Table of Contents

Executive Summary

This report walks through one of the malicious software i.e. ransomware that prevents users from accessing their data unless a ransom is payed in order to regain access. The report will go into providing the details about how Ransomware is evolved, how users' computer is affected and also suggests various ways to detect it. The report also provides a description of the virtual environment setup done in order to make the technical demo. Step-by-Step guide is also provided for the technical demonstration part. The report then ends by giving precaution methods that needs to be taken, what to do if the computer is infected with ransomware and what the future of ransomware holds.

Section 1: Introduction

The present context of the world demands the protection of systems used in the cyber world, or the internet which incorporates hardware, software and data. The assurance incorporates security from hack or even the temporary disruption of services they provide. It is vital as the present world functions is intensely upheld through the web. In computer virology, as the advancement of technologies keep on developing, advanced encryption algorithms, on the brilliant side, can be used to successfully secure data from malicious attack. On the dark side, however, they can likewise be utilized by attackers to direct poisonous exercises looking for benefits or advantages. One of the use of malware in the cyberspace is Ransomware or Crypto virus that imposes serious threats to information assets protection. This report will be a walk through the ransomware. [23]

Section 2: History and Evolution of Ransomware

Ransomware can be defined as any software that is designed to either deny access to a computer system or data, or threaten to release the user's data, unless a sum of money is paid. The threat is either real or implied.

Ransomware can be broken down into three main groups depending on its actions. They are:

- Scareware
- Screen lockers
- Data Encryption (crypto ransomware)

First ransomware was in 1989, distributed on 5.25" diskettes via the US mail. It was a crypto ransomware. At the time, most people didn't use personal computers, mostly the internet was used by people in the science and technology sectors. At the time, encryption technology was also limited[1].

In 1996, a proof of concept crypto ransomware was developed by Adam L. Young and Moti Yung that used public key/private key using RSA. 10 years later, in 2005 - 2006, is when crypto ransomware became more prominent.

Between 1995 and 1998, with the release of Windows95 and Windows98, more and more people began using the internet and personal computers. These operating systems brought all the configuration settings for the computer together in a single manageable location, which made it easy to exploit for those that knew their way around the Window Registry. Also in the late 90's people were moving from dial up internet access to the always on broadband connections.

These advances in technology saw the emergence of scareware ransomware in the early to mid 2000s. Scareware is any software that makes the user think their system is compromised and they need to spend money to get it fixed. Scareware generally comes in the form of browser pop ups that are cleverly designed to look like legitimate Windows messages telling users something was wrong and a download would fix it.

As many people started to recognize scareware for what it was, a new breed of ransomware emerged. In the mid to late 2000s, misleading apps were a prominent way to extort money from computer users. These apps would install and when run, they would modify the Windows Registry. These modifications mainly targeted settings that Network Administrators would use to create Group Policies that dictated what resources domain users had access to. Generally the screen background would be changed to something containing a message indicating the machine had been compromised and a phone number or website to visit, as well as hiding everything under MyComputer and MyNetwork, removing tabs from the Display Properties interface and in some cases hiding the control panel. Some even modified the hosts file to prevent searching for

solutions on the internet. The user still had most of the functionality of the system and their files. A popular solution was to sell the user a fake anti-virus program to solve their problems, although many of these anti-virus programs didn't do anything other than revert the system settings.

As people found ways to reset their registry settings on their own and regain control of their systems, the ransomware apps changed again, this time morphing into screen lockers. Screen lockers prevent the users from accessing their system until something specific happens. Early lockers emulated the Windows Security Center and required users to re-authenticate their version of Windows. Although the re-authentication was free, the number users had to call was routed through a long distance company with extremely high rates. Further evolution of screen lockers included fake messages from law enforcement agencies claiming incriminating things had been found on the person's computer and they needed to pay a "fine" to have access to their system again. Finally ransomers just came out and told people their system was locked and they needed to pay to get their data back.

In 2013, 14 years after its original development, crypto ransomware began making a comeback and is the most popular type of ransomware in use today. In 2017, the FBI Internet Crime Complaint Center (IC3) received close to 1800 complaints of ransomware that cost users over 2.3 million dollars. This does not account for all the cases that were not reported.

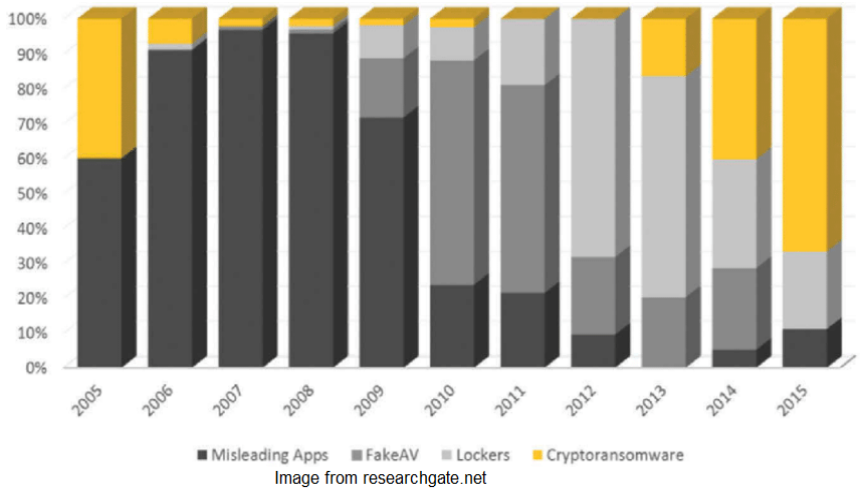


Image from researchgate.net

Section 2.1: List of Famous Ransomware

- Locky - Locky first appeared in February 2016, and is mainly distributed via email almost everyday. As such, its main method of infection is through social engineering and it only targets Windows PCs. It is able to disguise itself and can encrypt more than 160 types of files which may include source code and databases. It uses various scripting languages for delivery and uses RSA-2048 + AES-128 cipher with ECB mode for encryption. Files on fixed drives, removable drives, networks, and RAM disk drives are vulnerable to encryption by Locky [4].

- WannaCry - WannaCry is a wormable ransomware that spreads like a virus and it targets Windows computers. Symantec believes that WannaCry may have a North Korean origin. It is currently still active, but not as much as before [5].

