UNIVERSITY OF
ALBERTA

Analysis of Best Practices for the Prevention of Ransomware Attacks

MINT 709 CAPSTONE PROJECT REPORT

Submitted by:

Narendra Reddy Bodlapati

MASTER OF SCIENCE IN INTERNETWORKING

DEPARTMENT OF COMPUTING SCIENCE

Under the guidance of:

Leonard Rogers

ACKNOWLEDGEMENTS

I would like to express my gratitude to my supervisor ***Leonard Rogers*** for the useful comments, remarks and engagement through the learning process of this Project. Furthermore, I would like to thank ***Leonard Rogers*** for introducing me to the topic as well for the support on the way. Also, I would like to thank everyone in my survey, who have willingly shared their precious time during the process of interviewing. I would like to thank my student friends, who have supported me throughout the entire process, both by keeping me harmonious and helping me putting the pieces together. I will be grateful forever for your support.

EXECUTIVE SUMMARY

The main objective of this project is to study and analyse about the Ransomware malware and its types, attacking vectors, prevention techniques and analysed the system behaviour when infected with Ransomware and implemented basic recovery techniques of infected system. Ransomware is a malware that encrypts the data available in the infected system and demands ransom to gain access to data. The work analysis is focused on different Ransomware models and different existing prevention techniques. Among these, the best prevention techniques is maintaining the backups of data and training the users on social engineering techniques. After implementing the recommended prevention technique, some recommendations are provided to make improvements in the performance and to meet the future need.

Table of Contents

List of Figures

Tables

1. INTRODUCTION

1.1 Introduction of Ransomware:

Ransomware is a sort of malware from cryptovirology [it is a field that studies how to use cryptography to design powerful malicious software] that finds a way to block the access to the system or to the data in the infected system. It does that by encrypting the data in the infected system and attackers demand ransom from the victim to grant access to a compromised system or to get the decryption key to decrypt the encrypted data.[1]

While some fundamental Ransomware structure isn't difficult for a capable individual to identify it, most of the Ransomware malware uses a framework called cryptoviral pressure, in which it scrambles the data in the compromised system, making them hard to reach, and demands a ransom to unscramble them.[1]

In a suitably launched Ransomware attack, recovering the data without the decryption key is a determined issue. Attackers are conventionally launching Ransomware attacks using a Trojan that is represented as a legitimate functionality so that the customer is tricked into downloading or opening it, it does the expected functionality along with installing several kinds of malware including Ransomware.

A few instances of how these Ransomware functions are, locking the screen by demanding a ransom from the victim in order to get the decryption key to unscramble the scrambled files. Unfortunately, the victim can’t guarantee the decoded data from the attacker even after paying the demanded ransom. There are many sayings that the victims are fooled by an attacker and demanded subsequent ransom even after paying the demanded ransom. Few attackers even installed other kinds of malware into compromised systems after paying the ransom.[2]

In 2011 the strategies changed, the attackers began to utilize electronic payment techniques such as Bitcoins and cryptocurrency and they added more dialects to the messages which likewise changed dependent on the user's area which was gotten by geo-finding the user's IP addresses.[2] From 2011, attackers started increasing the launches of multiple variants of Ransomware.

As per reports stated by McAfee Labs reported the introduction of Ransomware had shown a significant increase from the third quarter of 2011. In 2011 about 60000 new Ransomware infections were detected by them which more than doubled in 2012 to around 200000 infections. The below figure represents the McAfee Labs Threat report.

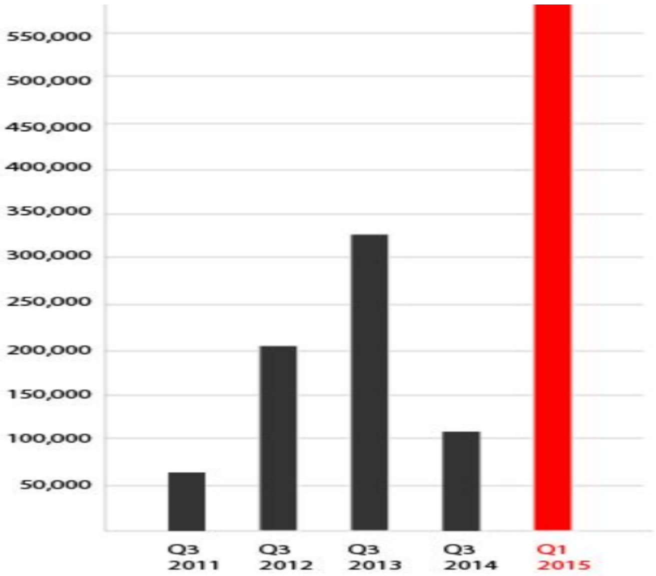


Figure 1: McAfee Labs Threat Report[2]

1.2 Ransomware Development:

Ransomware is developing quickly over the web. The Introduction of IOT devices makes a moving issue to the INFOSEC while expanding the attacking surface. They are developing into increasingly refined attacks and, they are getting progressively safe. Today, at a modest cost, the attackers thinking as launching Ransomware attacks as easy money. The major issue is that a large amount of dollars is lost by certain organizations and businesses that have chosen to pay a ransom. In some cases, it is recommended to negotiate before paying ransom. For example, the Hollywood Presbyterian Therapeutic Center and MedStar Health have shut down their computers for few weeks and used paper documents and attackers come down the amount of ransom demanded[18]. The issue here is that by paying the payment, they are financing the cybercrime.

It is significant for organizations to make sure that their employees are aware of social engineering techniques used by attackers. Because Ransomware is ordinarily presented through email and social engineering procedures to either download a document, with malicious attachments in emails.

Interest in innovation to identify and stop these dangers must be kept up, yet alongside that we must recall and concentrate on our weakest connection, which is the client. Information based coercion has been around since around 2005 however the advancement of payment encryption programming and Bitcoins have enormously encouraged the plan.[3]

Ransomware can be separated into two essential sorts. The most widely recognized is Crypto Ransomware, which encrypts records and information. The subsequent sort is Locker Ransomware. This form locks the PC or other gadget, keeping the exploited people from utilizing it.[5] Locker Ransomware just locks the gadget; the information put away on the gadget is ordinarily immaculate.

Crypto Ransomware, then again, encodes the information, so regardless of whether the malware is expelled from the gadget or the capacity media is moved to another gadget, the information isn't available. Ordinarily, Crypto Ransomware doesn't target basic framework records, empowering the gadget to keep on working disregarding being tainted—all things considered, the gadget could be expected to pay the payment.[5]

In late 90's and up until 2005, online ransom demanding strategies were not all that promptly accessible. Victims were demanded to pay ransoms by means of SMS instant messages or via mailing prepaid cards. Another normal ransom demanding technique was having the victim call a premium rate phone number that earned cash for the attackers.[3]

Ransomware truly took off when in 2008 Bitcoin came into utilization. Bitcoin is electronic cash that is a lot harder to follow and, in this manner, helped anonymize the exchanges. That made it troublesome or even difficult to find the attackers by following the ransom demanding persons.[6] While Bitcoins have the preferred position of being hard to difficult to follow, they do have dangers. The two significant dangers are gigantic conversion scale swings and hacking of major Bitcoin trades.[5]

When all is said and done, Crypto Ransomware moved toward Bitcoin. The contaminated PC remains completely useful after infected with a crypto Ransomware, so the client can utilize the PC to buy Bitcoins. With storage Ransomware, the PC is locked and hence unusable, making the acquisition of Bitcoins increasingly troublesome. It is in this way simpler for the person in question to purchase payment vouchers locally and enter a decryption code.[5]

Instalments in Bitcoin can be utilized straightforwardly due to the security of digital currency. In any case, numerous culprits are stressed over law requirement. Therefore, several Bitcoinwashing administrations have gotten accessible for offenders to utilize. There are additionally Bitcoin anonymizers that attackers can utilize.[5]

1.3 **Evolution of Ransomware:**

In 1989, The first Ransomware, called the AIDS Trojan (and referred as the PC Cyborg), was made by Joseph L. Popp. Popp was a Harvard-trained biological scholar. It was circulated by floppy disk at the World Health Organization's International Aids meeting. It utilized straightforward symmetric cryptography to scramble document names and tools were soon accessible to decode them.[4]

In 2005, the primary modern-day Ransomware was Trojan.GpCoder, which is also referred as GP Code and GPCoder. It was discharged in May 2005 and at first utilized a simple symmetric encryption system that was not effective. Its creators kept on improving the malware.[5] Trojan.GpCoder was spread by means of a spam email attachment that presented to be a request for employment.[7] Most of the early Ransomware was created in Russia by Russian attackers. It initially exploited the Russian people and aimed mostly to other nations, like Belarus, Ukraine, and Kazakhstan.[8]

Trojan.Cryzip appeared in March 2006. It used a commercial zip library to store the files in that zip file by deleting the original files which will be password-protected. A brute force attack is possible to determine the password for that zip file so recovering becomes easier.

Trojan.Archiveus in like manner proceeded the scene in 2006. It was the first Ransomware type that uses RSA encryption technique to encrypt the infected system. It worked a great deal of like Trojan.Cryzip, beside demanding a ransom, it anticipated that victims should buy prescription from online medication stores and present the solicitation ID in order to get the decryption key.[5]

In 2007, Locker Ransomware started to show up. Early forms struck in Russia and showed a pornography pictures on the machine and requested ransom to evacuate it, either by SMS instant message or calling a premium-rate telephone number. Attackers launched this Ransomware in Europe and the US.[4]

In 2008, a variation of Trojan.Gpcoder called GPcode.AK first showed up. It utilized a 1024-bit RSA key. It left a content document with directions in every subdirectory where it encrypted files. It requested ransom of $100 to $200 in e-gold.

In 2011, there was significant increase in Ransomware attacks because of increase in anonymous payment services. There were around 30,000 new Ransomware tests in quarter one and another 30,000 in quarter two. By quarter three, there were 60,000 new examples.[7]

In 2012, a toolkit called Citadel was discharged at an expense of about $3,000. Stronghold made it easy to deliver and disperse Ransomware.[9] Another toolkit, called Lyposit, additionally turned out in 2012. It was intended to create Ransomware that claims to originate from law authorization with the definite office contingent based on the PC's provincial settings

One variant made with Lyposit was known as Reveton. It showed a message saying the machine had been associated with child pornography action, downloading copyrighted material, or some other crime, and had been locked by the FBI or Justice Department.[7],[5]

Another early Ransomware was Trojan.Randsom.C. It satirizes a Windows Security Center message and asked the client to call to reactivate their Windows license.[5] An average attacker demanded ransom of around $300, and the attackers turned out to be considerably more capable.[5]

In 2013, the most acclaimed bit of Ransomware, CyptoLocker, was discharged in August by a hacker named Slavik. It utilized an asymmetric encryption method in which he used public and private cryptographic keys to encode, and later unscramble, a victim's data.

It was initially dispersed by means of the Gameover ZeuS banking Trojan botnet. Afterward, it was circulated by means of an email that seemed to originate from UPS or FedEx.[4] The first form of CryptoLocker encoded around 67 distinctive document types, including all Microsoft Office files.[10] CyptoLocker allowed victims three days to pay. Costs were around two Bitcoins, or $100 around then. Other payment techniques included are CashU, Ukash, Paysafecard, and MoneyPak. If the three-day cut-off time was not met, exploited people could pay a lot higher payment to recover their documents.

In November, the value of the two Bitcoin deliver expanded to about $460. Missing the first cut-off time raised the cost to ten Bitcoins. By December, 250,000 machines were compromised with Ransomware. It was discovered that 41,928 Bitcoins of payment had been paid.[7] In December, a copycat called Locker developed. Its payoff was $150, with instalment by Perfect Money or QIWI Visa Virtual Card number.

Afterward in December, CryptoLocker 2.0 was discharged. It was written in another language in comparison to CryptoLocker and so likely was discharged by various attackers. [7] During

2013, Symantec gauged that the quantity of attacks increased from 100,000 in January to 600,000 in December. They likewise determined that three percent of contaminated clients paid the ransom.[6]

From September 2013 to May 2014, it is identified that in excess of 500,000 victims were compromised with CryptoLocker. An expected 1.3 percent of exploited people paid the ransom.[10] In June, Activity Tovar, an alliance of law authorization organizations, security sellers, and scholastics, brought down the CryptoLocker dissemination servers. Two merchants, FireEye and Fox-IT found the database of decryption keys for all the CryptoLocker exploited people and discharged a help that considered free unscrambling by all victims.[8]

In February, CryptoDefense was discharged. It was a genuinely weak type of Ransomware, however still earned $34,000 in its first month. An improved adaptation called CryptoWall was discharged in April. It exploited the weakness in Java and was conveyed by means of spam advertisements.[7]

In 2015, the FBI evaluated that victims had paid $27 million in payments to the attackers behind CryptoLocker.[10] CryptoWall passed Cryptolocker as the main rendition of Ransomware.[7] An examination by Kaspersky found that for 2014-2015, Ransomware attacks increased by 17.7 percent in which crypto Ransomware attacks increased by 448 percent.[11]

In September, LockerPin was discharged. It compromised the Android devices and changed the PIN. It charges a $500 emancipate. In October, another report from the Cyber Danger Alliance announced complete Ransomware damage at $325,000,000.[7] In November, Linus.Encoder.1 was found by Dr. Web, a Russian PC security firm. As the name suggests, it targets Linux systems. It scrambles the two data documents and files related with web applications.[8]

In 2016, in January a JavaScript-just Ransomware-as-a service was found. Utilizing JavaScript permits for a multi-stage attack, including Linux and MacOS. In February, Ransomware tainted a huge number of WordPress destinations. WordPress is a well-known blogging stage. In April, a Ransomware called Petya turned up. Petya makes the entire hard disk unavailable until the ransom is paid. It does this by overwriting the Master boot record (MBR) of the compromised PC. Apple needed to discharge an update to prevent from the KeRanger Ransomware. KeRanger is the first Ransomware focusing on Apple PCs. Once introduced, KeRanger takes three days to operate and is intended to scramble more than 300 document types.[12]

In February, malware called Xbot was identified and it mostly compromised Android devices in Australia and Russia. In addition to the fact that it encrypts documents, it additionally attempts to discover the banking information from the infected devices.[13]

In July, the Locky Ransomware included a safeguard component that starts scrambling documents regardless of whether the Ransomware ask for encryption key from the offenders' servers because of the objective PC either being disconnected or obstructing the interchanges.[13]

The FBI stated that Ransomware produced $209,000,000 in the initial three months of 2016 and is on track to be a one-billion-dollar crime this year. During the first quarter, McAfee Labs estimated that there were around 1.2 million Ransomware attacks. Which was a 24-percent increase when compared to the fourth quarter of 2015.[15]

The three top forms of Ransomware right now are CryptoWall, CTB-Locker, and TorrentLocker. CryptoWall is an improved variant of CryptoDefense. It not only scrambles documents on the infected PC, but additionally focuses on any external capacity or shared drives associated to the PC. While, Torrent Locker exploits the email contact list of infected PCs in order to gain contacts from the compromised PC [3]

1.4 Ransomware to work, it requires more than Software

In order to compromise the system, we require more than the Ransomware software. The Ransomware must speak with a server to get an encryption key and report its outcomes. This requires a server facilitated by an organization that will overlook the criminal behaviour and assure the hiding of attacker's identity.

These facilitating organizations are called Impenetrable Hosting. Most of these kinds of organizations are situated in China or Russia. Attackers additionally utilize a proxy as middleman or VPN to further hide their own IP addresses.[9]

Today, Ransomware is an emerging issue across the globe. Since various parts of the world have various methods to pay, Ransomware like CryptoWall utilizes dynamic geological valuing. At the point when a PC is infected, CryptoWall checks with its command and control (C&C) server. It reports the IP address of the contaminated PC and the C&C server checks a database and returns a cost for the nation related with that IP address.[5]

In like manner, a few attackers targeted organizations as opposed to singular clients. Culprits realize they can charge organizations a lot of higher ransoms than individual persons. While organizations infrequently report attacks and the ransom paid, there is some curing proof. In 2012, a few Australian organizations detailed paying ransoms of up to AU$5,000 (US$4,750) and in 2015, a US online financial database got a demand of $50,000.[5]

As indicated by Liam O'Murchu, a security official at antivirus developer Symantec Corporation, the attacks related to organizations are focussed around small businesses, mainly because bigger firms have more data reinforcements, and networks that are compartmentalized by departments and highly knowledgeable security experts.[6]

1.5 If infected, then the question is to pay or not to pay ransom

People and organizations face the choice whether to pay or not to pay ransom when they are infected, and they don't have the data backup's in place. Accordingly, the choice comes down to two related inquiries. To begin with, is the information worth more than the payment? What's more, if this is true, what is the degree of possibility that the attacker will decrypt the information if the ransom is paid.

