# A Review on Ransomware Prevention Technique

**Rima A. Patel**
Department of Computer Engineering
Vadodara Institute of Engineering, Kotambi, Vadodara, India

*Abstract*— Ransomware is a type of malware which takes the access of the user's system before user notices. It can also damage the user's system. Now a days due to increase rate of this kind of attacks, the effective prevention techniques are required. This paper represents the different types of prevention techniques which is vulnerable to ransomware. The system will identify the abnormal behavior of the process and if any suspected file is detected then the system will take the necessary steps to stop the process.

***Key words:*** Ransomware, Malware, Prevention Technique

## I. INTRODUCTION

Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid[1]. The first cases of ransomware first infection were first seen in Russia between 2005 and 2006. One of earliest reports on ransomware discussed a variant that compresses then password-protects certain files in a victim's computer.[2] It also left a file that served as ransom note to ask the victim for US$300 in exchange for his files. In the threat's early stages, .DOC, .XLS, .JPG, .ZIP, .PDF, and other commonly used files were held hostage. Later on, variants that could infect mobile phones3 and even computers' Master Boot Record (MBR),4 preventing the OS from loading, emerged. By 2012, ransomware made its way from Russia across other European countries.5 This could be a result of the clampdown on fake antivirus (FAKEAV) and so cybercriminals had to look for another means to continue profiting from unwitting victims.6 Ransomware operators started coming up with new tactics to spread the threat. A popular ruse at that time was introduced by Reveton7 —impersonating law enforcement agencies and threatening victims by implicating them with online crimes. Ransomware operators also experimented with the use of various payment methods, including Ukash, paysafecard, and MoneyPak, to limit their monetary trail. FAKEAV variants typically scare users into doling out cash with fake alerts touting computer infection ! 1 Early ransomware variants scared users with screen lockouts 2 Today's ransomware variants not only lock users out of their systems but also threaten to delete all of their files if they do not pay the ransom. n late 2013, what we know now as "crypto-ransomware" led by variants like CryptoLocker8 came to the fore. This threat no longer just encrypted files, it started deleting files if victims refused to pay. To get files back, victims were asked to pay varying ransom amounts in the form of Bitcoins in exchange for a decryption key. Since the introduction of crypto-ransomware, cybercriminals increasingly took steps to more effectively extort money from victims—individuals and businesses (regardless of size) alike from virtually any part of the world.[3]

Fig. 1.1: FAKEAV

FAKEAV variants typically scare users into doling out cash with fake alerts touting computer infection

Fig. 1.2: Ransomware Variants

Early ransomware variants scared users with screen lockouts. They lock the system of user and gets all the access of the system.

Fig. 1.2: Ransomware Variants

Today's ransomware variants not only lock users out of their systems but also threaten to delete all of their files if they do not pay the ransom.

## II. SYMPTOMS OF RANSOMEWARE

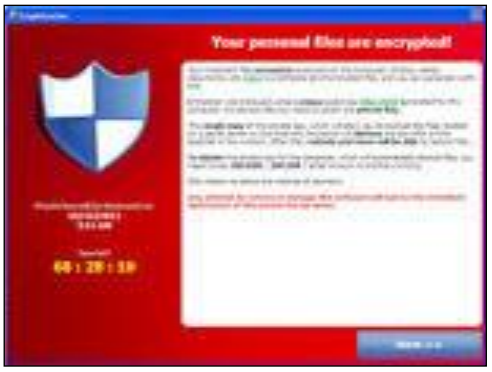

Fig. 2.1: Symptoms of Ransomeware

1) It features unbreakable encryption, which means that you can't decrypt the files on your own (there are various decryption tools released by cyber security researchers – more on that later);

 

2) It has the ability to encrypt all kinds of files, from documents to pictures, videos, audio files and other things you may have on your PC;
3) It can scramble your file names, so you can't know which data was affected. This is one of the social engineering tricks used to confuse and coerce victims into paying the ransom;
4) It will add a different extension to your files, to sometimes signal a specific type of ransomware strain;
5) It will display an image or a message that lets you know your data has been encrypted and that you have to pay a specific sum of money to get it back;
6) It requests payment in Bitcoins because this crypto-currency cannot be tracked by cyber security researchers or law enforcements agencies;
7) Usually, the ransom payments have a time-limit, to add another level of psychological constraint to this extortion scheme. Going over the deadline typically means that the ransom will increase, but it can also mean that the data will be destroyed and lost forever.
8) It uses a complex set of evasion techniques to go undetected by traditional antivirus (more on this in the "Why ransomware often goes undetected by antivirus" section);
9) It often recruits the infected PCs into botnets, so cyber criminals can expand their infrastructure and fuel future attacks;
10) It can spread to other PCs connected to a local network, creating further damage;
11) It frequently features data exfiltration capabilities, which means that it can also extract data from the affected computer (usernames, passwords, email addresses, etc.) and send it to a server controlled by cyber criminals; encrypting files isn't always the endgame.
12) It sometimes includes geographical targeting, meaning the ransom note is translated into the victim's language, to increase the chances for the ransom to be paid.