- NotPetya - NotPetya affects Windows PCs and masquerades as the Petya ransomware. Unlike Petya whose goal is to extort money, NotPetya's goal is to destroy files as quickly as possible. It uses a bunch of tools to navigate through a network, infecting machines as

it goes. It seeks to gain administrative access on a machine and then leverages that power to commandeer other machines on the network [6].

- Bad Rabbit - Bad Rabbit is a variant of NotPetya and was primarily distributed in Ukraine and Russia to a number of major corporations. It uses unique Bitcoin wallets for every victim, and utilises DiskCryptor which is open source legitimate software that is mainly used for full drive encryption. It is mainly spread via a fake Flash update on compromised websites. In addition, it contains Game of Thrones references [7].

- Cryptolocker - Cryptolocker is a Trojan horse that infects a computer and then searches for files to encrypt, which may include anything on hard drives and any connected media. Files on the cloud may also be affected. Only Windows PCs are affected. Cryptolocker uses asymmetric encryption to lock the files, and computers are mainly infected via emails with unknown attachments which contain a double extension (a hidden executable). The malware must be downloaded first to infect a computer because it cannot self-replicate as it is a Trojan horse. The malware may also come from websites that prompt users to download a plug-in or video player [8].

- Crysis - Crysis is typically spread by hacking into Remote Desktop Services and manually installing the ransomware. The attacker usually downloads and installs monitoring programs like keyloggers to collect data from the system and also to gather data of the activities and data of the victim. The Crysis variant is executed on the victim machine and the ransomware encrypts almost every file of the affected machine including executable files. Additionally, a richer company which is affected will be asked for more money than a smaller company or a private individual [9].

- Jigsaw - Jigsaw comes with a countdown timer that starts ticking once the malware is deployed. During the first 24 hours, the malware will start deleting a few files every hour. On the second day, it will delete hundreds of files. On the third day, it will delete thousands of files until the ransom is paid. Furthermore, if the victim tries to tamper with

the malware or restart the infected computer, the malware will delete 1000 files as punishment [10].

Section 3: Methods of Infection

Ransomware is most often spread through phishing emails through malicious attachments, or "Drive-by" downloading[21]. This occurs when the user is visiting an infected site and the malware is downloaded and installed without the user's acknowledgement[21].

In Microsoft products, macros are disabled by default due to the ability of being utilized for malicious intents. When a document is downloaded, such as Word or Excel, the user is prompted to enable macros if *'enter problem here'*. If the macro is enabled, it will connect to a web server to download the executable file. Once the file is downloaded, the file is launched and looks for attached drives. The ransomware will then begin to encrypt documents, images, music, videos, databases, or other "important" files. There are usually Read Me documents left behind to give the user instructions on how to get the key for decryption (usually payment via bitcoin or other payment types).

Section 4: Methods of Detection

Since ransomware infections are no doubt unavoidable, an individual or an organization should be prepared to recover from a ransomware attack as soon as the attackers strike[16]. An important method of defense against such attacks is to detect the attacks the moment it starts to appear[16].

It is necessary that all individuals employ an all-out, multi-pronged approach of endpoint, network, server, and backup level detection in order to protect the data[16]. Moreover, one should not forget about local and remote machines, be it physical and virtual machines[16].

Some methods of detection involve the active monitoring of known ransomware extensions[16]. For example, it is possible that a computer has been hit with a ransomware attack if these ransomware extensions are found as part of the computer's file names[16]. Furthermore, network administrators have the option of monitoring a boost in the renaming of files[16]. In this case, if there is a large amount of files getting renamed, it is very likely that the change was caused by ransomware attacks[16]. In addition, it is a good idea to utilize machine learning and change rate monitoring to enhance the capacity to detect ransomware[16]. Using predictive analytics to determine the probability that ransomware is operating on any computer may be our most powerful tool as of now to monitor and detect ransomware attacks[16].

Antivirus software may also be utilized to block any attempts by ransomware to encrypt data[16]. Their designs include the ability to monitor for text strings that are known to be related to ransomware[16]. The antivirus programs then match these text strings to massive databases of digital signatures[16]. Unfortunately, this technique does not prove effective against new or obscure strains of ransomware[16].

Behavioral analysis detection

Behavioral analysis detection of ransomware is a much more effective detection method[20]. It is also known as dynamic-based analysis detection, and involves the live monitoring of processes[20]. It determines if any processes are behaving in a way they should not be behaving at all or with any malicious intent[20]. If the process is determined to be behaving suspiciously, it will be flagged as dangerous and will be terminated[20].

The main difference between static and behavioral analysis is that during static analysis, behavioral traits are inferred from the binary file of an unknown executable, then used by a matching algorithm to assign a threat level[20]. On the other hand, during behavioral analysis, behavioral traits of the executable is known as it is observed in real-time, then inferences are made by an inductive decision algorithm on the threat level[20]. In this case, the executable must prove that is it acting in a safe and unsuspicious manner[20].

Because ransomware can be easily defined and is a subset of malware, it is possible for us to predict that an unknown process is ransomware due to the existence of a well-defined behavioral construct[20]. Behavioral analysis has been proven to be extremely effective against crypto-ransomware because it contains core behavioral traits necessary for a data encryption attack[20]. This works because such traits do not change across variants and families of ransomware[20]. These traits are divided into two distinct tasks: suspicious setup procedure, and data encryption[20].

For suspicious setup behavior, there are 6 behavior traits of ransomware that is shared with other malware[20]. They include:

- Payload persistence: an attack must persist across reboots and be able to resume upon starting.
- Anti-system restore: ransomware has been known to delete Windows shadow copies which prevents encrypted data from being restored to an older unencrypted version.
- Stealth techniques: malware will try to execute in a stealthy manner to avoid being noticed.
- Environment mapping: When malware is executed, it may map its system environment before initiating its setup procedure.
- Network traffic: ransomware requiring an internet connection will either download payload related files, and/or for communication of the encryption key.
- Privilege elevation: executing some system-related activities may require access rights that belong to admin or the root.

It should be noted that not all ransomware will exhibit all of these traits[20].