Also, there is an argument that paying the ransom will support the criminality. Given the measurement cited over that the FBI expected Ransomware would turn into a billion-dollar business in 2016, victims are obviously choosing to pay the ransom and recover their data.

Ransomware attackers appear to have enough negotiating prudence to understand that if they don't convey the decrypting key after the ransom is paid; their plan of action will fizzle, and exploited people will quit paying. Some Ransomware plans attempt to construct trust by decoding a couple of documents before the payment is paid. For instance, Trojan.Cryptolocker. G has the choice to decode five randomly chosen files.

In 2016, Kansas Heart Hospital paid the ransom when they were contaminated with an undisclosed Ransomware. Instead of decoding the records, the attackers demanded a subsequent payoff, which the emergency clinic would not pay.[16]

In some cases, it is recommended to negotiate before paying the ransom. In 2016, Hollywood Presbyterian Medical Center was hit with Ransomware that locked their PCs for over seven days. Instead of paying the underlying $3.7 million payment, the medical clinic returned to paper records until they had the option to bring the ransom down to 40 Bitcoins or about $17,000 [18]

In any case, experts give four reasons for why you should not pay the ransom. In the first place, you become a greater objective. Attackers talk and reveal to one another who paid and who didn't. Second, as talked about above, you can't confide in attackers to decode your information. CryptoWall has a notoriety for fantastic "customer service", while other malware families don't. Third, your next payoff will be higher. Maybe the attackers request a subsequent payoff before decoding your information or maybe you are infected a subsequent time. In any case, you will pay more. Fourth, your payment energizes the criminals to keep doing what they are doing.[17]

1.6 Ransomware Infection reports

As indicated by Osterman Research, Inc., from June 2015 to June 2016, 59 percent of Ransomware infections came by means of email, in the form of malicious links or malicious attachments in that email. Another 24 percent came by means of visiting a malicious website or web application. Other eight percent come by social media, USB stick, or business application, and nine percent were of obscure birthplace. When contaminated, just three percent of US organizations paid the ransom, while 75 percent of Canadian organizations paid.[18]

Symantec utilizes telemetry information to follow Ransomware contaminations by nation. The rankings appear in the Table 1 below. Generally, attackers are focusing on huge or well-to-do nations.[5]

During recent years, 64 percent of Ransomware infections have been crypto Ransomware, while 36 percent has been Locker Ransomware[18]

Rank	Country
1	USA
2	Japan
3	UK
4	Italy
5	Germany
6	Russia
7	Canada
8	Australia
9	India
10	Netherlands
11	Brazil
12	Turkey

Table 1: Top 12 Countries impacted by Ransomware[18]

1.7 Future Trends in Ransomware

Law organizations and computer security sellers like Symantec, are beginning to focus on Ransomware. This has constrained the attackers to change the way they work, with more utilizing Tor and the Invisible Internet Task (I2P) to conceal their tracks.

In like manner, more are going to digital forms of money like Bitcoin to hide the cash trail. As the weight on Ransomware builds, the attackers will probably search for more approaches to block and muddle endeavours to follow and comprehend their exercises.[5]

As of now, Locker Ransomware that attacks smart watches has been identified. As the world moves to the Internet of Things (IoT), there is no uncertainty that Ransomware will move to the IoT too. While that may appear implausible from the outset, analysts have just had the option to assume control over the PC frameworks of a moving Jeep Cherokee. On the off chance that scientists can do it, so can Ransomware.[5] By then, the cost may not be money but your life.

The big money can be made by attacking organizations, thus far, Crypto Ransomware is a generally safe, high yield attempt with practically zero dread of law organizations indicting attackers in the uncommon occasion the contamination is accounted for and most infections go unreported. Organizations often don't report since they would prefer not to make things more regrettable or become focuses for other attackers.[19]

From June 2015 to June 2016, as per a review by Osterman Research Inc., 79 percent of organizations in the US were compromised with at least one Ransomware attack and 22 percent endured more than twenty[18] In these assaults, 78 percent detailed that individuals were affected, 12 percent announced the business halted quickly, 11 percent detailed that personnel needed to utilize personal computers while corporate systems were down, and six percent lost income subsequently.[18] .The highly attacked four industries were Health Services, Financial institutions, Manufacturing industries, and Government sectors.[18]

At present, most Ransomware rapidly declares that it has scrambled information records to quickly collect the ransom. Some Ransomware is moving to postponed declarations, at the same time encoding files in the background. That enables the scrambled documents to unobtrusively overwrite files in backups, making it harder to recover data from the Ransomware utilizing backups [54]

It is additionally getting increasingly regular for Ransomware to take steps to disclose documents publicly except if the ransom is paid. As indicated by FireEye, one organization paid more than one million dollars to prevent sensitive information from being disclosed [54] .This has genuine potential for both expense and humiliation.

Attackers are additionally searching for additional assault vectors. In late 2016, they started utilizing SVG (versatile vector illustrations) records via web-based networking media as an assault strategy. SVG records permit PC code, for example, JavaScript, to be inserted in the Graphic. That code can be opened and executed by means of a web browser.

In late 2016, the Locky malware was being propagated by means of a Word macro.[14] One adaptation of Ransomware that was identified by Malware Hunter Team called Popcorn Time, in which attackers find ways to make victims as criminals by threating them to compromise other systems in order to get decryption key to decrypt the encrypted files without paying ransom [55]

2.ANALYSIS OF RANSOMWARE ATTACK

2.1 Phases of Ransomware activity

It is important to understand the stages of Ransomware attack before driving through the models and prevention methods of Ransomware. The below figure represents the stages of Ransomware attacks.

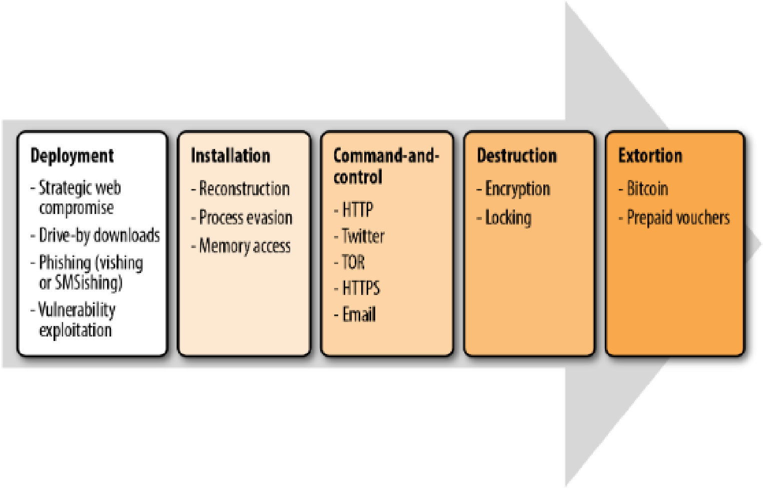


Figure 2: Stages in Ransomware attack [21]

a) *Deployment:*

There are multiple methods to deliver the Ransomware malware into targeting systems. The various methods used are represented in deployment phase in the above figure, such as "drive-by-downloads" which automatically installs malware into the victims system without user interaction, social engineering techniques like phishing to send emails to an individual victim or a group of individuals by including malicious links or malicious attachments to email which installs malware into victims system when the user clicks on or opens them.[22]

Some other deployment methods of Ransomware malware are comprising a trusted website visited by many users, which is referred to as watering hole attacks. When the victim visits the compromised website, it will automatically install the malicious software into a system without user knowledge.

b) *Installation:*

Second stage of a Ransomware activity is the installation, which means the Ransomware is infected into system. After getting infected into system it will not immediately start encrypting the data files. When infecting windows systems, Crypto Ransomware sets the keys in the windows registry and starts automatically when the system boots up every time.[23] Sometimes the components will be broken into several chunks of scripts, embedded to other tools to bypass the detection of antivirus or antimalware solutions.[22]

c) *Command- and- Control:*

Once Ransomware gets installed into system, it actively starts to communicate with Command-and-Control (C&C) server in order to get the instructions from C&C server. C&C servers are managed by attackers and they send instructions from that to all the compromised systems. The main reason for communicating with the C&C server is to get the encryption key required to encrypt the data in the infected system.

d) *Destruction:*

After getting instructions and encryption keys from the C&C server, Ransomware starts searching for the contents in the compromised system in order to start encryption of data. For e.g., WannaCry encrypts the files of infected system with "*.wncry*" extensions. The Ransomware can encrypt any kind of Microsoft office documents, files such as JPG, GIF and many other file types.[22]

e) *Extortion:*

Finally, after encrypting the files of infected system the extortion phase Ransomware displays a message on the victim's screen stating that the files are compromised and in order to regain access to data the victim needs to pay ransom within a determined deadline. The amount of ransom demanded varies between variants of Ransomware and in general most variants of Ransomware demands a ransom of worth \$300 - \$500.[22]

2.2 Components of WannaCry Ransomware

The key motive behind launching Ransomware attacks is to encrypt the data and to demand ransom to get the decryption key. Among all the kinds of available Ransomware, WannaCry is the highly effective and it spread across 150 countries. The below figure shows the countries that were affected with WannaCry Ransomware[23]

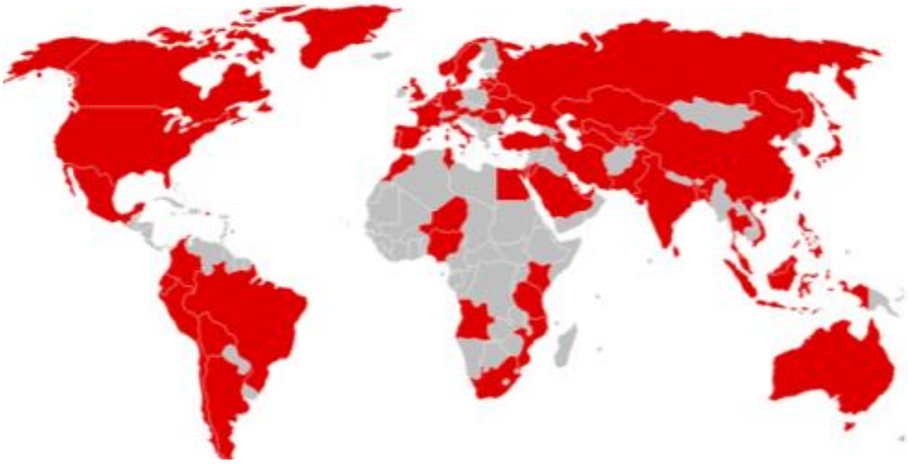


Figure 3: Distribution of WannaCry Ransomware [23]

WannaCry has become so strong because of its strong encryption technologies and its distribution mechanisms.

Generally, Ransomware attacks comes mostly in two structures: Locker and Crypto Ransomware. Crypto Ransomware is again divided as Private-key Crypto Ransomware (PrCR) and Public-key Crypto Ransomware (PuCR). PrCR acquires the challenge of symmetric key which can be determined by using crypto analysis. This disadvantages of symmetric key PrCR makes it crackable. This has subsequently prompted the across the board usage of PuCR over PrCR. [23]

The figure below shows the conventional structure of crypto Ransomware payload normal in both PrCR and PuCR. Here the question is how the encryption key will be generated when infected with Ransomware. Depending on the structure of attack, it can be embedded in the Ransomware payload delivered, or it can be retrieved from the C&C server.

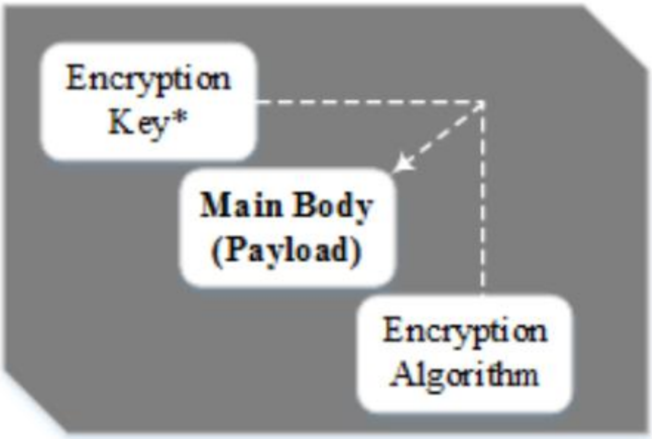


Figure 4: General structure of crypto Ransomware [23]

2.3 Crypto Ransomware comprises of three major components they are:

a) *Encryption Methodology*

As we know from our studies that encryption is the key in Ransomware. So, attackers started using the most advanced encryption algorithms like AES, RSA etc without any compromises. Due to the speed advantage of symmetric encryption attackers developed model of hybrid attack structure in which attackers started encrypted symmetric key which is data encrypting key by using asymmetric encryption technologies. Figure 3 underneath outlines the attack structure of hybrid crypto Ransomware [23]

In the above attack structure, the general public key *Kp* created from the PuCR key pair {*Kp*, *Ks*} is embedded into the payload is utilized to scramble the symmetric key Ksecret which encodes the infected victims' documents. In this methodology, the key Ksecret for unscrambling client information, having been encoded by *Kp*, must be decoded by the private key *Ks* residing on the C2 servers.

Client information encryption, which is the real Ransomware attack is defined by *Ci*. In other attack structures, the Ransomware payload creates an asymmetric key pair of which the general public key is utilized to encode client information while the Ransomware looks to exfiltrate the private key to the C2 servers for future decryption.[23]

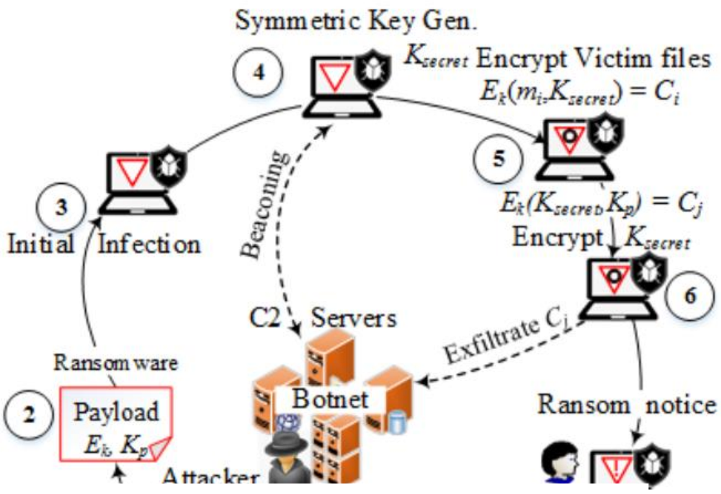


Figure 5: Hybrid PuCR attack structure [23]

b) *Command-and-Control Servers:*

The center of operations of a Ransomware attack relies on Command-and-Control (C&C) servers. These can be owned by attacker or it can be a botnet which is compromised and managed by attacker. Once the Ransomware is infected then the payload of it will communicate with the C&C server to retrieve the encryption key. All the encryption keys and ransom payments will be managed by this C&C server. So, when Ransomware payload is delivered to victim it contacts C&C server for the instructions.

c) *Infection Vectors:*

The key component of the Ransomware attack is the methods that we use to deliver the Ransomware payload into victim's system. This is the key component for succeeded in the launching of any kind of attacks.

An effective delivery method should be in place to ensure that the Ransomware is delivered to the targeted system. Attackers achieve this by using infection vectors and they use both the simplex and complex methods. Among all the available methods spam email tops the infection vector list and ensures the maximum successful delivery of Ransomware payloads.[23] The below figure shows these various infection vectors.