## III. TYPES OF RANSOMEWARE

### A. *Encrypting Ransomeware*

This type of ransomeware is incorporated with the advance encryption algorithm. The encryption algorithm is desigened in such way that it blocks the user's system and ask for ransome to the user. It suggests the user that after paying the ransome the decryption key will be given to the user to access the blocked contents. Examples of such ransomeware includes:

*1) CryptoLocker:*

If the downloaded file is opened by an unknowing user, the Cryptoware will be dropped on the PC, where it will infect itself in several processes, continuing the infection by encrypting all of the locally stored data, as well as the data available in network-connected devices.

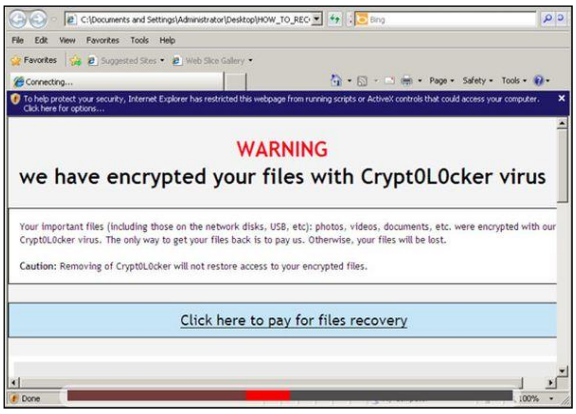


Fig. 2.2: CryptoLocker

*2) Locky:*

It starts infecting the files by spam emails. Once the Locky enters into the user's system, its main component starts running on machine, and after that all the locally stored file will get infected and will get encrypted by the Locky virus.

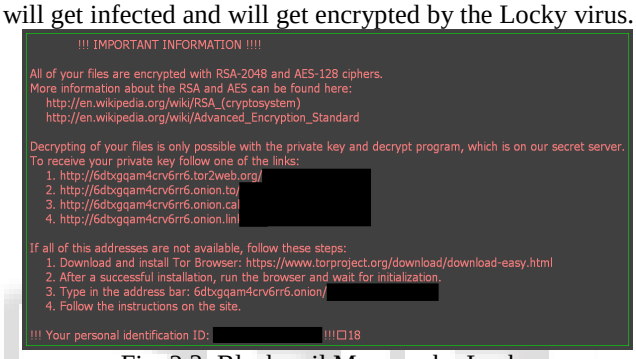


Fig. 2.3: Blackmail Message by Locky

*3) Cryptowall:*

The infection starts with an e-mail received by the victim, which contains a link that is connected to a number of compromised domains. When the potential victim follows the link, a downloader is placed on the system. The downloader connects to a number of domains controlled by hackers, from where it can download CryptoWall. One of the domains sends back and installs CryptoWall on the system. The ransomware encrypts the system data. A warning is presented on the screen with instructions on how to pay for the decryption key.

### B. *Locker ransomware*

This type of ransomeware locks the user out of the operating system. In this acse the virus or attacker will not encrypt the files or data of user's system but still ask for ransome pay to unlock the system. Examples of such ransomeware includes:

*1) WinLocker:*

Itlocks the user's system and ask victim to transfer money for unlocking the system.

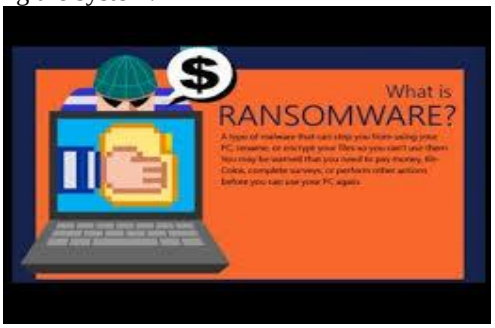


Fig. 2.4: WinLocker

 

## IV. PREVENTION TECHNIQUES OF FROM RANSOMWARE

Ransome prevention can be divided in two steps:

1) The human Factor
2) On The System

### A. *Startergy 1: The human Factor*

1) Learn to Read eMail Message Header: It is a good practice to track down the spam email source. Whenever a mail looks like suspicious in nature (even for regular emails), it is strongly advised to look for the header for source IP address for a quick reverse lookup to validate.
2) Double Attention before Downloading an Attachment: Most of the malicious files are being downloaded by the users through email. Look for the header information to validate the user, domain etc. correctly before downloading an attachment. It is also the worst practice to auto-run a downloaded file. File extension should be checked and passed through security software before further processing.
3) Beware of pop-up: This is where many users are social engineered with some catchy advertisement, rumor, and news etc. to click on a link which ended with infected the system by creating a hidden channel (backdoor) to the bad guys.
4) Control your own browsing: This is advised not to follow a pop-up or random link guide you to your target website. Always use search engine.
5) Educate yourself with Security Awareness Trainings: Follow organizational or some trusted online security awareness trainings on regular basis to update yourself with latest preventions techniques w.r.t the latest attacks methods.