There are 3 categories in data encryption[20]. They include:

- Class A: opens original file and directly overwrites its content with its encrypted data.
- Class B: first moves the file to a discrete location, encrypts the file (Class A), then moves the file back to original location.
- Class C: reads the original file, encrypts content, writes the encrypted content to a new file, then deletes the original file.

To identify the ransomware, the detection software must have the ability to track file operation, and/or the ability to identify data encryption[20]. Extracting behavioral features associated with data transformation and file operation can provide valuable information necessary to detecting ransomware. However, it cannot be solely relied upon[20].

In machine-learned behavioral-based detection, it requires a decision making algorithm that accepts a quantitative behavioral trace of a running process as an input, to output a simple binary decision on whether it is safe or not[20]. A supervised machine learning approach is best suited to detect ransomware, in which there is training of a decision algorithm to recognize certain behavioral traits of running processes and outputs whether it is behaving suspiciously or not[20]. It requires 3 ingredients: training dataset containing examples of known ransomware; capturing of behavioral traits in a quantifiable manner; and classification scheme which defines the training and prediction algorithm[20].

The limitations of behavioral analysis detection are that behavioral obfuscation techniques have been used by malware developers to attempt to mask the malware's malicious behavior[20]. Such techniques include: behavioral noise (randomly ordered system call insertion, system call substitution, or system call reordering), and system noise that includes general noise introduced by variability in development techniques[20]

4.1: Free Dedicated Tools to Combat Against Ransomware

Even though ransomware malware quite often utilizes unbreakable open key encryption to lock files, the number of variants is generally little at any one time. It is possible that a security program can be tuned to detect the most active ransomware by looking for referred behavior, associating with the filesystem. Here is the list of free dedicated tools that can be utilized for the detection, decryption and clean up.

a) NO More Ransom!: The "No More Ransom" website is an initiative by the NATION High Tech Crime Unit of Netherlands' police, Europol's European Cybercrime Centre and McAfee with the objective to help victims of ransomware recover their encrypted data without paying the culprits. The project has a list of about 80 decryption tools to decrypt the files encrypted by various ransomware. The project also aims to instructs users about how ransomware operates and what countermeasures can be taken to prevent it.
    a. www.nomoreransom.org/en/index.html [12]

b) Free Anti-ransomware software: Several behavioral detective tools are available nowadays to combat against ransomware. One of the example is RansomFree that we used in our demo. In addition, many antiviruses like AVG, BitDefender also comes with anti-ransomware detection. One of the easiest way to protect against ransomware is to prevent it.

c) Free Ransomware rescue kit: A ransomware removal and rescue kit has been discharged to give organizations an option in contrast to paying a fee to unlock encrypted files. In order to combat this kind of attacks on enterprise, security professional Jada Cyrus has compile a rescue kit which is accessible for free online. Intended to help "streamline the way toward reacting to ransomware infections," the ransomware response kit accompanies guidelines and decoding instruments for various strains of ransomware. [22]

4.2 RansomFree

a) What is RansomFree?

RansomFree is a free ransomware protection software, developed by Cybereason. It is able to detect and prevent ransomware from encrypting files on both computers and servers. It is a behavioral anti-ransomware tool, which means it does not rely on malware signature detecting. It protects against local encryption, encryption of files on networks and shared drives, catches stand-alone ransomware programs as well as fileless ransomware[13].

b) How does RansomFree work?

RansomFree works by watching the way applications interact with files, and when it detects ransomware behavior, RansomFree will immediately stop it before the targeted files are encrypted. It deploys bait files that is strategically placed where ransomware often begins its encryption. RansomFree is supported on Windows 7, 8, 10, 2008 R2, and 2012 R2. RansomFree requires about 100 MB on the drive [13].

Section 5: Impacts

Ransomware targets both home users and businesses. This can lead to serious consequences which include:

- Loss of sensitive or proprietary information which may be either temporary or permanent
- Disruption of regular operations
- Financial losses due to the process of restoring systems and files
- Harm to an organization's reputation and branding
- Potential legal penalties arising from poor security policies and insecure data handling [11]

It is important to note that paying the ransom does not guarantee that the encrypted files will be released. Instead, it only guarantees that the malicious actors receive the money, and therefore

continue to terrorize the victim users. Additionally, being able to decrypt the files does not necessarily mean that the malware infection itself can be removed [11].

Section 6: Sandboxing

a) What is a Sandbox?

A Sandbox is a virtual operating environment that is isolated from the rest of the computer. Sandboxed files cannot damage the host computer or access the host computer's data and files[14]. Using a Sandbox, we can install and run new and untrusted apps without harming our host system[15].

b) Sandbox applications for Windows

- BitBox (browser in the box) - It allows web browsing in a sandbox environment, and is applicable for both Chrome and Firefox. There is also a virtual box instance for Linux. Howver, it is more memory-demanding. After testing files on BitBox, it is capable of downloading files on to the host PC [14].

- BufferZone - BufferZone is an endpoint sandbox tool. It is good for when the user is heading to parts of the internet that may be dangerous, or the user may be using a USB stick that cannot be trusted. It is easy to add programs to run through BufferZone, and every major browser works well within it. A good feature is that not much tinkering and configuration is needed to set BufferZone up. Additionally, everything that runs through BufferZone is "read-only", which means that nothing can be written to the hard drives[14].

- Sandboxie - Sandboxie is lightweight and free. It allows us to install and run almost any Windows software through it. Besides installing and running programs within Sandboxie,

it allows us to run any already-installed programs via Sandboxie, for instance, a web browser[14].

- SHADE Sandbox - Its user interface is much simpler, straightforward, and beginner friendly as compared to Sandboxie. Through SHADE Sandbox, all browsing history, temporary files, cookies, windows registry, and system files are well isolated from the Operating System[14].

- Toolwiz Time Freeze - Toolwiz Time Freeze creates a virtual copy of the entire system settings and files and saves the state. After using the application that the user wishes to test, all the user has to do is to just reboot the system, and the original state will automatically be restored. It is extremely useful in testing a program thoroughly with no limitations, and without making any changes to the host Operating System[14].