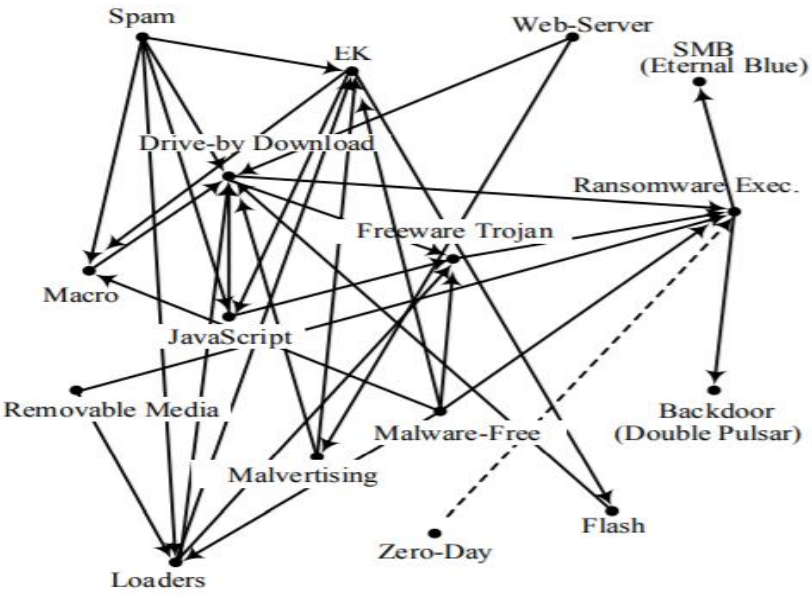


Figure 6: Infection Vector Methods [23]

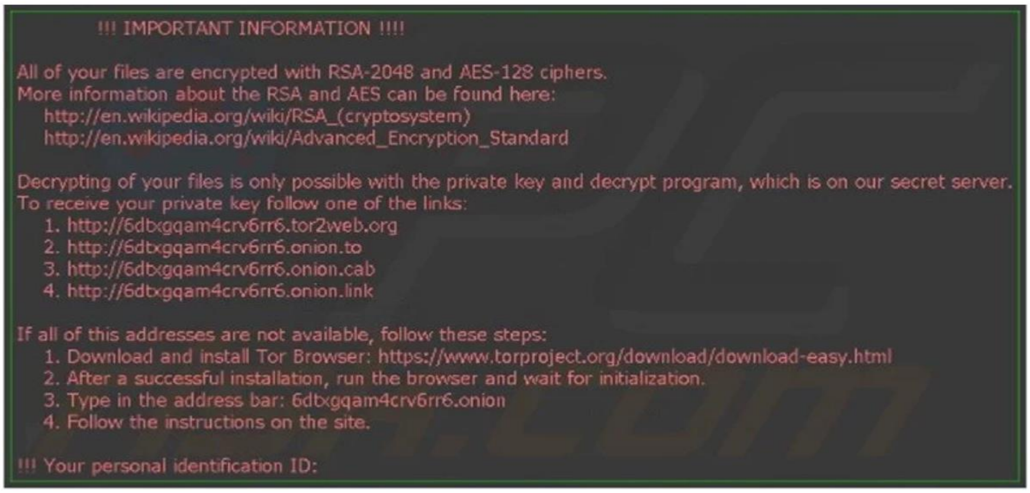
3. MODELS OF RANSOMWARE

Presently you comprehend what Ransomware is and the two principle kinds of Ransomware are Locker and Crypto that exist. We will now investigate 8 acclaimed Ransomware to assist you with seeing how extraordinary and risky each type can be.

3.1 Locky Ransomware

Locky is a kind of Ransomware that was first discharged in a 2016 by a sorted out gathering of hackers, it has the capacity to scramble more than 160 file types. The most common infection vector of Locky Ransomware is phishing emails with malicious attachments which will open in Microsoft word and pop up a notification asking the victim to enable macros to correct the encoded document sent by an attacker in the infected system.[24]

After enabling macros, it enables the malicious code in the Ransomware payload to execute and it starts encrypting several file types like images, videos and many other file types in the compromised system. Locky Ransomware encrypts all the infected system files with "*.locky*" extensions.[24] The below figure represents the message displayed by the Locky Ransomware which demands the victim to pay ransom.



```
          !!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
    http://en.wikipedia.org/wiki/RSA_(cryptosystem)
    http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:
    1. http://6dtxgqam4crv6rr6.tor2web.org
    2. http://6dtxgqam4crv6rr6.onion.to
    3. http://6dtxgqam4crv6rr6.onion.cab
    4. http://6dtxgqam4crv6rr6.onion.link

If all of this addresses are not available, follow these steps:
    1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
    2. After a successful installation, run the browser and wait for initialization.
    3. Type in the address bar: 6dtxgqam4crv6rr6.onion
    4. Follow the instructions on the site.

!!! Your personal identification ID:
```

Figure 7: Locky Ransomware displaying message[25]

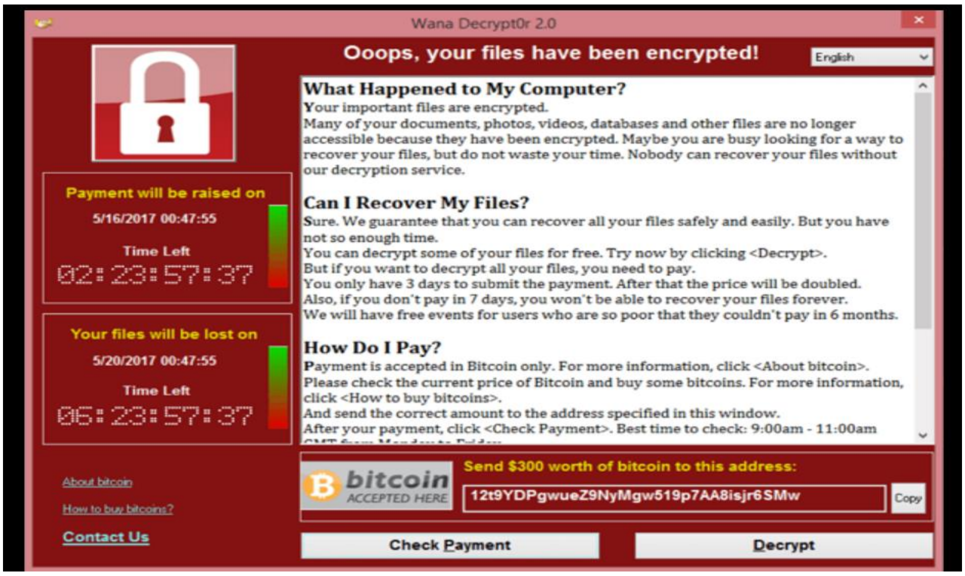
Locky Ransomware uses the strong encryption algorithms like Advance Encryption Standard and RSA. The major difference of Locky, when compared to other kinds of Ransomware is in size of payload and the encryption algorithms used by the Locky. To prevent Locky Ransomware we should not enable the macros in Microsoft word, take regular backups of data and provide awareness training to individuals on phishing email techniques.[25]

3.2 WannaCry Ransomware

WannaCry Ransomware spread over 150 nations in 2017. It was intended to exploit a vulnerability in Windows; it was supposedly made by the group of hackers called as Shadow Brokers gathering. WannaCry influenced 230,000 PCs all around. This infected about 33% of medical clinic confides in the UK, costing the NHS an expected £92 million[26]

WannaCry is the example of a Crypto Ransomware which is a type of malware that encrypts the victim's data and demands ransom. It spread across the world by exploiting the Windows operating systems that were not updated with the latest patches. So, the main reason for this Ransomware infection is due to the lack of knowledge by individuals on the importance of updating the systems.[26]

The attackers of WannaCry demanded a ransom of $300 to $600 worth of Bitcoin with a determined deadline of three days. If the victim fails to pay the ransom within the determined time, then the attackers told victims that the files will be deleted. The below figure represents the message sent by the WannaCry to the victim.



Ooops, your files have been encrypted!

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

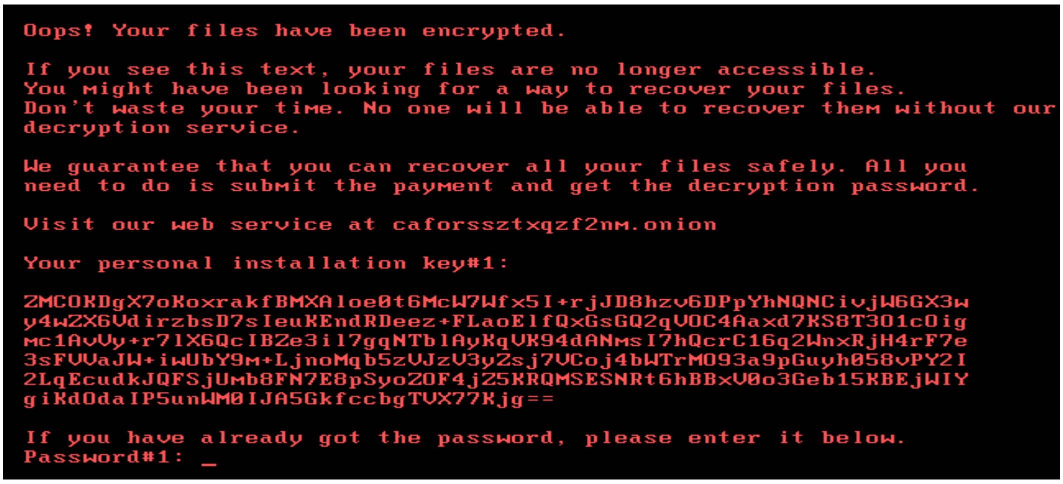
Figure 8: WannaCry Ransomware demanding ransom[27]

Two months prior to this attack, Microsoft released a security update and many individuals and organizations didn't update their systems with the patches released. Then attackers exploited all the vulnerable systems. So, it is highly recommended to keep systems up to date with patch updates and awareness training should be provided to employees by the organization about the importance of patch updates.

3.3 Bad Rabbit Ransomware

Bad Rabbit is a 2017 Ransomware attack that spread utilizing a technique called a 'drive-by' assault, where insecure sites are targeted and compromised on and used to complete an attack. During a drive-by download, a victim visits a legitimate site, not realizing that they have been downloading malware automatically.

This Ransomware does not spread widely like other kinds such as WannaCry and Locky. It was seen majorly in Russia and Ukraine. This Ransomware is disguised as Adobe Flash Installer, when the victim clicks to install it then it starts encrypting victim's data. This Ransomware demanded a ransom of around $280 and attackers gave a time period of 40-hour deadline to pay ransom.[28] The below figure represents the ransom message shown by Bad Rabbit Ransomware.



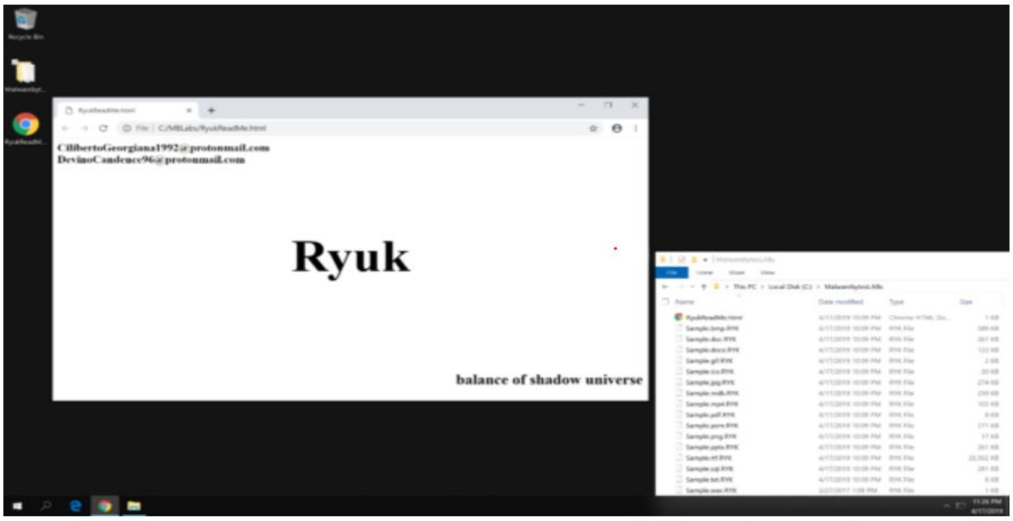
```
Oops! Your files have been encrypted.

If you see this text, your files are no longer accessible.
You might have been looking for a way to recover your files.
Don't waste your time. No one will be able to recover them without our
decryption service.

We guarantee that you can recover all your files safely. All you
need to do is submit the payment and get the decryption password.

Visit our web service at caforssztxqzf2nm.onion

Your personal installation key#1:

ZMCOKDgX7oKoxrakfBMXAloe0t6McW7Wfx5I+rjJD8hzv6DPpYhNQNCivjW6GX3w
y4wZX6VdirzbsD7sIeuKEndRDeez+FLaoElfQxGsGQ2qVOC4Aaxd7KS8T3O1cOig
mc1AvVy+r7lX6QcIBZe3il7gqNTblAyKqVK94dANmsI7hQcrC16q2WnxRjH4rF7e
3sFVVaJW+iwUbY9m+LjnoMqb5zVJzV3yZsj7VCoj4bWTrMO93a9pGuyh058vPY2I
2LqEcudkJQFSjUmb8FN7E8pSyoZOF4jZ5KRQMSESNRt6hBBxV0o3Geb15KBEjWIY
giKdOdaIP5unWM0IJA5GkfccbgTVX77Kjg==

If you have already got the password, please enter it below.
Password#1: _
```

Figure 9: Bad Rabbit Ransom Message[29]

3.4 Ryuk Ransomware

Ryuk Ransomware spread in August 2018. This Ransomware is mainly designed to target the critical system in the network and then attackers started spreading it across the network manually. Check point security analysts stated thar Ryuk Ransomware doesn't have a feature of automatic spreading.

It used strong encryptions algorithms like AES, RSA key pairs to encrypt the data of infected systems. Ryuk Ransomware was not spread widely, hence it makes difficult to track the malware authors.[30] The below figure represents the images displayed by Ryuk Ransomware on the infected system.



CilibertoGeorgiana1992@protonmail.com
DevinoCandence96@protonmail.com

Ryuk

balance of shadow universe

Figure 10: Images displayed by Ryuk on Infected system[30]

3.5 Troldesh Ransomware

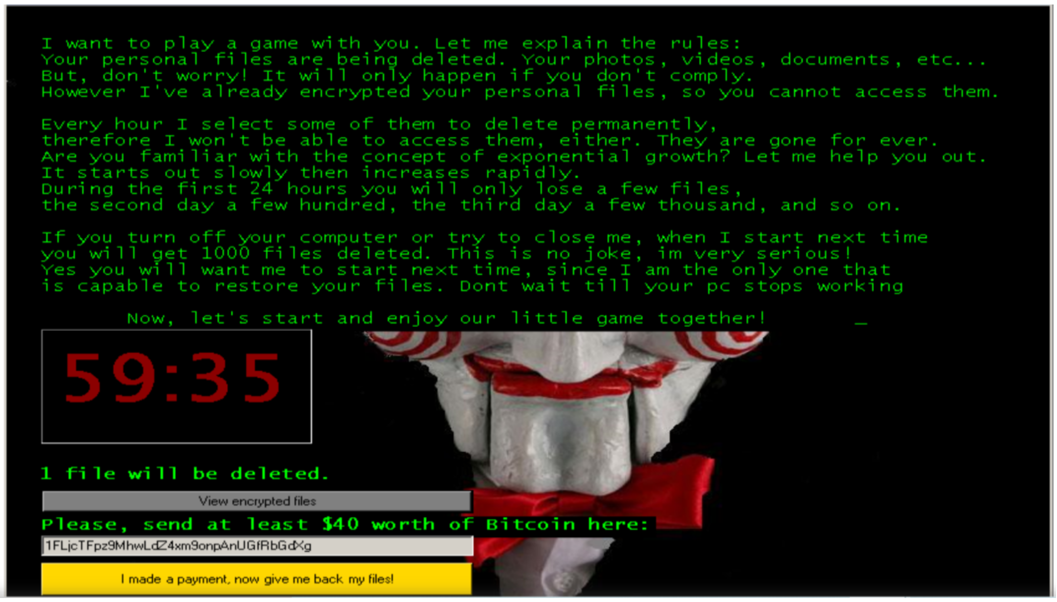
The Troldesh Ransomware attack occurred in 2015 and was spread through spam email with malicious attachments. It included Zip files as malicious attachments and tricked the victim into opening that Zip file quickly. The downloaded zip file is a JavaScript that downloads malicious content into the victim system. Infection vector for Troldesh is mostly phishing.[31]

It is believed that Troldesh originated from Russia as ransom note displayed by this is written in both Russian and English. Behaviour of this Ransomware is it starts creating the numbered text files after encrypting the infected system files and every text file contains the message of ransom note. Some of the protection methods against this Ransomware is using anti-malware solutions, user education about phishing emails, backup files, etc.[31]

3.6 Jigsaw Ransomware

Jigsaw is a Ransomware attack that began in 2016. This attack got its name as it included a picture of the manikin from the "Saw" film establishment. Once the system was infected with Jigsaw, it starts a time counter.