### B. *Startegy 2: On the System*

1) Data Backup (Online and Offline): This is the most important task that everyone must do. It is highly recommended to take data backup on both online (cloud etc.) and offline (local HDD backup etc.) mode on regular basis to protect your data for any further ransomware attack and destruction.
2) Strong Security Guard: This is somewhere many users are lagging behind. The practice of having a strong Antivirus, Firewall, Spyware etc. with the latest updated patch can prevent many incoming attacks. It is also advised to personalize the security protections to run on their best configuration to protect the system. Enable the security softwares to run on heuristic mode and enable to scan for compressed or archived files as well.
3) Updating of OS and all Services/Softwares: One must keep the operating system and all other services and softwares updated with the patch released by the vendor or vendor authorized 3rd party and not from any other random source who claims for providing robust and quick update.
4) Use of Spam Filter: It is a good way to detect unsolicited and undesired email and prevent those from getting to inbox.
5) Running on-time Remote Service and File Sharing: It is advised to run any required remote service or file sharing only when it is needed. Ransomware takes this advantage to spread the attack into other systems or network connected with the infected one.
6) Disabling of Unused Active Network Connection: If someone is not using a particular network connection (which is still on active mode), then connection traffic will also be ignored for obvious reason. Attackers take this advantage to expand their attaching range. So this channel must be stopped by disabling the unused but active network connection.
7) Disabling of Auto Execution of files: There are some services which are authorized by admins to auto execute of files on system. These features need to be evaluated to keep on the system.
8) Enable 'Show File Extension' on Windows system: Generally end users do not want to see the common file extensions. Attackers try to puzzle their target users to hide malicious files inside well known file types. By showing all file extension feature in Windows system, users will understand the correct file type and refrain to execute some unwanted malicious extensions.

### C. *Startergy 3: Other Ways of Prevention[4]*

1) Email and Gateway Protection: Trend Micro™ Cloud App Security, Deep Discovery™ Email Inspector, and InterScan™,Web Security address ransomware tied to common delivery methods such as email and web pages.

Capabilities:

- Spear-phishing protection
- Malware sandboxing
- IP/Web reputation checking
- Document exploit detection

2) Endpoint Protection: Trend Micro Smart Protection Suites detects and stops suspicious behavior and exploits associated with ransomware at the endpoint level.

Capabilities:

- High-fidelity machine learning
- Ransomware behavior monitoring
- Application control
- Vulnerability shielding
- Web security provision

3) Network Protection: Trend Micro Deep Discovery Inspector detects malicious traffic, communications, and other activities associated with attempts to inject ransomware into the network.

Capabilities:

- Network traffic scanning
- Malware sandboxing
- Lateral movement prevention

4) Server Protection: Trend Micro Deep SecurityTM detects and stops suspicious network activity and shields servers and applications from exploits.

## ACKNOWLEDGMENT

I would like to take this opportunity to express my profound gratitude and deep regard to our Institute, for the guidance, valuable feedback and constant encouragement. I would also like to give my sincere gratitude to our management, all the friends and colleagues who filled in the survey, without which this research would be incomplete. I am also very

 

thankful to my husband Mr. Anant B Patel for all his support and help.

## V. CONCLUSION

We have presented an in-depth analysis of the current state of ransomware. We have defined the types of the ransomeware along with the symtomps of ransomeware. We have described various aspects of their operation, their infection mechanisms and the. We have shown how to deal with the ransomeware attacks and also the different prevention techniques for ransomeware. In future we can develop the more secure technique to copup with the malwares."

## REFERENCES

[1] X. Luo andQ. Liao, "Ransomware : a new cyber hijacking threatto enterprises," inHandbook of Research on Information Security
[2] Trend Micro Incorporated. (14 March 2006). TrendLabs Security Intelligence Blog. "Ransomware! Ransomware! Ransomware!" Last accessed on 20 March 2017
[3] Threat Study Issue Date: August 12, 2016 | TLP-WHITE1 | Serial: W-TS-EN-16-00734 | Industry: All
[4] Ransomeware: Past, Present and Future White paper.
[5] CERT.be "Ransomware Whitepaper TLP: WHITE"

 