- Shadow Defender - Shadow Defender is similar to Toolwiz Time Freeze. Users can specify folders and files to exclude from Shadow mode, and can pick and choose which changes to keep and which to discard. In Shadow mode, if the user wishes to save a downloaded file or commit to a system change, the user can just click on the "Commit now" button [14].

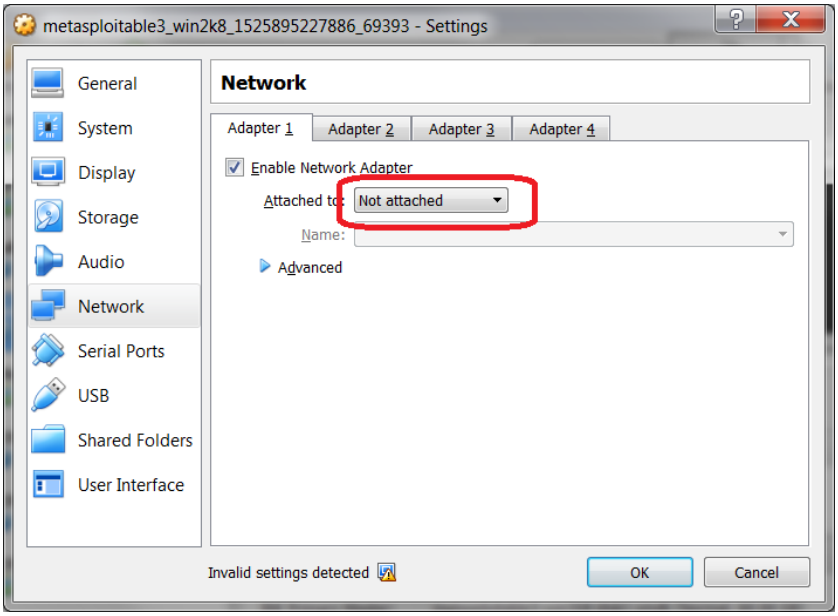
- Create a Virtual Machine - All the applications mentioned above are doing Light Virtualization. This means that the apps that are being tested are still running on the host OS. VirtualBox utilizes Full Virtualization and users can run on other operating systems besides the host Operating System[14].

Section 7: Technical Demonstration

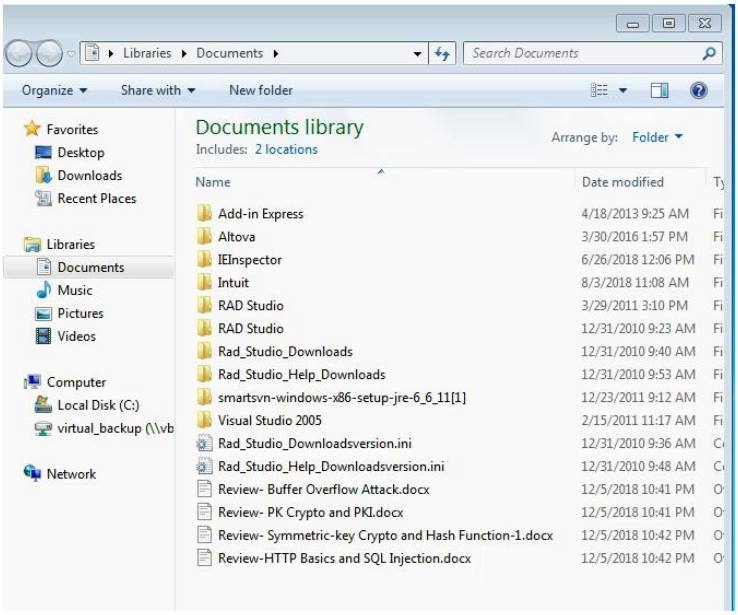
The technical demo was done using Windows 7 Pro running on a virtual machine inside VirtualBox. The two configuration changes made to Windows 7 were to turn off the hiding of

known file type extensions, and to turn on the option to show hidden folders. The guest machine was cloned so installed software would be identical. The guest machines did not have any anti-virus installed on them. One guest machine had RansomFree installed. Both machines had Wireshark installed to monitor network traffic. The Host machine had RansomFree and Avast Anti-Virus installed.

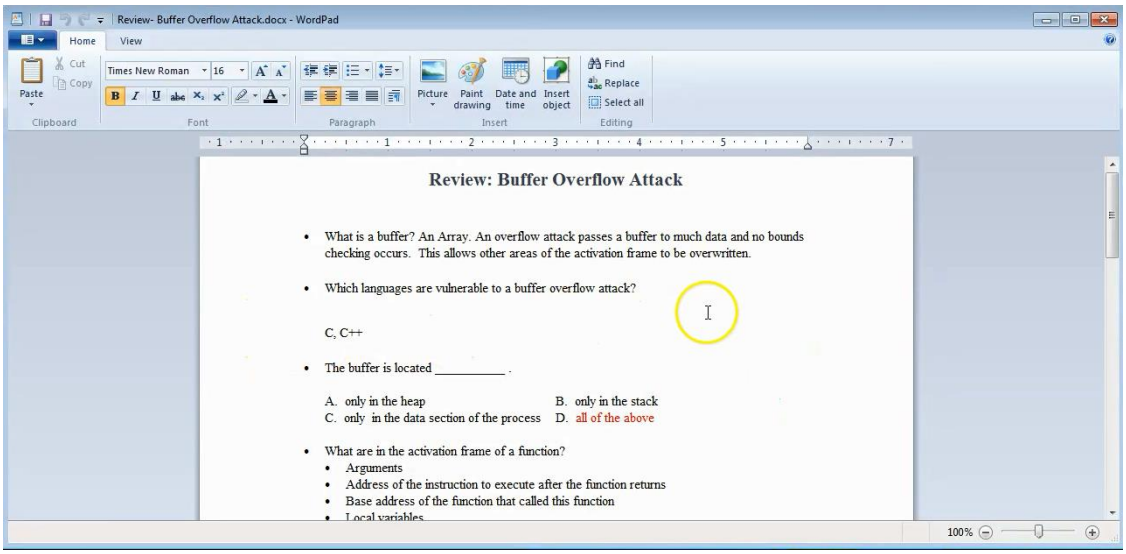
VirtualBox was installed in a default configuration as well as the Windows 7 Pro operating system. After Wireshark, WannaCry and RansomFree were installed on the respective machines, the network adaptor for those virtual machines was changed to "not attached" which essentially unplugs the network cable to prevent spread of WannaCry to the host machine or any other machine on the network.