If the demanded ransom is not paid within an hour, then it will delete one file. As this Ransomware deletes files on a timely manner it is crucial for victims to respond as quickly as possible after encryption. Jigsaw uses a strong AES encryption algorithm.[32] The below figure presents the image displayed by the Jigsaw Ransomware on the infected system.



```
I want to play a game with you. Let me explain the rules:
Your personal files are being deleted. Your photos, videos, documents, etc...
But, don't worry! It will only happen if you don't comply.
However I've already encrypted your personal files, so you cannot access them.

Every hour I select some of them to delete permanently,
therefore I won't be able to access them, either. They are gone for ever.
Are you familiar with the concept of exponential growth? Let me help you out.
It starts out slowly then increases rapidly.
During the first 24 hours you will only lose a few files,
the second day a few hundred, the third day a few thousand, and so on.

If you turn off your computer or try to close me, when I start next time
you will get 1000 files deleted. This is no joke, im very serious!
Yes you will want me to start next time, since I am the only one that
is capable to restore your files. Dont wait till your pc stops working

        Now, let's start and enjoy our little game together!
```

1 file will be deleted.

Please, send at least $40 worth of Bitcoin here:

1FLjcTFpz9MhwLdZ4xm9onpAnUGfRbGdXg

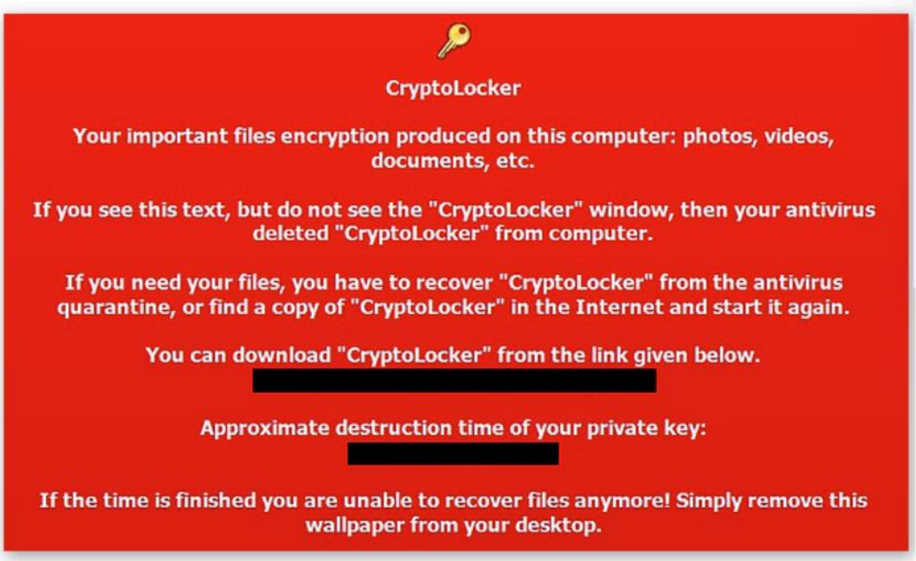
Figure 11: Jigsaw message on Victims system[20]

3.7 CryptoLocker Ransomware

CryptoLocker is a Ransomware that was first observed in 2013 and spread through emails with malicious attachments. To spread the CryptoLocker to other systems the attackers used a Zeus botnet. But, in Mid 2014 Zeus botnet was taken down by experts and made the CryptoLocker decryption keys available for free to the victims.[33]

Once on your PC, it scans for significant documents to scramble and hold to emancipate. Thought to have infected around 500,000 PCs, law organizations and security organizations in the long run figured out how to hold onto an overall system of seized home PCs that were being utilized to spread Cryptolocker.

This enabled them to control some portion of the criminal system and get the information as it was being sent, without the lawbreakers knowing. This activity later prompted the advancement of an online entrance where exploited people could get a key to open and discharge their information without paying the ransom. The below figure shows an example of a message displayed by the CryptoLocker Ransomware demanding the ransom.



CryptoLocker

Your important files encryption produced on this computer: photos, videos, documents, etc.

If you see this text, but do not see the "CryptoLocker" window, then your antivirus deleted "CryptoLocker" from computer.

If you need your files, you have to recover "CryptoLocker" from the antivirus quarantine, or find a copy of "CryptoLocker" in the Internet and start it again.

You can download "CryptoLocker" from the link given below.

[redacted]

Approximate destruction time of your private key:

[redacted]

If the time is finished you are unable to recover files anymore! Simply remove this wallpaper from your desktop.

Figure 12: CryptoLocker ransom message[33]

3.8 Petya Ransomware

Petya (not to be mistaken for ExPetr) is a Ransomware attack that originally hit in 2016 and resurged in 2017 as GoldenEye. As opposed to encoding explicit documents, this horrendous Ransomware scrambled the victims whole hard drive. Once infected it starts encrypting the Master Boot Record and sends notification to victim to conduct the reboot of the system. When user does reboot, it locks out the victim from gaining access to system. Petya virus is launched using spam or phishing emails.[34]

3.9 GoldenEye Ransomware

The resurgence of Petya, known as GoldenEye, a Ransomware attack that happened in 2017. It is delivered by using phishing emails and first sample of it was recorded in Germany. Once GoldenEye malware is infected into victim's system then the malware installs its files in %APPDATA% directory with some random application name.

This installed copy is executed automatically without any user interaction. First it encrypts all the files and then it uses privilege escalation techniques in order to start encrypting the drives. The prevention technique from this malware is to carefully be clicking the links received via emails.[35]

3.10 GandCrab Ransomware

GandCrab initially hit in January 2018, it encrypted the user's data and demands ransom in order to regain access to data. Reports stated that GandCrab does was not seen in Russia, so it is believed that is originated from Russia.

It displays a ransom note on victims' computer that redirects victim to the dark web. Because of weaker encryption techniques used by authors of GandCrab, cybersecurity researchers developed the free decryption tool. Some of the prevention methods are taking backup's, educating on phishing emails and finally when infected with GandCrab don't pay the ransom as servers are not active.[36]

4. ATTACK VECTORS

Regularly, malware needs the assistance of people to enter PCs, so they utilize what's known as social engineering. With regards to information security, social engineering is the practice of using techniques in order to trick the victim into clicking on some malicious link which leads to the installation of malware onto the targeted system. Ransomware can be delivered from two kinds of attack vectors such as Human attack vectors and Machine attack vectors.

4.1 Different types of Human attack vectors are:

a) *Phishing*

Phishing is a technique which uses email platform to send malicious links and malicious attachments to the targeted victims. Attackers can send phishing emails to individual or to a group of people called "spear phishing". While using phishing techniques attackers take time in order to impersonate as email from legitimate source. Even they can target top level executives of organization called "whaling". Once the victim clicks the link sent by attacker then it redirects to malicious site which installs Ransomware into victim's system.[37]

b) *SMSishing*

SMSishing is a practice of using instant messages to make victims visit to a malicious site or enter sensitive data on their device. Regular methodologies use verification messages or messages that give off an impression of being from a financial institution. Some SMSishing Ransomware endeavour to spread themselves by sending themselves to all contacts in the victim device's contacts list.[37]

c) *Vishing*

Like email and SMS, vishing uses the technique of sending voice message to the victim device. The voice message is told to call a number that is frequently faked to seem genuine.

On the off chance that the victim calls the number, the person in question is taken through a progression of activities to address some made-up issue. The directions incorporate having the victim to reveal sensitive information or allowing to install malware on their PC. Cybercriminals can seem proficient and utilize audio cues and different intends to seem genuine. Vishing can be focused on an individual or organization utilizing data that the cybercriminals have gathered.[37]

d) *Social Media*

Social Media can be an incredible method to persuade a targeted individual to open a downloaded picture from a social media webpage or make some other bargaining move. The transporter may be music, video, or other dynamic substance that once opened infects the victim's machine.[37]

4.2 Machine Attack Vectors

The other kind of attack vectors are machines. Some of Machine attack vectors are:

a) *Drive-By Download*

Drive-by download makes the victim open a site which contains malicious code, once the victim visits the site the malware will be installed automatically to the victim's system without their knowledge.[37]

b) *System Vulnerabilities*

Cybercriminals gain information with the vulnerabilities of systems and exploit those vulnerabilities to break in and install Ransomware on the machine. This frequently happens to systems that are not updated with the most recent security patches, not updated with the latest OS and missing updated software packages.[37]

c) *Malvertising*

Malvertising resembles drive-by, however utilizes advertisements to deliver malware. These advertisements may be put on web crawlers or well-known social media sites in order to infect many people.[37]

d) *Network Propagation*

Once the Ransomware compromises the system on a network. Then it can start scanning itself for file shares and starts encrypting them and starts spreading infection across the network. If organizations does not have adequate security policies in place then it can even spread to shared network storages and has the capability of spreading infection across the organization[37].

5. ANALYSIS OF EXISTING PREVENTION METHODS OF RANSOMWARE

Ransomware malware can be infected into any type of computing equipment, among all the computing equipment the end-user devices receive the largest percentage of Ransomware infections. Top ten best prevention techniques to prevent the systems getting infected from Ransomware and other kinds of malware are:

1. Installing Anti-malware Solutions
2. Ensuring systems are up to date with latest patches
3. Training and User Education
4. Segmentation of Network
5. Deploying Anti-Ransomware solutions
6. Data backups
7. Firewalls
8. Honeypots and IDS/IPS
9. Security Policy
10. Incident Response Plan

5.1 Installing the security solutions like Anti- virus / Anti-malware software:

Anti-virus solutions are considered as the first defencing technique used by the computing systems to prevent Ransomware. There are many anti-virus solutions available in the market with built in Firewall, and other features like anti-phishing and anti-spam adds an additional layer of defence to prevent from malware infection. It is time to talk about how anti-virus solutions detect and prevent the malware from infection [38]

Some of the detection techniques used by antivirus solutions to detect the patterns of malware are:

a) *Signature- Based detection:*

   This detection technique consists of a database of signature patterns of malware. Antivirus vendors identify the malware first, then they add patterns of malware to the signature database then they release for customers.

This type of detection technique is most widely used in home environment antivirus solutions. But the disadvantage with this detection technique is it will not detect the new patterns of Ransomware malware which is introduced for first time. [38]

b) *Behaviour based detection:*

In this detection technique antivirus vendors analyse the behaviour of Ransomware when it has infected a system, like what it is doing to data in the system like encrypting, deleting etc. In this method it alerts and stops the attack. [38]

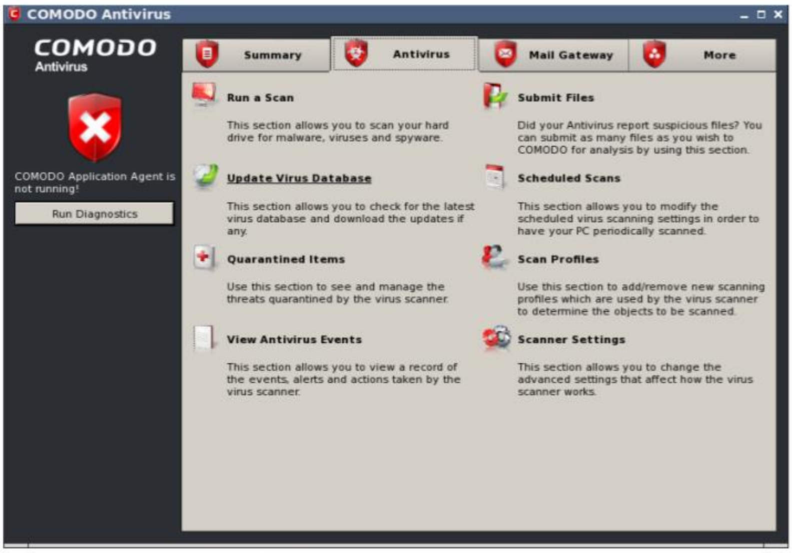
c) *Sandboxing:*

In sandboxing technique, if antivirus solution detects any malware suspicious file then it immediately isolates that file into a virtual environment so that it can stop the malware infecting the host. [38]

Some of the recommendations before purchasing an antivirus solution are: [38]

- Ensure that the anti-virus solution has additional features like anti-phishing, anti-spam as phishing and spam are the top infection vectors for most Ransomware models
- Antivirus solution should have automatic update, signature database files should be kept up to date.
- Antivirus solution should have the capability of scanning the external USB drives when connected to end devices to prevent from infecting malware.

The below figure represents the Graphical User Interface of one of the popular Antivirus solutions Comodo and it includes multiple features like inspection of compressed files and folders and scans them for malware patterns, after scanning files, if it identifies any files with malware it has the feature of isolating them to prevent the spread, every antivirus solution has scanner feature in order to scan the documents, they contain signature databases of malware patterns which need to be updated regularly, inbuilt firewall feature to inspect the network outgoing and incoming traffic, feature of self-protection to protect it from malware etc [52]



COMODO Application Agent is not running!

Run a Scan

This section allows you to scan your hard drive for malware, viruses and spyware.

Submit Files

Did your Antivirus report suspicious files? You can submit as many files as you wish to COMODO for analysis by using this section.

Update Virus Database

This section allows you to check for the latest virus database and download the updates if any.

Scheduled Scans

This section allows you to modify the scheduled virus scanning settings in order to have your PC periodically scanned.

Quarantined Items

Use this section to see and manage the threats quarantined by the virus scanner.

Scan Profiles

Use this section to add/remove new scanning profiles which are used by the virus scanner to determine the objects to be scanned.

View Antivirus Events

This section allows you to view a record of the events, alerts and actions taken by the virus scanner.

Scanner Settings

This section allows you to change the advanced settings that affect how the virus scanner works.

Figure 13: GUI of Comodo Antivirus [52]

5.2 Install System and OS updates:

To prevent an infection of Ransomware we must keep our system OS up to date with installed current patches and to keep the system up to date with security updates and application package updates. Because unpatched systems are vulnerable, and attackers start exploiting them once they determine systems is vulnerable. For example, WannaCry Ransomware exploited the Windows systems that were not patched.[39]

We need to configure our operating system to be updated automatically, and it also should include the automatic updating of antivirus solutions, application packages etc. Many of the operating system vendors support the automatic updating of OS, for e.g.: Microsoft windows systems supports automatic updates. Though we can turn it off manually it is highly recommended to always turn on the automatic update feature.[40]

When software vendors identify any bugs in the system applications, OS or security features they write the code and release the patch to overcome the bugs. So, if we are not keeping systems with current patches then it causes systems to be vulnerable and encourages attackers to launch malicious attacks like Ransomware. Outdated computer systems are highly vulnerable to Ransomware attacks.[39]

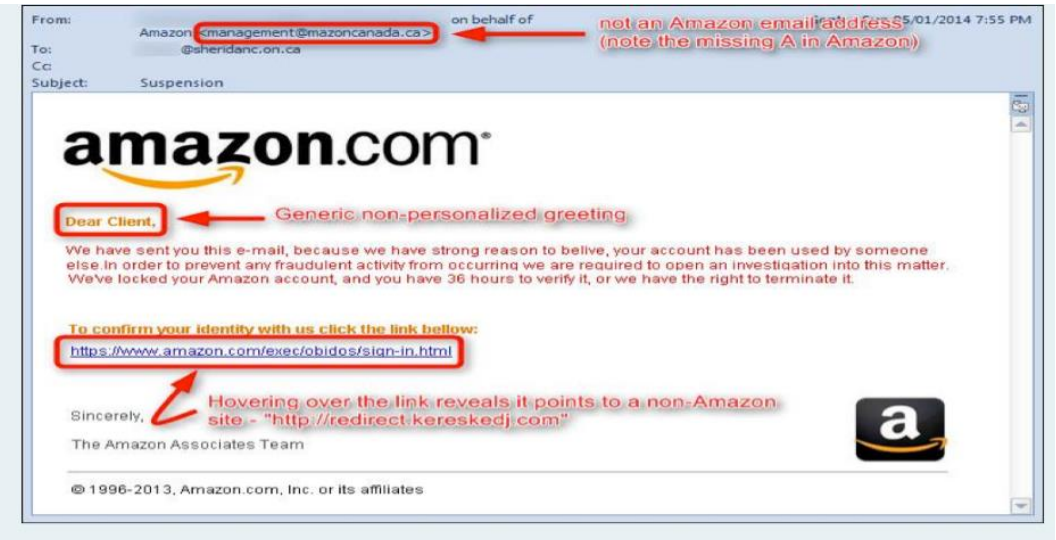
5.3 User Education

One of the common methods that attackers follow to launch Ransomware attacks is using social engineering techniques like phishing, vishing and spear phishing. It is highly recommended that organizations should educate employees and provide security awareness trainings on malicious emails, spam emails, malicious websites and other kind of social engineering techniques.[40]

All recent studies indicate that attacks related to Ransomware are mostly because of human errors due to lack of knowledge on social engineering techniques. Security awareness training will help employees to understand the different threats that they might see when using organizations systems and train them how to eradicate them. [38]

Educating employees on how to deal with emails from unknown sources and emails including malicious links and malicious attachments will prevent the maximum number of Ransomware attacks.[38]

The below figure represents the sample phishing email from attackers trying to impersonate as email from Amazon [51]



From: Amazon <management@mazoncanada.ca> on behalf of
5/01/2014 7:55 PM
To: @sheridanc.on.ca
Cc:
Subject: Suspension

not an Amazon email address (note the missing A in Amazon)

Dear Client,

Generic non-personalized greeting

We have sent you this e-mail, because we have strong reason to belive, your account has been used by someone else.In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter. We've locked your Amazon account, and you have 36 hours to verify it, or we have the right to terminate it.

