trees, Gradient Boost, Multi-Layer Perceptron and among these, Gradient Boost Algorithm was found the best for classifying ransomware samples from original ones. In addition, another module for the prevention of ransomware attacks was introduced in this attack. This technique is based on encryption discharged by Microsoft Corporation which uses AES encryption with 128 or 256 length keys and termed as 'BitLocker Driven Encryption'. This encryption scheme prevents the data in the drive from being seen by other users. However, the specified classifiers were tested on the DARPA IDS assessment dataset.

Hybrid Approach

A hybrid approach for ransomware detection was proposed in 2018 which combines the static and dynamic type of analysis; an approach was termed as RansomWall [23]. Static analysis is performed by digital signature verification using WinVerifyTrust [3] API of Windows, the presence of cryptos/packers using the PEiD [4] tool and analyzing suspicious strings using the FLOSS[5] tool. In addition to this, the honey trap was set by detection scheme which sets some folders and files by itself to be attacked by ransomware. This trap layer keeps track of those files and folders and any deletion in shadow copies and any registry modifications. On the other hand, dynamic analysis is done by analyzing changes in file extensions or file creation or deletion and higher entropy. All these features for some samples were, then, fed into the machine learning classifier for training and some samples are set for testing. This paper also proposed a technique for file backup of files that are considered suspicious. The dataset, on which this technique is analyzed, consists of 574 samples from 12 ransomware families and 442 benign samples; this data is collected from VirusShare. A thorough analysis of selected feature set using different machine learning classifiers on different ransomware families generated the best TPR of 98.25% with the Gradient Tree Boosting Classifier algorithm.

2. **Connection Monitoring for Detection:**

Almost every family of ransomware, when it starts execution, tries to connect with the C&C server for exchange of public or private keys to encrypt or lock the data on an infected machine. Some authors utilized this idea to detect ransomware and made such techniques that are able to distinguish network traffic when a machine is infected from the one when the machine is not infected. Some of these techniques are provided in this section. However, techniques that are developed by training classifiers using network traffic features are categorized separately.

The technique proposed by authors in [24] was found to be the first technique to detect ransomware by monitoring network connection of infected computers with the C&C server through which the machine got infected. This technique is used to detect High Survivable Ransomware (HSR) and is termed as CM & CB (Connection Monitor and Connection Breaker) technique. A machine encrypted using High Survivable Ransomware can be decrypted only by the C&C server through which the whole data has been encrypted. However, the decryption key of one machine is not the same as other if HSR ransomware is used. Since all the addresses requiring network connectivity to connect to any server must be verified by Certification Authority (CA), this technique checks the connectivity which has not been verified by CA and considers that connection as suspicious. However, network connectivity is also required for connecting injected ransomware with the C&C server to exchange public and private keys for encrypting data. After testing this technique on 20 unknown ransomware samples, it was found that this technique can detect HSR before encryption is performed with 100% accuracy. This ransomware for testing is selected from *malwaretips*[6] and *bleepingcomputer*[7] available on the internet. In addition, to prevent only HSR type of ransomware, this technique could be able to detect other malicious software also. Since this technique uses an only key-exchange feature of HSR, another HSR feature can be used in the future to detect unknown ransomware.

Machine-Learning Based Approach

In [25], a machine learning-based technique was introduced, called NetConverse, which analyzing features of network traffic after ransomware infection. These network traffic features from these samples are extracted using Wireshark, which were then fed into different classifiers using WEKA tool. This technique was tested by analyzing network traffic of 201 ransomware and 264 goodware samples from 9 and 3 families respectively. Among 6 different classifiers used, J48 Decision tree classifier provided the best accuracy of 97.10% followed by 96.8% accuracy with LMT classifier and so on.

A new machine learning-based technique was introduced in [26] which used multiple classifiers to detect crypto-ransomware; one classifier is used at the packet level

[3] https://msdn.microsoft.com/en-us/library/windows/desktop/aa388208(v=vs.85).aspx
[4] http://www.softpedia.com/get/Programming/Packers-Crypters-Protectors/PEiD-updated.shtml
[5] https://www.fireeye.com/blog/threat-research/2016/06/automatically-extracting-obfuscated-strings.html
[6] www.malwaretips.com
[7] www.bleepingcomputer.com

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

Table 3 Connection monitoring detection technique

Paper	Technique	Features	Ransomware detected	Result
[24] CM&CB -2015	Connection monitoring with C&C server	Key exchange feature	20 unknown samples from malwaretips and bleepingcomputer	Accuracy-100%
[25] -2018 NetConverse	6 different classifiers (Decision Tree best)	Network traffic features	201 ransomware and 264 goodware samples	97.10% with Decision Tree (J48)
[26] -2019	Multi-Classifier approach	Network traffic features	Locky ransomware	97.5 % accuracy

of the network while the other at flow level of the network. However, these classifiers were trained using network traffic features analyzed from Locky ransomware. A testbed environment was set up by the author to create a dataset where one PC was used to capture the network traffic using Wireshark from the other two infected PC's which were infected using Locky ransomware. These infected PCs were supposed to make a connection with the C&C server altering the expected network traffic pattern which was used as a feature then. However, 18 features, in total, were collected from these traffic protocols i.e. TCP (Transmission Control Protocol), HTTP (HyperText Transfer Protocol), DNS (Domain Name Service) and NBNS (NETBIOS Name Service). After analyzing the performance of different classifiers by training them with the extracted features using Weka tool, the best accuracy was found to be 97.92% and 97.08% for Random Tree classifier (packet-based) and Bayes Net classifier (flow-based) respectively.