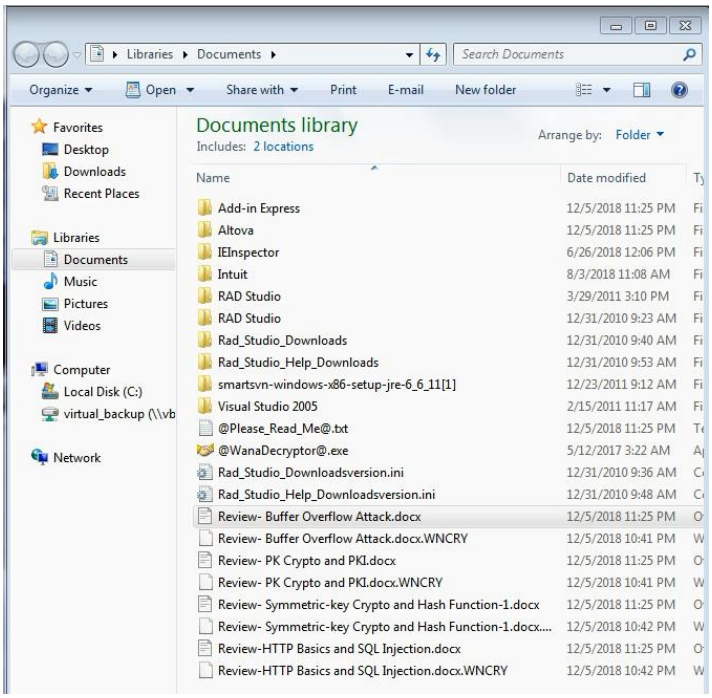
Once the configuration was finished, it was time to run WannaCry.
Starting with the machine to be infected, we look in the Documents folder where we have loaded four docx documents.



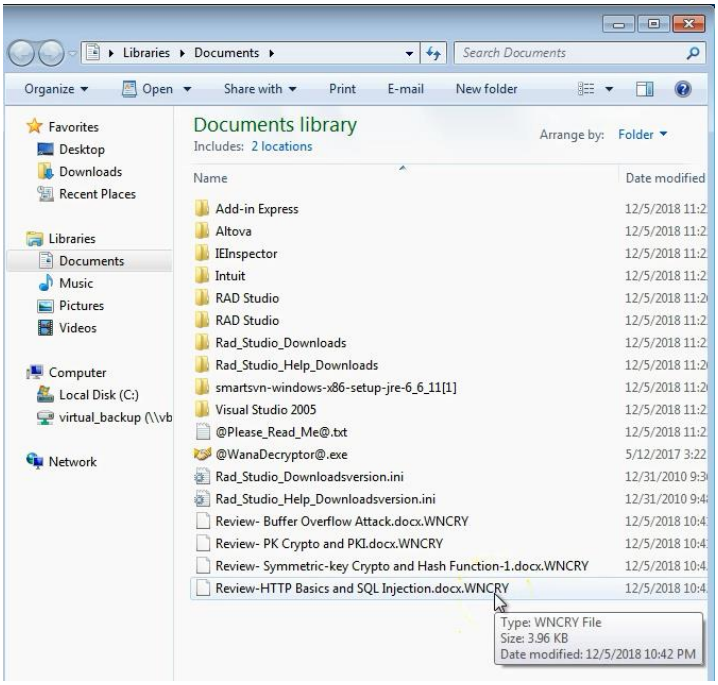
These documents are not encrypted as we can see in the next image.



As WannaCry runs it makes encrypted copies of your files and adds a WNCRY file extension.

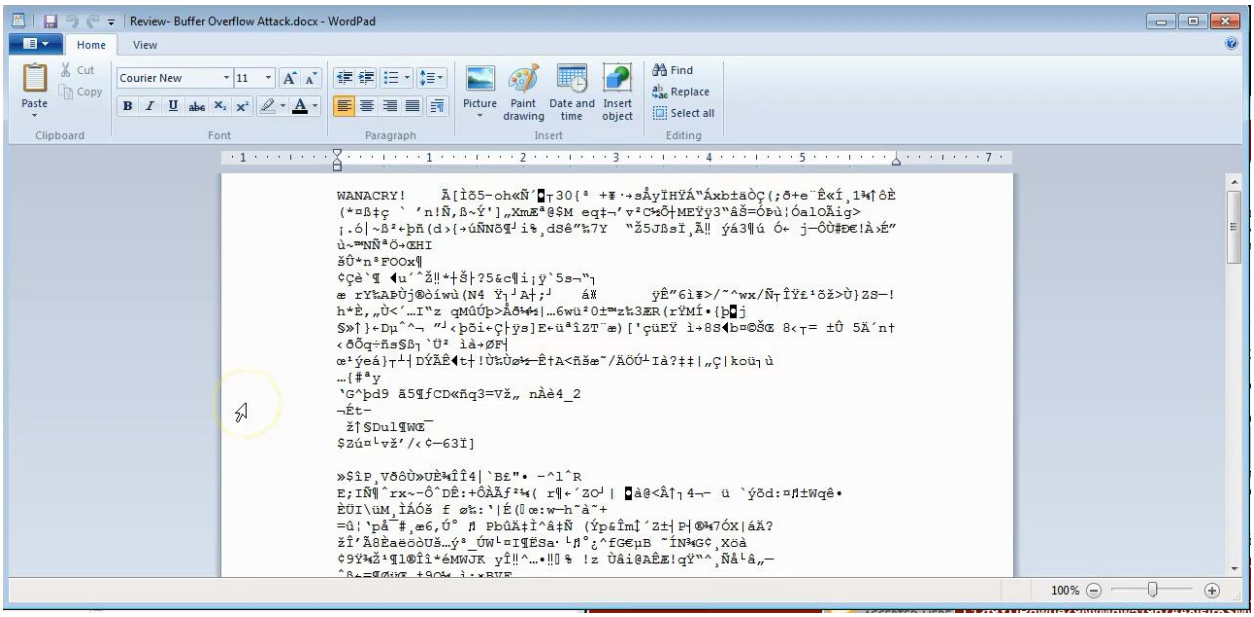


After the files have been encrypted, the original files are deleted.