To confirm your identity with us click the link bellow:

https://www.amazon.com/exec/obidos/sign-in.html

Hovering over the link reveals it points to a non-Amazon site - "http://redirect.kereskedj.com"

Sincerely,

The Amazon Associates Team

© 1996-2013, Amazon.com, Inc. or its affiliates

Figure 14: Sample of Phishing email [51]

5.4 Network Segmentation:

Segmentation of larger networks is also one of the effective prevention techniques for preventing Ransomware because, by segmenting the larger network into smaller networks we can prevent the spreading of Ransomware across the larger network. It also allows us to store the sensitive data separately in a secured environment and prevent attackers from discovering it. [38]

When we did not do the segmentation of network, if one system gets infected then it will spread across the network and begin infecting other systems in the network. The below figure represents the network topology without segmentation.

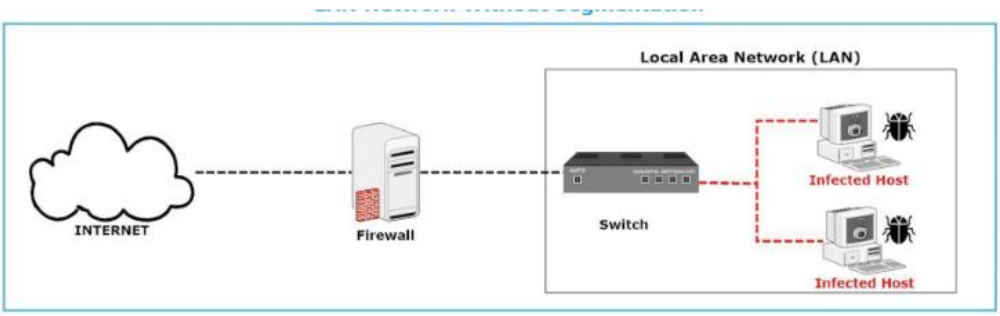


Figure 15: Infected host infecting the other systems [38]

Let’s consider another case where we segmented our network and place a firewall between them which means all the communications between the networks should go through the firewall. So, if one system in the network gets infected with Ransomware and if that system tries to communicate with the systems in other network the packet will be sent to the firewall and the firewall drops out that packet when it detects the malicious malware in it.

The below figure represents the method of preventing Ransomware by segmenting into multiple networks.

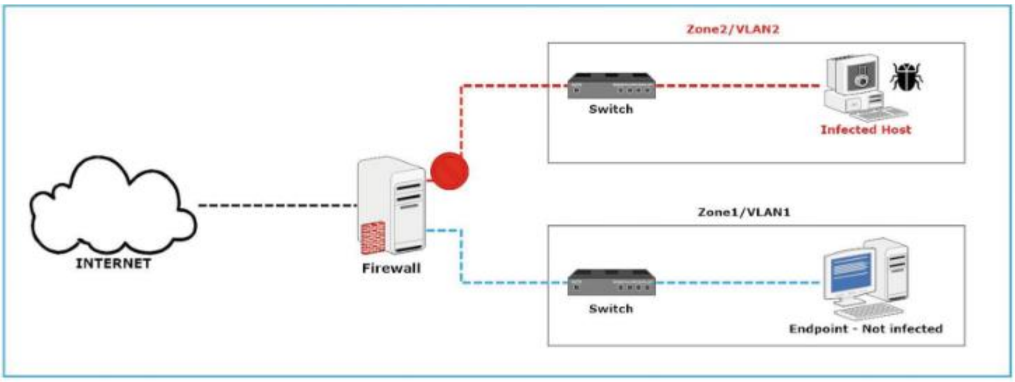


Figure 16: Separating the Networks prevents the spread of Ransomware [38]

5.5 Deploy Anti- Ransomware products:

Presence of antivirus solutions does not guarantee the prevention of infection of Ransomware, so it is highly recommended to install anti-Ransomware products available in the market.

They use behavioural detection and cloud-based detection techniques to detect the patterns of Ransomware and stop it. Best example for this kind of solution is Windows 10 firewall defender which has a built-in Ransomware protection feature.

Ransomware protection in Windows 10 systems, prevents unauthorized applications from gaining access to critical system files and important personal data files.[41]

5.6 Taking backups of systems:

The important prevention technique from Ransomware is to always take backups of your system and it is recommended to keep the multiple backups in multiple sources like the cloud and remote locations so that organizations can implement methods to clean the infected systems. They can then take the data from backups without paying any ransom to the attacker.

Among all the backups a cloud backup will be more beneficial as it resides in cloud providers network so that it will be safe even if our network is infected with Ransomware. The important consideration needed to be taken care of is that one should stop the backup procedures immediately if the network is infected with Ransomware to prevent the encryption of backups. [38]

To conclude, backup server should be isolated from our network and need to connect to network only during the backup procedures, it is also recommended to use Linux servers as Windows operating systems are mostly vulnerable to Ransomware attacks. [38]

5.7 Firewalls

Firewalls are the hardware or software-based devices that prevents the entering of any kind of malware onto the network. Software based firewalls, installed on critical systems, monitor the network traffic passing through the NIC of system and detect any patterns of malware and blocks it from execution. It will be highly beneficial to prevent Ransomware attacks as the Ransomware payload need to be executed to encrypt the data on infected system. [38]

Currently many organizations utilizing next generation firewalls, which come with additional features like anti-virus, anti-spam, anti-malware solutions installed .They also perform deep inspection of packets and look at the content, if any suspicious content is identified it immediately blocks and prevents from spreading across the network.

In General, firewalls act like guards between a trusted network which is usually corporate network and untrusted network which is internet. The below figure represents the firewall placement [43]

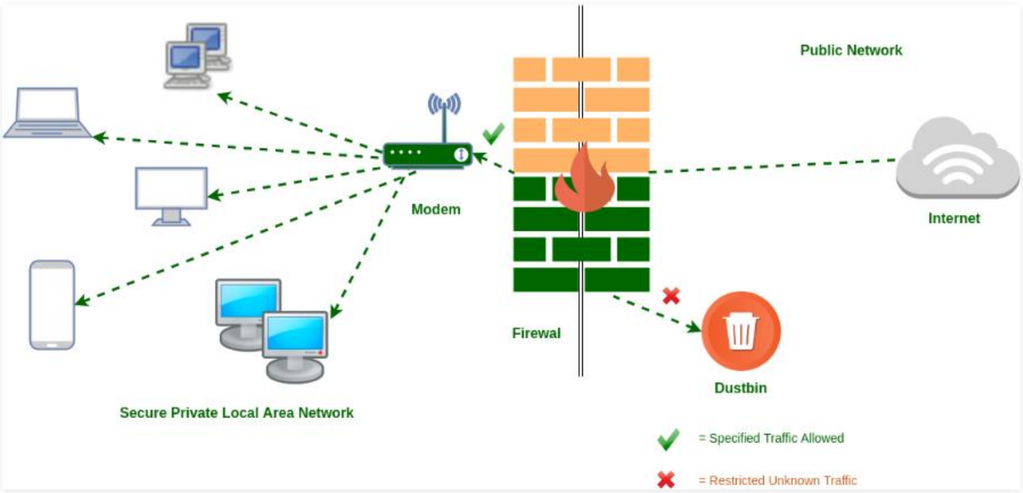

Public Network
Modem
Internet
Firewal
Dustbin
Secure Private Local Area Network
✓ = Specified Traffic Allowed
✗ = Restricted Unknown Traffic

Figure 17: Implementation of Firewall [43]

Firewalls can be helpful in two ways to prevent the malware infecting into systems by making application installing decisions based on some criteria such as preventing the installing of applications that are not in the list of approved applications [44]

There are several different types of Firewalls, such as:

a) *Packet Filtering Firewalls:*

Packet Filtering Firewalls usually works at network layer of OSI model, they inspect the headers of packet like IP header and then they take forwarding decisions based on the pre-determined rules called Access control Lists. So, they will permit the traffic that can be allowed and will block the traffic if it should be denied [43]

Packet filtering Firewalls have limited features, but these kinds of firewalls are easy and quick to deploy to mitigate the spreading of infected systems and it is also considered as the quickest solution to deploy [45]. The main disadvantage of packet filtering firewalls are they don’t inspect the content or payload of packets for patterns of malware. So, these are usually used to prevent the systems from accessing the malicious websites by predefining the list of malicious websites in the denial list [45]

b) *Application Firewalls:*

As in the name it indicates that these works at the application layer of OSI model and these firewalls are also called as Proxy firewalls. They act as middle person between the client and web server, and they process requests to web server on behalf of the client [45]. These firewalls protect the client systems from infecting from malware.

In case of watering hole attacks, in which the attackers infect the trusted websites or compromise the websites making them in such a way that installs malware when victim visit's the site. So, in these kinds of attacks application firewalls protects the clients from getting infected with several kinds of malicious software as it needs to pass through it [45]

c) *Deep Packet Inspection Firewalls:*

These firewalls are extension of stateful firewalls. In general, stateful firewalls inspect the packet headers including the sequence numbers and communication flags used for TCP. Whereas Deep Packet Inspection firewalls performs and additional check by inspecting the contents of payload of packet, by doing this it potentially identifies the attack patterns even they are hidden deep in the communication flow [46]

Does Firewalls alone can prevent malware attacks ? No, Firewalls are the part of layered security approach that provides additional protection to our network and to individual systems. Most of malware attacks are due to human vectors, so in order to prevent malware infections addition to implementing firewalls, antivirus solutions it is important to educate the users on various social engineering techniques used by human attack vectors to launch malware attacks[47]

5.8 Honeypots and Intrusion detection and prevention systems

Honeypots are also helpful in preventing the Ransomware attacks. Honeypots are the devices that are deployed by organizations to redirect the attacker from the real network. Security experts use Honeypots as a tool to study the behaviour of attacker and the patterns of Ransomware used by the attacker.

For example, organizations can install a Honeypot which will be very vulnerable and easy for attacker to exploit it. By placing the kind of information files in the Honeypot server it can draw the attacker's attention. When attacker tries to exploit it by sending malware to it. It will alert the administrator when attacker exploited it and administrator can see the patterns of Ransomware launched by attacker. The below figure shows installation of Honeypot in a network.

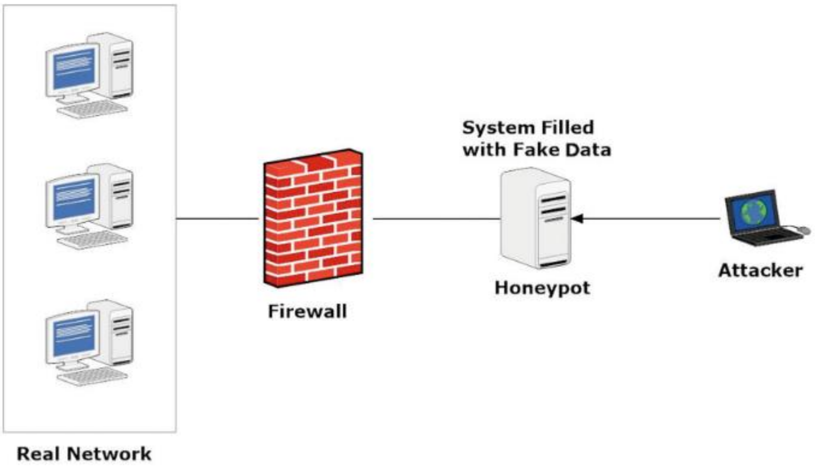


Figure 18: Honeypot Installed to redirect attacker [38]

Intrusion detection and Intrusion prevention systems alert the administrators when they identify intrusions in a host or in a network, they do this by continuously monitoring the activity of host and network traffic activity for intrusions and if they detect any suspicious activities then they alert the administrator about the intrusion. The below figure represents the functionality of Intrusion detection system [49]

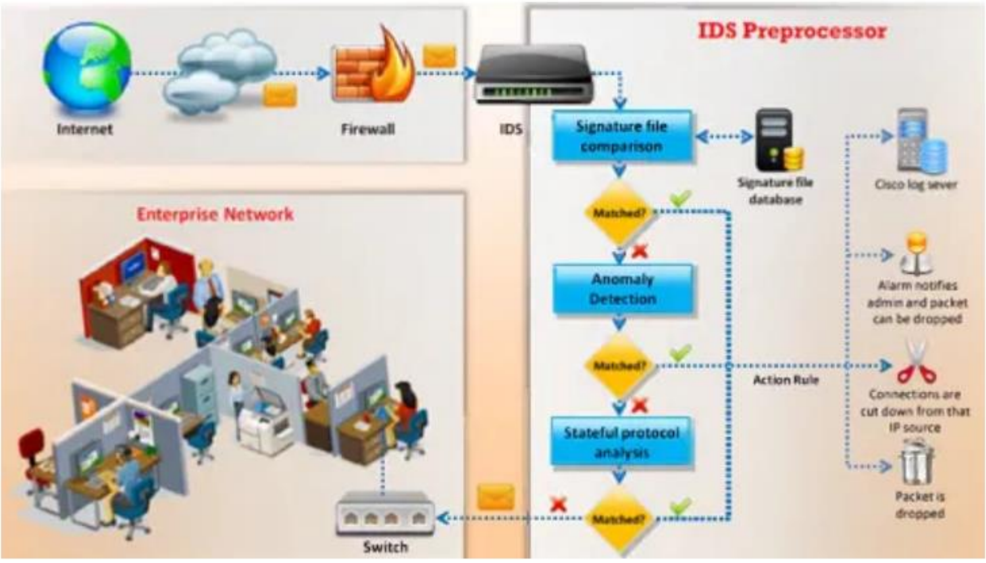


Figure 19: Functionality of Intrusion detection system [49]

Intrusion detection systems detect the intrusions by using the following methods:

a) *Signature-based detection:*

Intrusion detection systems use database of attack and malware patterns to detect the intrusions in signature-based detection method. They continuously monitor the activity on host or network and compare with database of known patterns, if match is found then intrusion detection systems alert the administrator on the intrusion detected. The main idea is to compare the current activities with the existing signature patterns to detect the attacks [50]

The main disadvantage of signature-based detection is this technique cannot detect the new attack patterns; in other words, it cannot detect the intrusions that are not in the database. This problem is addressed by using anomaly-based detection techniques.

b) *Anomaly-based detection:*

This method starts by identifying the baseline behaviour of system or network by using statistical-based methods, machine learning etc. After defining the baseline, intrusions detection systems continuously monitor the traffic and compares it with the baseline behaviour, and it identifies any deviation from its baseline then they alert the administrator on intrusions [50]

5.9 Security Policy

Organization should ensure that they have security policies in place in order to prevent many malware attacks and other kind of attacks. We also need to ensure that we are reviewing the policies in place and making sure that personnel in organization comply with the policies implemented, and they are getting updated regularly in order to mitigate the recent attacks. They include plans, procedures and guidelines on implementing them [53]

The below figure represents the organizational security control relationships recommended by National Institute of Standards and Technology [NIST 800-53]

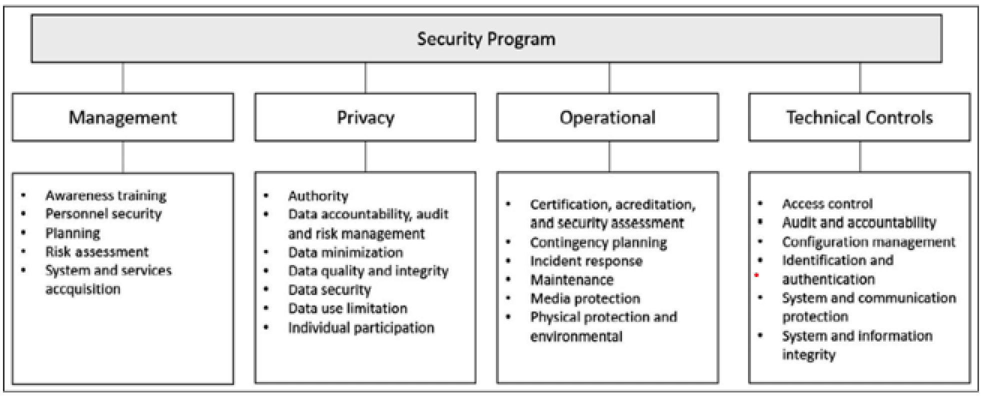

Security Program
Management
Privacy
Operational
Technical Controls
• Awareness training
• Personnel security
• Planning
• Risk assessment
• System and services accquisition
• Authority
• Data accountability, audit and risk management
• Data minimization
• Data quality and integrity
• Data security
• Data use limitation
• Individual participation
• Certification, acreditation, and security assessment
• Contingency planning
• Incident response
• Maintenance
• Media protection
• Physical protection and environmental
• Access control
• Audit and accountability
• Configuration management
• Identification and authentication
• System and communication protection
• System and information integrity