Since ransomware or any malware were meant to attack any kind of operating system, some techniques to detect ransomware on the Android operating system were also proposed [10, 27]. Not only a different operating system or device, ransomware can affect online storage along with offline or IoT devices along with simple computing devices also. However, ransomware detection techniques have also been proposed for the same [28, 29]. Although most of the techniques developed to detect a particular type of ransomware were found to have good accuracy, a full-fledged technique has not been developed yet to detect all ransomware because of frequent updation of ransomware signature.

III. RESULTS

This paper provides a brief overview of various ransomwares proposed till now along with some methodologies to detect them. Some of these techniques are based on analyzing the contents of new files created or a sequence of API's called on the introduction of ransomware while some techniques focused on a new network connection created by the victim computer with a specified C&C server, as discussed in the paper. Some of the best techniques, to the best of author's knowledge, found for the detection of ransomware are given in Table 4.

Table 4 Comparison of some techniques

Paper	Technique	Result
[14]	File type analysis	Accuracy: 100%
[20]	Machine learning on event frequency	F-measure: 99.6%
[24]	Key exchange over network	Accuracy: 100%

Although the techniques demonstrated in Table 4 are found having best accuracy and performance, but they test their technique under some constraints. For instance, the author in [14] could not distinguish between user generated content and ransomware generated content while the author in [20] and [24] tested their technique on limited set of data. However, a technique should be proposed that could detect any type of malicious operations occurring in the computer to detect any ransomware, either known or unknown. And there should be sufficient methodology to consider any relation as malicious also.

IV. CONCLUSION AND FUTURE DISCUSSION

With advancements in the digital world, means to protect and secure digital data have also increased. Since this protection can be easily compromised using different ransomware or malware developed by professionals for their own financial or organizational benefit, detection mechanisms must be there to prevent or detect such malwares. This paper provides a detailed overview of most of the ransomware detection techniques which are classified based on the type of features being analyzed for detection. One set of techniques examined file type and file content for ransomware detection while another set analyzed connection set up by ransomware file with C&C server. Thorough analysis of most of the techniques performed in this paper revealed that the technique proposed in [24] was found to provide the best detection accuracy but on a relatively small number of ransomware samples. On the other hand, techniques proposed in [14], [20] and [23] were found to provide good detection accuracy on a large variety of ransomware samples. As every new technique detected different type of ransomware, a framework or technique should be developed that can cope up with the continuously updating ransomware signatures.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

Moreover, these detection techniques have been proposed for windows operating system only, Linux environments should also be explored though more secure.

However, an individual should have the proper knowledge about such kind of malicious attacks and should be careful while working over the network and follow precautionary measures to prevent the machine from being attacked. Preventive measure should be taken before ransomwares established strong hold on your machine.