Once WannaCry has finished encrypting all the data files it can find, the software displays a message to alert the user as to what has happened. This message gives details about how to pay the ransom to get the data back as well as running timers. When the first timer runs out, the amount of the ransom increases. When the second timer runs out, all the encrypted files will be deleted.

After renaming one of the encrypted files and removing the WNCRY extension, the file was opened again and it is clear that the file has been encrypted.

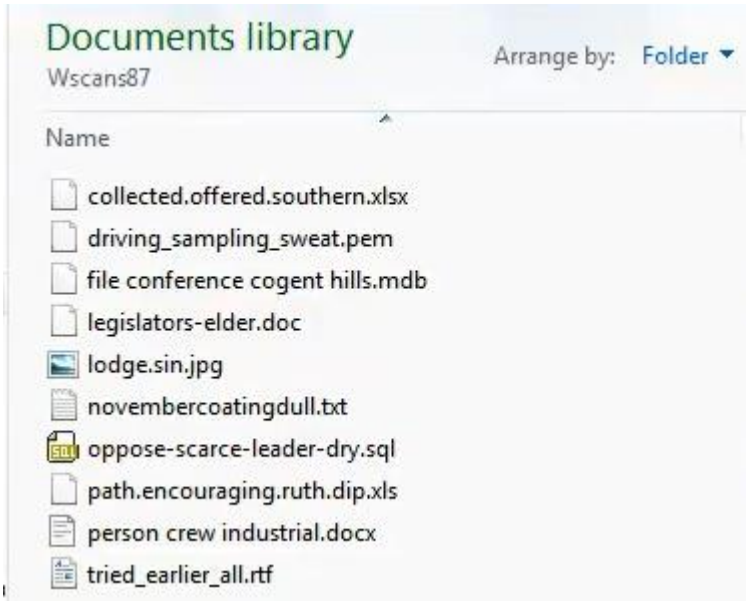


The first bit of text in the file is even the label “WANACRY!”.

Running the test again with RansomFree installed, a few things can be noticed. First, in the Documents folder, there are two new hidden folders that contain files with office document extensions as well as some other popular extensions.

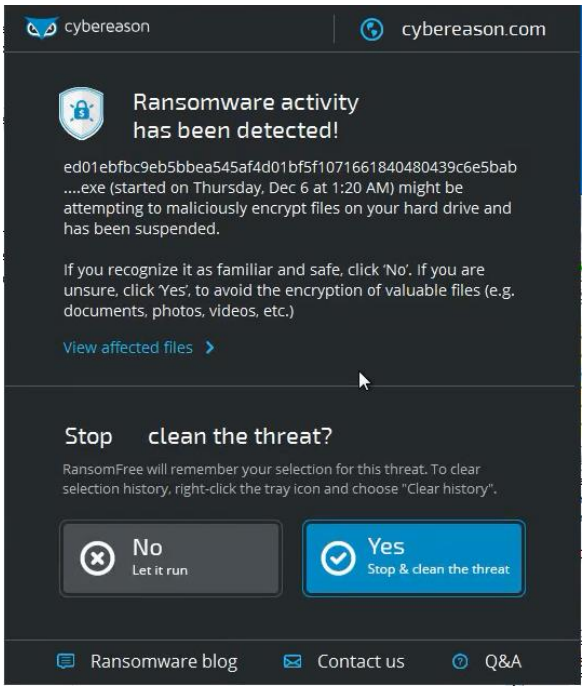
One of these hidden folders, Wscans87, is shown below along with the same clean files used on the machine that was infected.

Viewing the Wscan87 folder shows the following document list.



In this way, RansomFree can monitor the bait files it deploys to see if and when they are being accessed.

With RansomFree running, when WannaCry is executed, RansomFree intercepts it and displays the following confirmation dialog:



Thus, prompting the user to confirm access for the running process.

During both tests, Wireshark was running on each machine. However since the machines were not connected to a network, no additional traffic was seen. If the infected machine had been connected to a network, Wireshark would have much more traffic sending out LLMNR packets. These packets are used for name resolution by the operating system but also used by WannaCry as a way to find other machines to spread to.

Section 8: Countermeasures

8.1 How to Prevent a Ransomware attack?

1. Backup

A standout amongst the most recommended approach to get ready for Ransomware attack is backup. It is advised to have two reinforcement duplicates, one service that makes an automatic reinforcement of records on cloud and another to store physically. There is no assurance that reestablishing from backup during ransomware attack will be a smooth and complete process. However, it is abundantly favored alternative than paying ransom. Thus, with the end goal to ensure that the Backup is a suitable alternative, a few stages should be considered and put into action.

a. Recovery Point Objective (RPO):
    i. Recovery Point Objective is the time period directing how frequently backups are made. It likewise advises the dates and times you can recoup from. On the off chance that you take week by week backup and you got attack from ransomware during the interval, you can reestablish the information precisely as it was seven days back. On the off chance that you take day by day backs and suffer from ransomware attack, you can reestablish your information as it was the day preceding. It is critical to comprehend what your RPO is and how much information you could

remain to lose on the off chance that you were hit with ransomware and needed to recoup from your reinforcement. For example: Wes Tebo's company has the backup policy of daily backups that are kept for 60 days.

b. Recovery Time Objective (RTO):

i. Recovery Time Objective (RTO) is the rough estimate of time it will take to re-establish a computer from backup and get it back fully operational. RTO is regularly used to enable the IT department to group gauge to what extent it will take to recuperate from any data loss. Depending upon the sort of data loss, the time to really recoup the information may be longer than it is foreseen.