Figure 20: Organizational security controls [53]

Some of the policies that need to be implemented by organizations to protect from cyber-attacks are: [53]

a) *Awareness Training:*

From the above figure, we can see that it is the part of Management control, and it is very important factor in preventing any kind of malware attacks because an uneducated user can cause potential damage to organization by clicking on phishing emails and giving way for the attackers to enter into the organizations network.

b) *Application Whitelisting:*

Organization policy should also include that only licensed and authorised software allowed to run on user machines, restricting the use of unauthorized software. When designing policies organizations define the list of authorized applications that can be allowed to run in the user systems.

c) *Hardening:*

Organizations should include the policies to harden the systems and applications in order to mitigate the attack surface for attackers. It is recommended to create security baseline configurations for deploying systems to ensure that they start in secure state.

d) *Auditing and Monitoring:*

It is also important for organizations to conduct internal audits and external audits from third parties to ensure that the policies are implemented and followed by the personnel in the organization. For example, conducting annual assessments to the personnel on the social engineering practices prevents the attackers launching the phishing attacks against the personnel and at the same time monitoring the critical systems for vulnerabilities also plays a crucial role in preventing the many malicious attacks

5.10 Implement Incident Response plan

Organizations must have a proper incident management process in order to defeat the Ransomware once it gets into systems. The below figure defines the stages in Incident response plan:

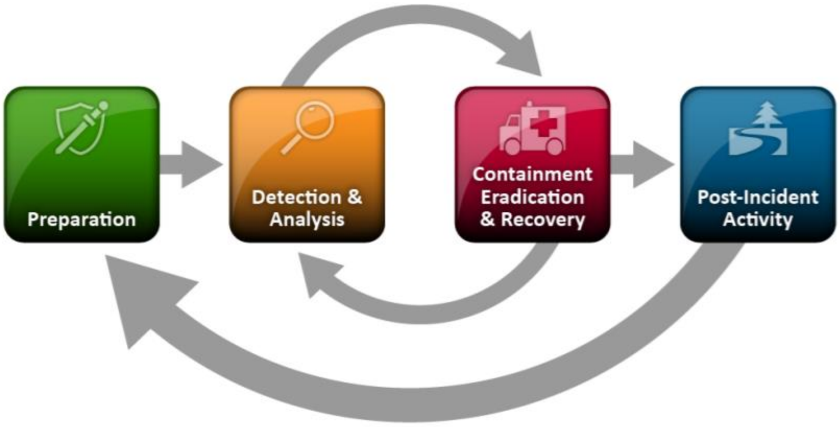


Figure 21: Incident Response Plan [48]

There are multiple that every organization need to follow in order to prevent the malware infections. They are:

a) *Preparation:*

The first phase of an Incident response plan is preparation, where every organization needs preparation in order to deal with the malware infections. Some of the recommended measures in preparation phase are, Incident response team should be aware of organizations security posture, policies and implementations to identify and analyse the threats [48]

Organization should train its personnel on following the policies in place, and technical upgrade skills training should be provided to the administrators to make sure that they are ready to handle the latest malware infections. Communication also plays a crucial role in effective Incident response plan, so organizations need to make sure they have a dedicated small team for communicating and coordinating the malware incident process [48]

b) *Detection and Analysis:*

The second phase of Incident Response plan is detection of malware and analysing it to prevent its spreading or distribution across the network. It is mandatory to validate all the security events alerted and need to ensure that if it is a valid event or not because in some cases even antivirus solutions will generate false positives. Based on the impact of malware we need to prioritize the incidents [48]

When infected it is important to understand some of factors like type of malware, services, ports that are attacked, Vulnerabilities exploited by attackers, how malware infected host, how to remove it [48] . Overall, it is important to identify the hosts that are infected with malware , once we identify that we can proceed with the next phases such as containment, eradication and recovery phases. We can identify the infected systems by using antivirus solutions, IDS, IPS, Firewalls, Packet sniffers etc. [48]

c) *Containment:*

When identified system infected with Ransomware, then you need to containment it immediately to prevent the spreading of malware to other systems. It can be done in many ways like by pulling the power cable, shutting down the system, etc [42]. In some cases of malware infections, it is also important to protect the disconnected system OS files, critical system files, data on hard disk because several malware infections start damaging these things on infected system.

Organizations need to decide on disconnecting the infected system from network or not, it depends on the system capability if it is a critical system that generates a revenue to the organization then organizations should have different strategies on handling these systems [48] . Containment can be done through several ways such as user participation, which means providing training to users on identifying the infections, reaching out to helpdesk, disconnecting infected system from network [48]

Organizations can also implement automatic containment by using network scans, disabling the services that are not in use, blacklisting of executable files, signature-based detections – where if patterns of malware are detected then IDS/ IPS stops them spreading into network.

d) *Eradication:*

After isolating the infected system from the network, now we need to eradicate the Ransomware from the infected system which can be done by cleaning out the all the Ransomware infected files and deleting all the hidden files by booting system in safe environment which is can be seen later in the "Analysis of testing Ransomware-Implementation" section to follow [42]

Eradication does not only mean the removal of malware, it includes the rebuilding of compromised systems which includes the reinstallation of system OS, applications and restoration of data from backups. In some cases, it is recommended to rebuild the compromised system from starch rather than spending time on analysing the malware infected and removing all traces of it from the compromised system [48]

e) *Recovery:*

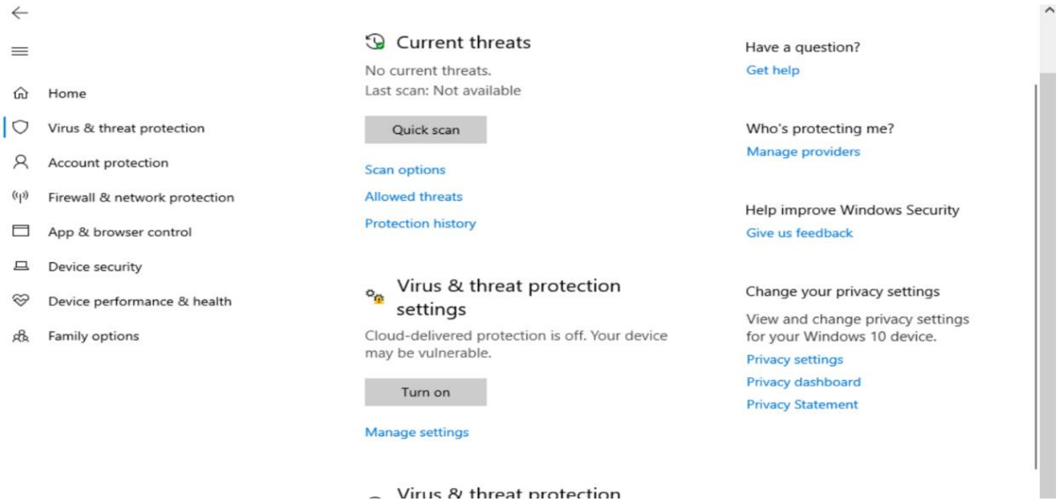
Once the isolation and eradication of Ransomware from infected system is done, we need to recover the system from Ransomware which means we need to make sure that the system is performing the normal operations. Recovering the encrypted data from backups [42]

All the above-mentioned prevention techniques are essential to consider in order to prevent the Ransomware attacks. In this project, I am diving through some of the prevention techniques such as taking backups of data, isolating the infected VM, sanitizing the infected files, and finally recovering the data from backups.

6. IMPLEMENTATION

6.1 Infecting a system with Ransomware

Step 1: In order to install WannaCry Ransomware sample test file, I have installed windows 10 VM on VirtualBox with completely isolated environment. Before downloading the WannaCry file we need to disable Windows Firewall Defender, Ransomware protection, virus and threat protection settings to allow the file to be downloaded.



Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options

Current threats
No current threats.
Last scan: Not available
Quick scan
Scan options
Allowed threats
Protection history

Virus & threat protection settings
Cloud-delivered protection is off. Your device may be vulnerable.
Turn on
Manage settings

Virus & threat protection

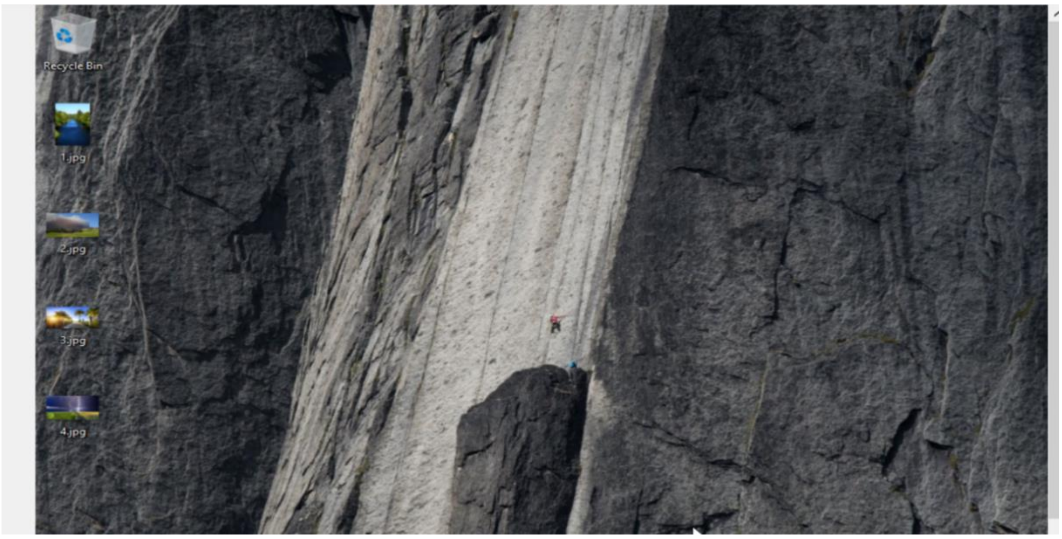
Have a question?
Get help

Who's protecting me?
Manage providers

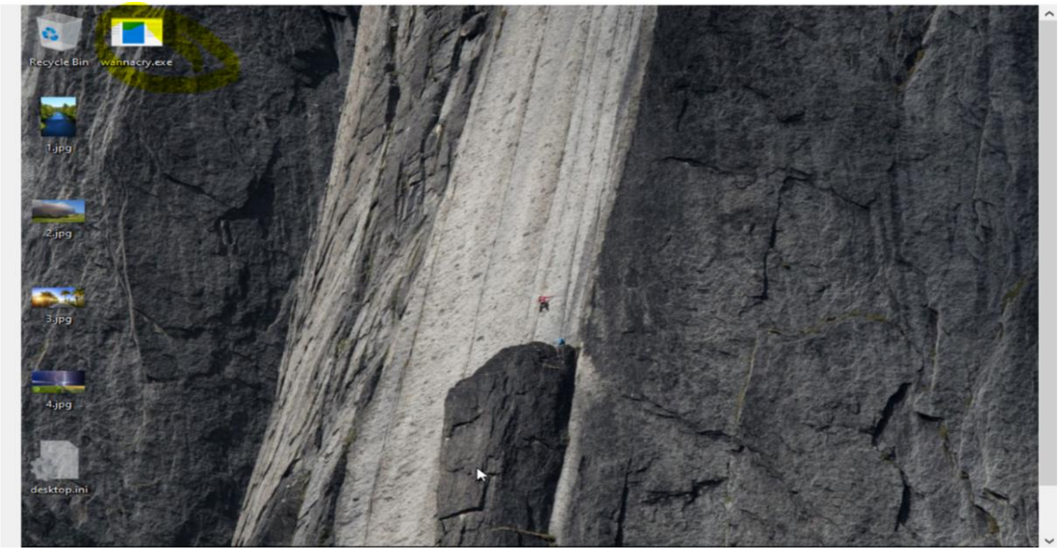
Help improve Windows Security
Give us feedback

Change your privacy settings
View and change privacy settings for your Windows 10 device.
Privacy settings
Privacy dashboard
Privacy Statement

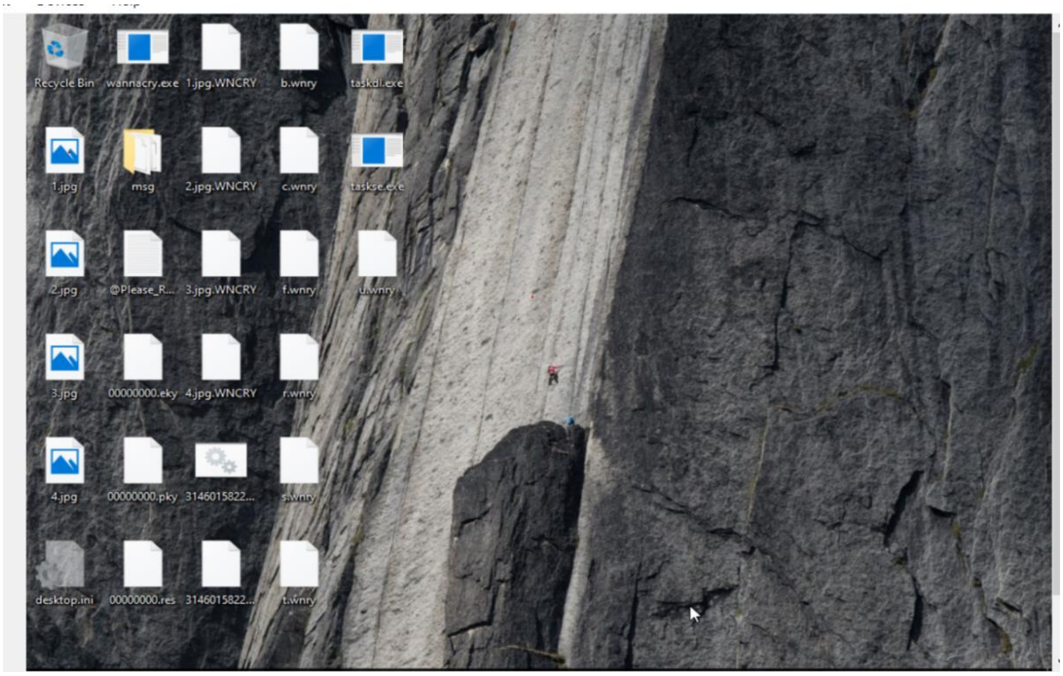
Step 2: I have downloaded some images as my personal files which are going to be encrypted once WannaCry is downloaded and run. To ensure the redundancy of data I have taken backup of data in external hard disk which will help us to recover the data without paying any ransom to the attacker



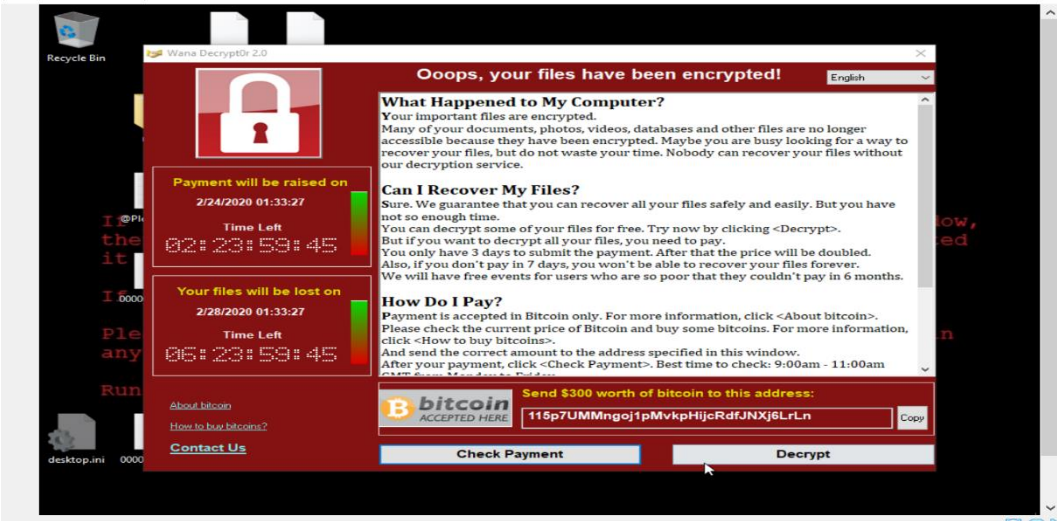
Step 3: I have downloaded WannaCry sample file to study the behaviour of Ransomware when it is infected to system



Step 4: I have executed the WannaCry file and it starts creating multiple files with. wncry extension as shown below.