REFERENCES

1. https://searchsecurity.techtarget.com/definition/ransomware
2. Vinayakumar, R., Soman, K. P., Velan, K. S., &Ganorkar, S. (2017, September). Evaluating shallow and deep networks for ransomware detection and classification. In *2017 International Conference on Advances in Computing, Communications, and Informatics (ICACCI)* (pp. 259-265). IEEE.
3. Tailor, J. P., & Patel, A. D. (2017). A comprehensive survey: ransomware attacks prevention, monitoring and damage control. *Int. J. Res. Sci. Innov*, *4*, 2321-2705.
4. https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf
5. Al-rimy, B. A. S., Maarof, M. A., &Shaid, S. Z. M. (2018). Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. *Computers & Security*, *74*, 144-166.
6. Feng, Y., Liu, C., & Liu, B. (2017). Poster: a new approach to detecting ransomware with deception. In *38th IEEE Symposium on Security and Privacy Workshops*.
7. https://www.kaspersky.co.in/blog/evolution-of-ransomware/13450/
8. Brewer, R. (2016). Ransomware attacks: detection, prevention, and cure. *Network Security*, *2016*(9), 5-9.
9. Mohurle, S., & Patil, M. (2017). A brief study of wannacry threat: Ransomware attack 2017. *International Journal of Advanced Research in Computer Science*, *8*(5).
10. Andronio, S. Zanero, and F. Maggi, "HelDroid: dissecting and detecting mobile ransomware," 2015, in Research in Attacks, Intrusions, and Defenses, vol. 9404 of Lecture Notes in Computer Science, pp. 382–404, Springer.
11. TTandon, A., & Nayyar, A. (2019). A Comprehensive Survey on Ransomware Attack: A Growing Havoc Cyberthreat. In *Data Management, Analytics and Innovation* (pp. 403-420). Springer, Singapore.
12. Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., &Kirda, E. (2015, July). Cutting the gordian knot: A look under the hood of ransomware attacks. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment* (pp. 3-24). Springer, Cham.
13. Mbol, F., Robert, J. M., &Sadighian, A. (2016, November). An efficient approach to detect torrentlocker ransomware in computer systems.*InInternational Conference on Cryptology and Network Security* (pp. 532-541). Springer, Cham.
14. Scaife, N., Carter, H., Traynor, P., & Butler, K. R. (2016, June). Cryptolock (and drop it): stopping ransomware attacks on user data. In *2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS)* (pp. 303-312). IEEE.
15. Sharma, H., & Kant, S. (2019). Early Detection of Ransomware by Indicator Analysis and WinAPI Call Sequence Pattern. In *Information and Communication Technology for Intelligent Systems* (pp. 201-211). Springer, Singapore.
16. Detours. https://www.microsoft.com/en-us/research/project/detours/
17. Moore, C. (2016, August). Detecting ransomware with honeypot techniques. In *2016 Cybersecurity and Cyberforensics Conference (CCC)* (pp. 77-81). IEEE.
18. Sgandurra, D., Muñoz-González, L., Mohsen, R., &Lupu, E. C. (2016). Automated dynamic analysis of ransomware: Benefits, limitations, and use for detection. *arXiv preprint arXiv:1609.03020*.
19. Takeuchi, Y., Sakai, K., & Fukumoto, S. (2018, August). Detecting ransomware using support vector machines. In *Proceedings of the 47th International Conference on Parallel Processing Companion* (p. 1). ACM.
20. Homayoun, S., Dehghantanha, A., Ahmadzadeh, M., Hashemi, S., Khayami, R., Choo, K. K. R., & Newton, D. E. (2019). DRTHIS: Deep ransomware threat hunting and intelligence system at the fog layer. *Future Generation Computer Systems*, *90*, 94-104.
21. AI-rimy, B. A. S., Maarof, M. A., &Shaid, S. Z. M. (2017, April). A 0-day aware crypto-ransomware early behavioral detection framework. In *International Conference of Reliable Information and Communication Technology* (pp. 758-766). Springer, Cham.
22. Abraham J.A. & George S.M. (2019). Preventing Crypto-Ransomware Using Machine Learning. International Journal of Computer Science and Network (IJCSN), 8(3), 285-293.
23. Shaukat, S. K., & Ribeiro, V. J. (2018, January). RansomWall: A layered defense system against cryptographic ransomware attacks using machine learning. In *2018 10th International Conference on Communication Systems & Networks (COMSNETS)* (pp. 356-363). IEEE.
24. Ahmadian, M. M., Shahriari, H. R., &Ghaffarian, S. M. (2015, September). Connection-monitor & connection-breaker: A novel approach for prevention and detection of high survivable ransomware. In *2015 12th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC)* (pp. 79-84). IEEE.
25. Alhawi, O. M., Baldwin, J., &Dehghantanha, A. (2018). Leveraging machine learning techniques for windows ransomware network traffic detection. In *Cyber Threat Intelligence* (pp. 93-106). Springer, Cham.
26. Almashhadani, A. O., Kaiiali, M., Sezer, S., & O'Kane, P. (2019). A Multi-Classifier Network-Based Crypto-Ransomware Detection System: A Case Study of Locky Ransomware. *IEEE Access*, *7*, 47053-47067.
27. Scalas, M., Maiorca, D., Mercaldo, F., Visaggio, C. A., Martinelli, F., &Giacinto, G. (2019). On the Effectiveness of System API-Related Information for Android Ransomware Detection. *Computers & Security*.
28. Lee, J.K., Moon, S.Y. & Park, J.H. J Supercomput (2016). CloudRPS: a cloud analysis based enhanced ransomware prevention system
29. Azmoodeh, A., Dehghantanha, A., Conti, M., & Choo, K. K. R. (2018). Detecting crypto-ransomware in IoT networks based on energy consumption footprint. *Journal of Ambient Intelligence and Humanized Computing*, *9*(4), 1141-1152.

AUTHORS PROFILE

Shubham Sharma is a PG-scholar in Department of Computer Science and Technology (Cyber Security), Central University of Punjab, Bathinda. He got his bachelors degree (B.Tech.) in Computer Science and Engineering from Himachal Pradesh Technical University, Hamirpur. He is currently working in the domain of malware analysis and detection with special emphasis on ransomware detection.

Dr. Satwinder Singh is an Assistant Professor in Department of Computer Science and Technology, Central University of Punjab, Bathinda. He did his PhD and M.Tech. from GNDU, Amritsar in year 2014 and 2004 respectively. Dr. Singh is currently working in the area of data mining and software engineering and has over 35 publications in international and national journals.