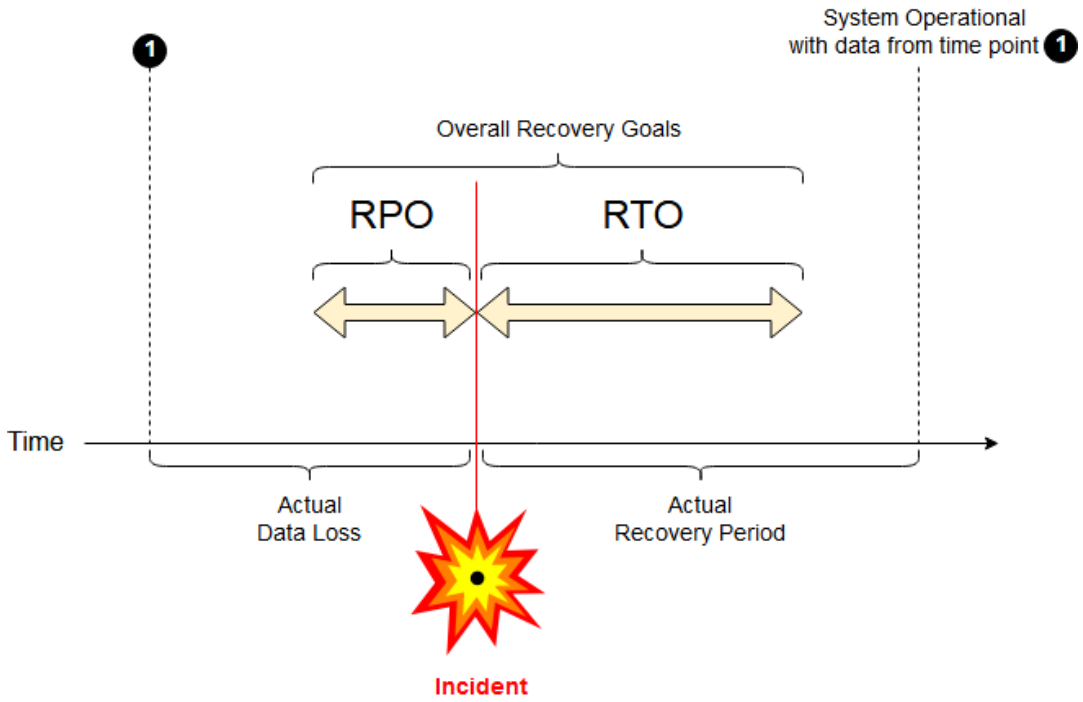


Fig: Schematic representation of terms RPO and RTO

Pricing of Backup

While it is feasible to keep your RPO and RTO very low and enhance your capacity to recuperate more information quicker, the sticker price on those kinds of backup frameworks can go up quick.

Most of the time, it can be more expense and time effective to invest into something like behavior-based endpoint detection as opposed to upgrading the backup policy. Behavior based endpoint detection is a part of Kaspersky Lab's multi-layered, next generation approach to protection. It evaluates an object dependent on its proposed activities before it can really execute that activity. An object's behavior, or now and again its potential behavior, is investigated for suspicious activities. Endeavors to perform activities that are plainly strange or unapproved would show the object is pernicious, or possibly suspicious.

Connectivity of Backup

On the off chance that the backup solution is local and associated with a computer that gets hit with ransomware the odds are great that the backups will be encrypted along with rest of data.

Ransomware, for example, CryptoFortress and Locky can encrypt associated network drives, so it is significant to have backups that isn't straightforwardly connected.

2. Patch Management

Patch Management is the way of dealing with a network of computers by frequently conveying all missing patches to stay up with the latest. There's an expression that goes, "In case you will do it more than once, automate it." This applies to patch management, from identification to the detection of missing patches, the whole process can be automated. Critical elements of the patch management process incorporate the following:

- Senior Executive support - Senior Executive Support is the executives' recognition of data security hazard in the association. In any case, past recognition of the issue is the

management’s support of patch management process, including guaranteeing that appropriate assets are coordinated toward the exertion over the organization[17].

- Dedicated resources and clearly defined responsibilities - Committed resources and plainly characterized responsibilities are essential to the achievement of the general procedure. Staff must be entrusted with the obligations of defining, actualizing, and dealing with the process[17].

- Creating and Maintaining a current technology inventory - A current technology inventory is fundamental to any patch management process. A current inventory of hardware and software helps the groups in charge of patch management decide the number of systems that are vulnerable, and the patches required. An inventory additionally enables the staff to find PCs and their proprietors over the organization[17].

- Identification of vulnerabilities and patches - Distinguishing proof of vulnerabilities and applicable patches is critical and one of a kind to every organization's patch management process. With the current technology inventory close by, the responsible group can screen for vulnerabilities and patches for software utilized all through the organization[17].

- Scanning and Monitoring the network - Pre-deployment scanning and monitoring of the organization's network can help evaluate hazard levels. Software tools can help distinguish the patch level of software on workstations with the goal that effective remediation steps can be taken[17].

- Pre-deployment scanning and monitoring - Testing patches in a controlled environment prior to deployment is a proactive advance regularly neglected by numerous organizations. Testing is critical to guarantee that patches work as expected and to perceive any potential antagonistic effects on an organization's frameworks[17].

- Post-deployment scanning and monitoring - Scanning and Monitoring the network explicitly after deployment of patches is a critical step to ensure that patches have been adequately applied. Few sectors like government and health services, post-deployment network filtering can be utilized as a review tool to help guarantee compliance with characterized standards. Even the government has taken ventures to address security vulnerabilities that influence its system in its offices[17].

Patch Management process utilized in the organization uses the accompanying methods:

- Manual: Patches and updates are handled physically at each workstation.

- Windows Automatic Update: Patches and updates are applied utilizing Windows Automatic Update in an entirely programmed mode, with no user intervention required.

- Automated: An automated patch management software product such as SUS, HFNetChk, BigFix Enterprise Suite, and PatchLink Update is utilized for patch management.

The use of automated patch management software product is most prominent among government and healthcare sectors whereas Education sector rely on windows update due to fewer resources available to implement and maintain automated process.

Section 9: Incident Response

In the event that the organization had enough foreknowledge to buy a cyber liability insurance policy, the initial step is to contact the insurer to inform them of a potential occurrence. The type of policy bought will decide how the insurer will react. Since both the organization and the insurer have an enthusiasm for restricting exposure and loss, a few safety net providers will

assume control over the digital occurrence reaction and get the specialized and lawful assets fundamental to react properly. [18]

In the event that the organization does not have cyber liability insurance policy, the IT resources needs to be alarmed with the goal that they can help react to the assault. In the worst case situation, IT will locate that the majority of the nearby and shared records that are utilized on a normal premise are encoded with a numerically difficult to-break encryption key. Contingent upon the business, the efficiency of the workplace staff may granulate to a stop. [18]

- Paying the ransom is never recommended, as it doesn't guarantee a solution to the problem.