Step 5: It displays a message that your files have been encrypted and provides an option for payment and displays the time given to victim by attacker to pay ransom in order to prevent the deletion of data.



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

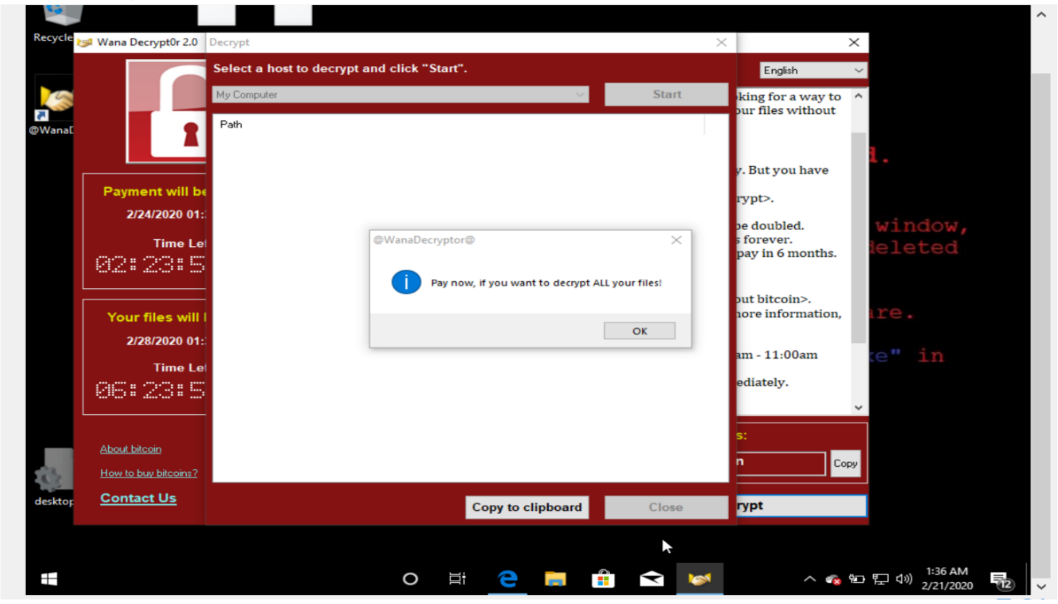
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
2/24/2020 01:33:27
Time Left
02:23:59:45

Your files will be lost on
2/28/2020 01:33:27
Time Left
06:23:59:45

Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

Step 6: If you click on decrypt option, it will display the message that we need to pay ransom if we want our files to be decrypted as shown.



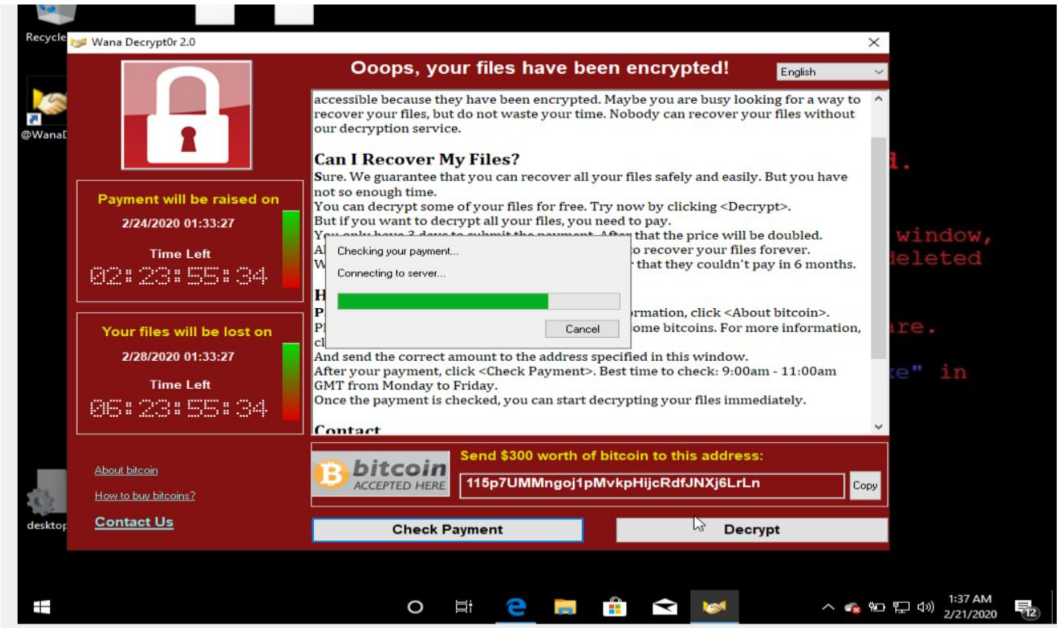
Wana Decrypt0r 2.0 — Decrypt

Select a host to decrypt and click "Start".

@WanaDecryptor@

Pay now, if you want to decrypt ALL your files!

Step 7: If we decided to do payment and then if we click on check payment option, it will redirect us to payment server.



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
Y that the price will be doubled.
Al o recover your files forever.
W that they couldn't pay in 6 months.

H
P rmation, click <About bitcoin>.
Pl ome bitcoins. For more information,
cl
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.
Once the payment is checked, you can start decrypting your files immediately.

Contact

Checking your payment...

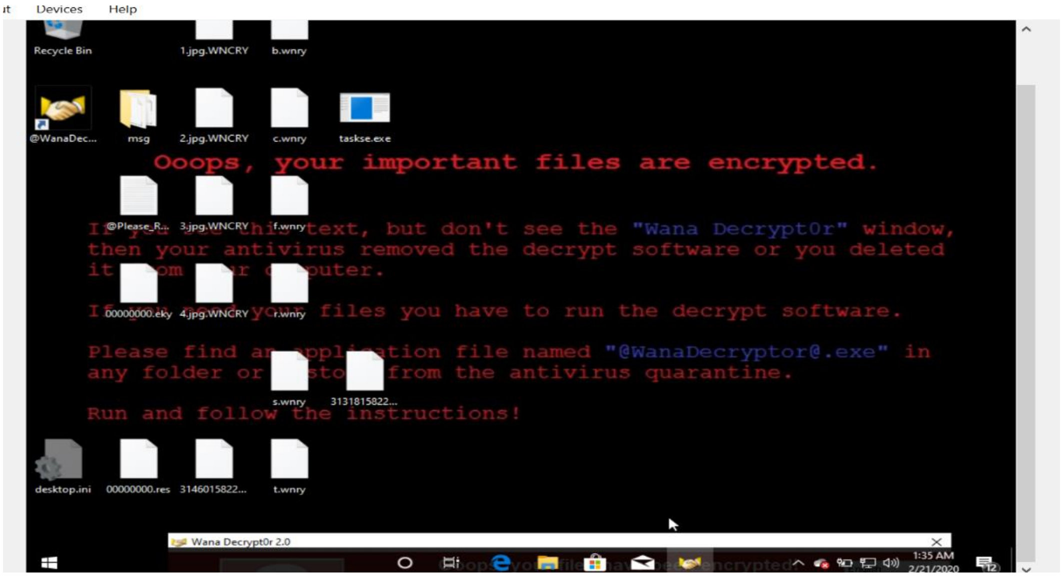
Connecting to server...

Payment will be raised on
2/24/2020 01:33:27
Time Left
02:23:55:34

Your files will be lost on
2/28/2020 01:33:27
Time Left
06:23:55:34

Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

Step 8: It also changes our desktop personalized image and displays an image that all of our files have been encrypted.



Ooops, your important files are encrypted.

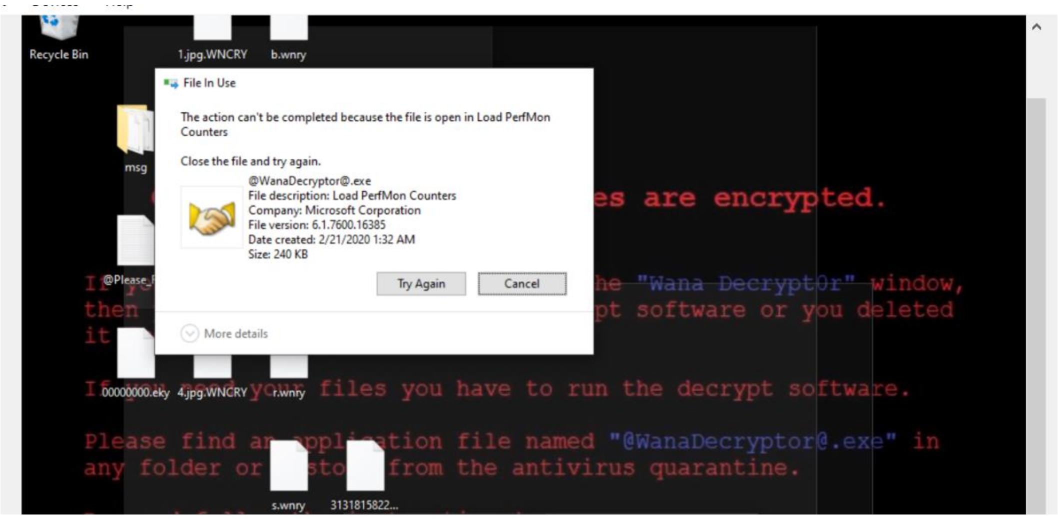
If you see this text, but don't see the "Wana Decrypt0r" window, then your antivirus removed the decrypt software or you deleted it om ur puter.

If you need your files you have to run the decrypt software.

Please find an application file named "@WanaDecryptor@.exe" in any folder or sto from the antivirus quarantine.

Run and follow the instructions!

Step 9: Even if we try to delete any of the files it will not allow us to delete any of the files.



File In Use

The action can't be completed because the file is open in Load PerfMon Counters

Close the file and try again.

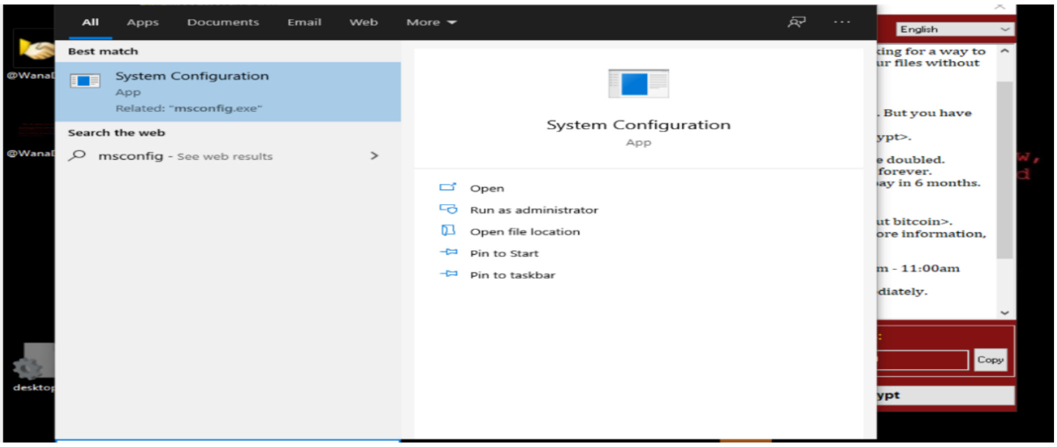
@WanaDecryptor@.exe
File description: Load PerfMon Counters
Company: Microsoft Corporation
File version: 6.1.7600.16385
Date created: 2/21/2020 1:32 AM
Size: 240 KB

Try Again
Cancel
More details
Recycle Bin
1.jpg.WNCRY
b.wnry
msg
@Please_
00000000.eky
4.jpg.WNCRY
r.wnry
s.wnry
3131815822...
es are encrypted.
he "Wana Decrypt0r" window,
pt software or you deleted
files you have to run the decrypt software.
Please find an application file named "@WanaDecryptor@.exe" in
any folder or restore from the antivirus quarantine.

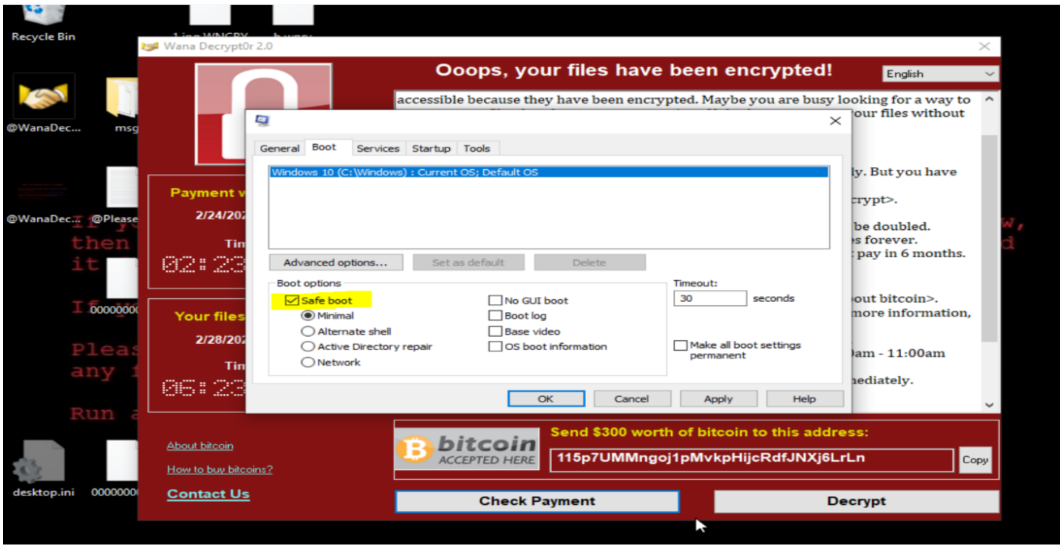
7. RECOVERY PROCESS

If we have our data backups, then we can recover our system safely from all WannaCry files and, we can recover our data from backups without paying any ransom to the attacker. The following are the steps included in the recovery process.

Step 1: First, we need to do safe boot of our system to go to safe mode environment which can be done by accessing the system configuration.



Step 2: Once you open the system configurations navigate to boot menu and select the safe boot option as shown below.



Windows 10 (C:\Windows) : Current OS; Default OS

Boot options

☑ Safe boot

● Minimal

○ Alternate shell

○ Active Directory repair

○ Network

□ No GUI boot

□ Boot log

□ Base video

□ OS boot information

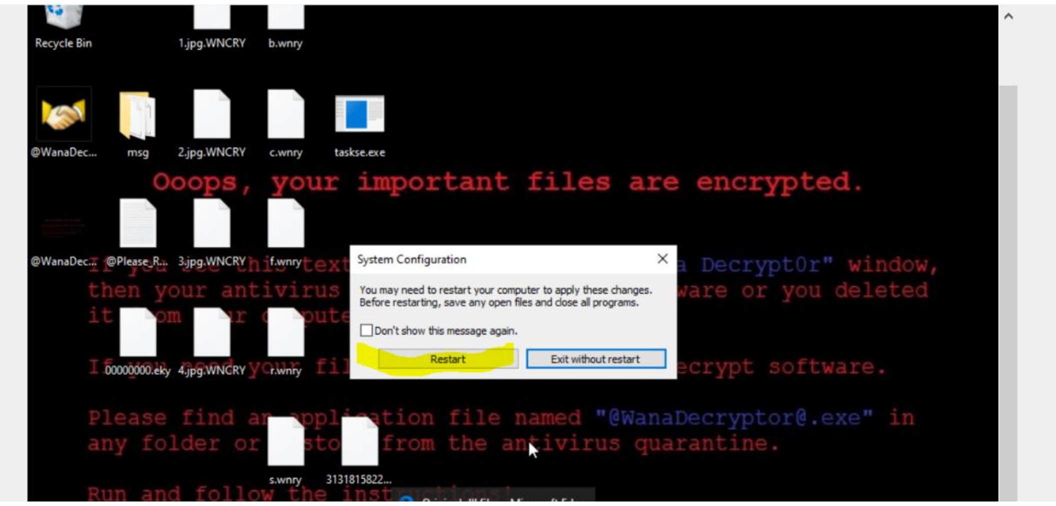
Timeout: 30 seconds

□ Make all boot settings permanent

Send $300 worth of bitcoin to this address:

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

Step 3: Once we do safe boot it prompts a message that system need to be restarted as shown below.