- Remove the infected machines from network, so the ransomware does not use the machine to spread throughout the network.

- Research if it is possible to decrypt the malware on your own. About 30% of encrypted data can be decrypted without paying a ransom.

Section 10: The Future of Ransomware

Malware attackers are continually searching for new and vulnerable targets to exploit particularly now that malicious code that has been monetize. It is expected that with the advancement in the crypto virology world, the Ransomware attacks won't only be limited to computer but also will expand to internet of things (IOT). The attackers are hoping to use the infected IoT devices to extort commercial website by threatening a DDoS attack or locking IoT devices to charge a ransom. [24] In addition, IDC's Worldwide Healthcare Predictions Report noted that, the quantity of ransomware attacks in health services industry are expected to increase by twice number. This comes as a result of attackers concentrating more on medicinal services suppliers and others within the industry with access to sensitive patient and other valuable data. [25]

Appendix

- Browser Locker - https://youtu.be/WKCUR2jBoCs
  Technical demonstration of a browser locker malware on Google Chrome.

- Browser Intro - https://youtu.be/lC0Z2zrKinQ
  Introduction to the three browsers.

- WannaCry - https://youtu.be/CgFSGUZMD9Y
  Technical demonstration of WannaCry encrypting some documents on a Virtual Machine.

- RansomFree - https://youtu.be/FYBl6oLQf0M
  Technical demonstration of WannaCry encrypting some documents on a Virtual Machine with RansomFree to stop it.

References

[1] Savage, Kevin; Coogan, Peter; Lao, Hon. “The evolution of ransomware”. August 6, 2015.
Retrieved at:
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf
[2] Dacri, Bryana. “8 Recent, Dangerous Ransomware Examples.” January 8, 2018.
Retrieved at: www.bitsighttech.com/blog/ransomware-examples
[3] Rayome, Alison DeNisco. “The top 10 worst ransomware attacks of 2017, so far.” October 31, 2017.
Retrieved at: www.techrepublic.com/article/the-top-10-worst-ransomware-attacks-of-2017-so-far/
[4] Avast. “Locky Ransomware.”
Retrieved at: www.avast.com/c-locky
[5] Fruhlinger, Josh. “What is WannaCry ransomware, how does it infect, and who was responsible?”. August 30, 2018.
Retrieved at: www.csoonline.com/article/3227906/ransomware/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html
[6] Thomson, Iain. “Everything you need to know about the Petya, er, NotPetya nasty trashing PCs worldwide.” June 28, 2017.
Retrieved at: www.theregister.co.uk/2017/06/28/petya_notpetya_ransomware/
[7] Palmer, Danny. “Bad Rabbit: Ten things you need to know about the latest ransomware outbreak.” October 25, 2017.
Retrieved at: www.zdnet.com/article/bad-rabbit-ten-things-you-need-to-know-about-the-latest-ransomware-outbreak/
[8] Kaspersky Lab. “Cryptolocker Virus Definition.”
Retrieved at: usa.kaspersky.com/resource-center/definitions/cryptolocker
[9] Mesesan, Sergiu. “Crysis, a dangerous ransomware that is infecting companies right now.” January 10, 2018.
Retrieved at: opendatasecurity.io/crysis-a-dangerous-ransomware-that-is-infecting-companies-right-now/
[10] Norton by Symantec. “Jigsaw ransomware wants to play a game, but not in a good way.”
Retrieved at: us.norton.com/internetsecurity-emerging-threats-jigsaw-ransomware-wants-to-play-a-game-but-not-in-a-good-way.html
[11] UC Berkeley. “What is the possible impact of Ransomware?”
Retrieved at: security.berkeley.edu/faq/ransomware/what-possible-impact-ransomware
[12] No More Ransom. “Need help unlocking your digital life without paying your attackers?”
Retrieved at: www.nomoreransom.org/en/index.html
[13] RansomFree Cybereason. “Topics.”

Retrieved at: ransomfree.cybereason.com/faq/#1481739149887-83cdf56a-2933
[14] Krishna, Vamsi. “7 of the Best Sandbox Applications for Windows 10.” July 2, 2018.
Retrieved at: www.maketecheasier.com/best-sandbox-applications-windows10/
[15] Comodo. “Sandbox Settings.”
Retrieved at: help.comodo.com/topic-394-1-767-9744-.html
[16] Unitrends. “What’s the best ransomware detection tool?”
Retrieved at: www.unitrends.com/solutions/ransomware-detection
[17] Gerace, Thomas and Huseyin, Cavusoglu. “The Critical Elements of the Patch Management Process.” August 2009.
[18] Valach, Anthony P. “What to Do After a Ransomware Attack.” New York. Vol. 63, Iss. 5. June 2016.
[19] Ball, Tom. “The history of ransomware.” February 23, 2018.
Retrieved at: www.cbronline.com/news/the-history-of-ransomware
[20] Nieuwenhuizen, Daniel. “A behavioural-based approach to ransomware detection.”
Retrieved at: abs.mwrinfosecurity.com/assets/resourceFiles/mwri-behavioural-ransomware-detection-2017-04-5.pdf
[21] UC Berkeley. “How does a computer become infected with Ransomware?”
Retrieved at: security.berkeley.edu/faq/ransomware/how-does-computer-become-infected-ransomware
[22] Ransomware rescue kit released to combat criminal enterprise. “A rescue kit designed for security professionals and system admins has been released to eradicate ransomware infections.”
Retrieved at: https://www.zdnet.com/article/ransomware-rescue-kit-released-to-combat-criminal-enterprise/
[23] Luo, Xin. “Ransomware: A New Cyber Hijacking Threat to Enterprises.” The University of New Mexico, USA. Handbook of Research on Information Security and Assurance. 2009. pp:6
[24] Cobb, Stephen. “RoT: Ransomware of Things.” Enjoy Safer Technology.
[25] Trend Micro. “Forecasting the Future of Ransomware.” July 24, 2017.