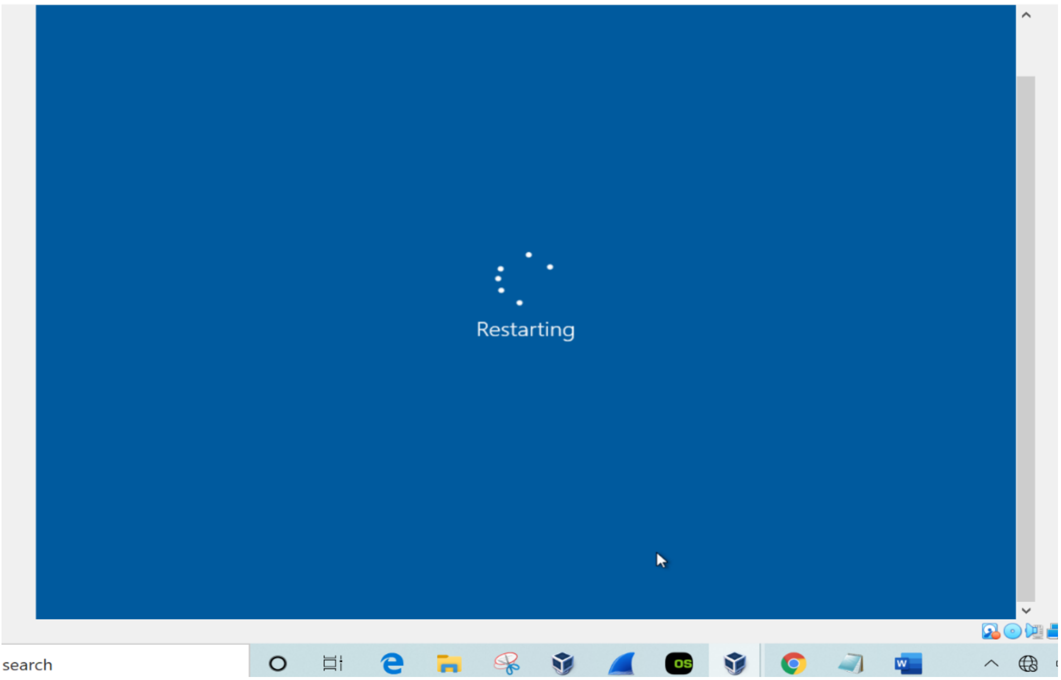
Ooops, your important files are encrypted.

System Configuration

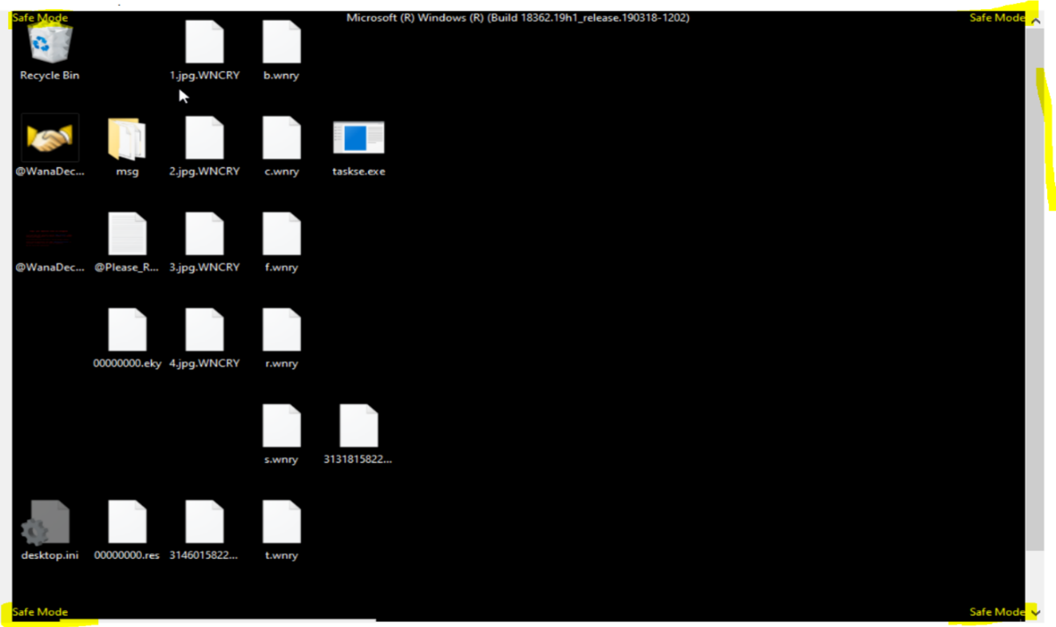
You may need to restart your computer to apply these changes. Before restarting, save any open files and close all programs.

□ Don't show this message again.

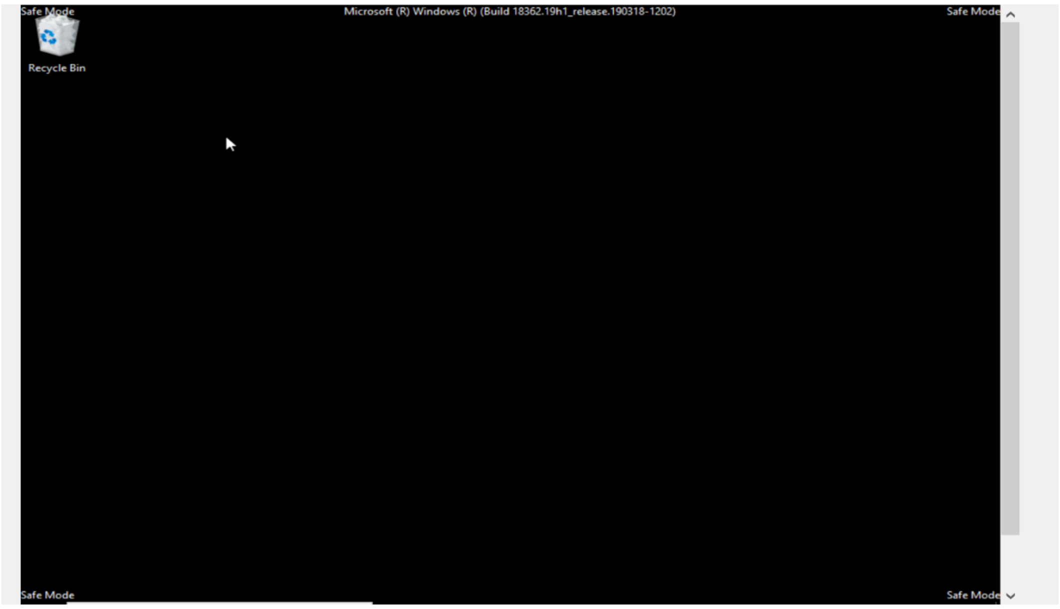
Step 4: Restarting in safe mode.



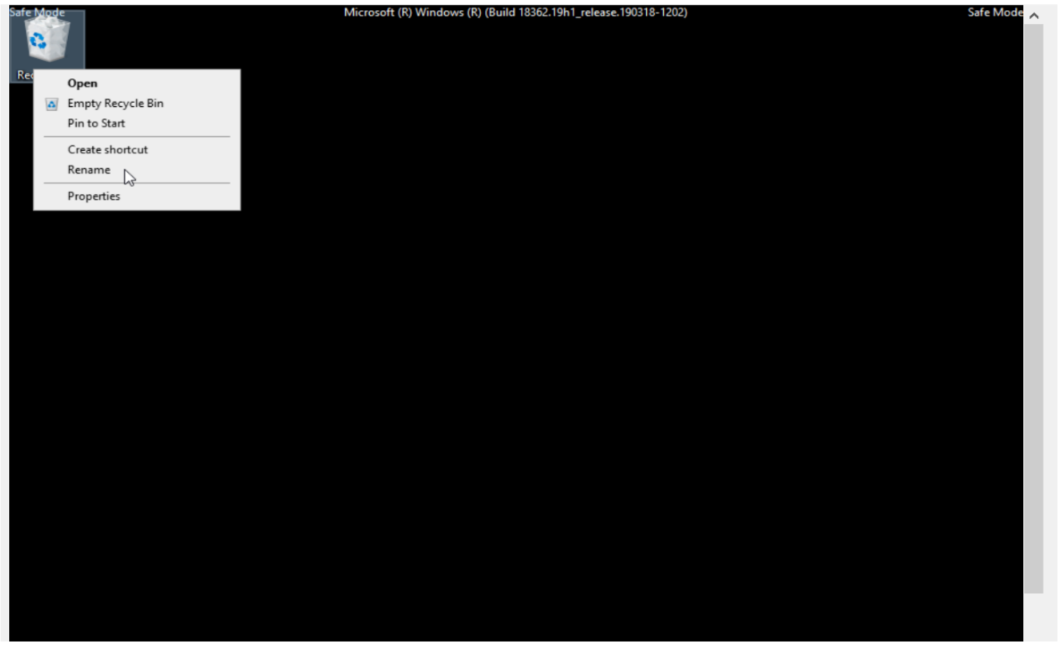
Step 5: We can ensure that we are in safe mode by seeing the safe mode option on four corners on our screen which enables us to operate system in controlled environment.



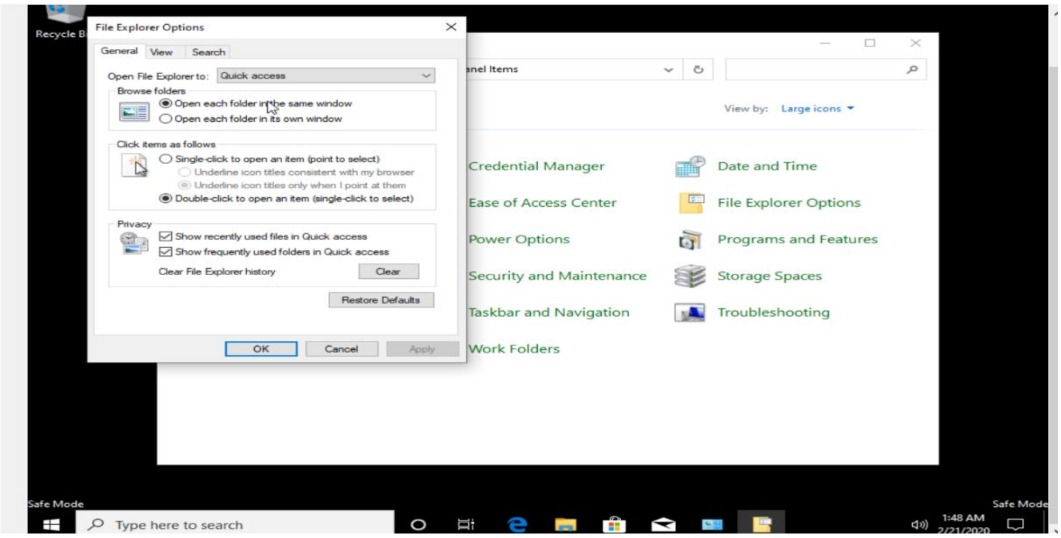
Step 6: As we are in controlled environment it allows us to delete all the files which we are unable to delete when we are in normal windows mode. I have deleted all the files including my personals which are infected with WannaCry.


Safe Mode
Microsoft (R) Windows (R) (Build 18362.19h1_release.190318-1202)
Safe Mode
Recycle Bin
Safe Mode
Safe Mode

Step 7: We need to make sure that we are clearing recycle bin as well.



Step 8: As we have deleted all the files that we see on the desktop that doesn't mean that we have deleted all the WannaCry files. So, we need to navigate to file explorer options as shown below in order to see the hidden files and folders.



Open File Explorer to: Quick access

Browse folders

● Open each folder in the same window
○ Open each folder in its own window

Click items as follows

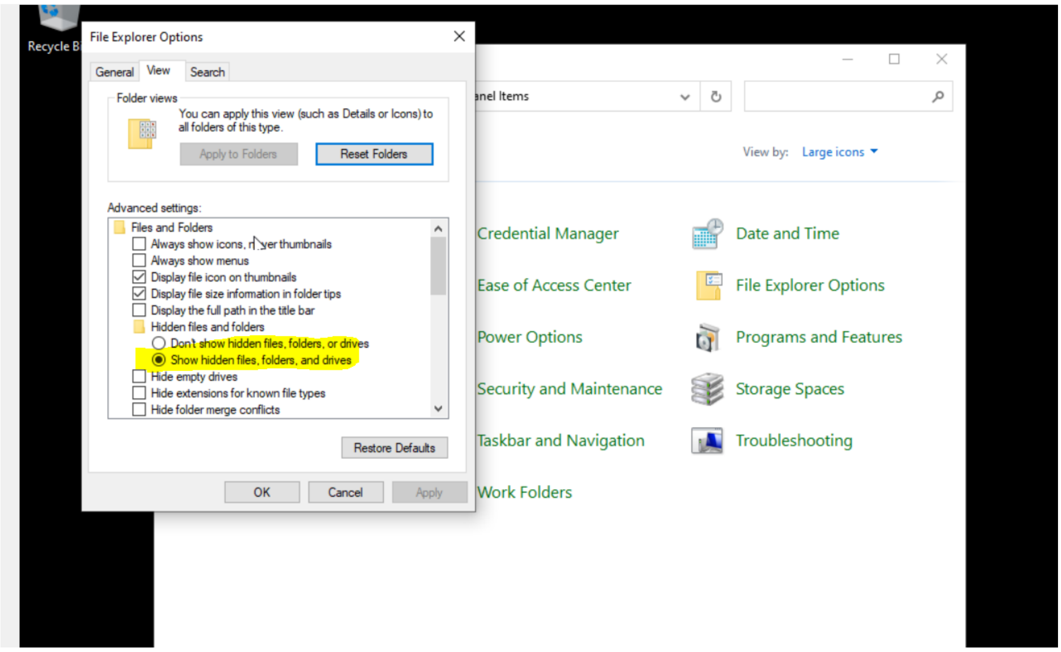
○ Single-click to open an item (point to select)
○ Underline icon titles consistent with my browser
● Underline icon titles only when I point at them
● Double-click to open an item (single-click to select)

Privacy

☑ Show recently used files in Quick access
☑ Show frequently used folders in Quick access

Clear File Explorer history

Step 9: Check box the option of show hidden files, folders or drivers.



File Explorer Options

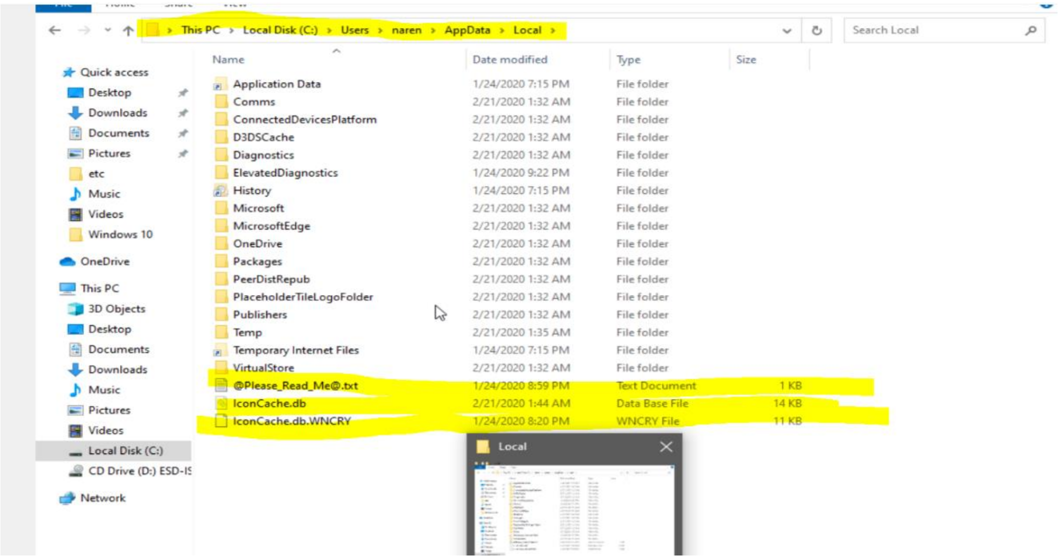
Folder views

You can apply this view (such as Details or Icons) to all folders of this type.

Advanced settings:

Files and Folders
□ Always show icons, never thumbnails
□ Always show menus
☑ Display file icon on thumbnails
☑ Display file size information in folder tips
□ Display the full path in the title bar
Hidden files and folders
○ Don't show hidden files, folders, or drives
● Show hidden files, folders, and drives
□ Hide empty drives
□ Hide extensions for known file types
□ Hide folder merge conflicts

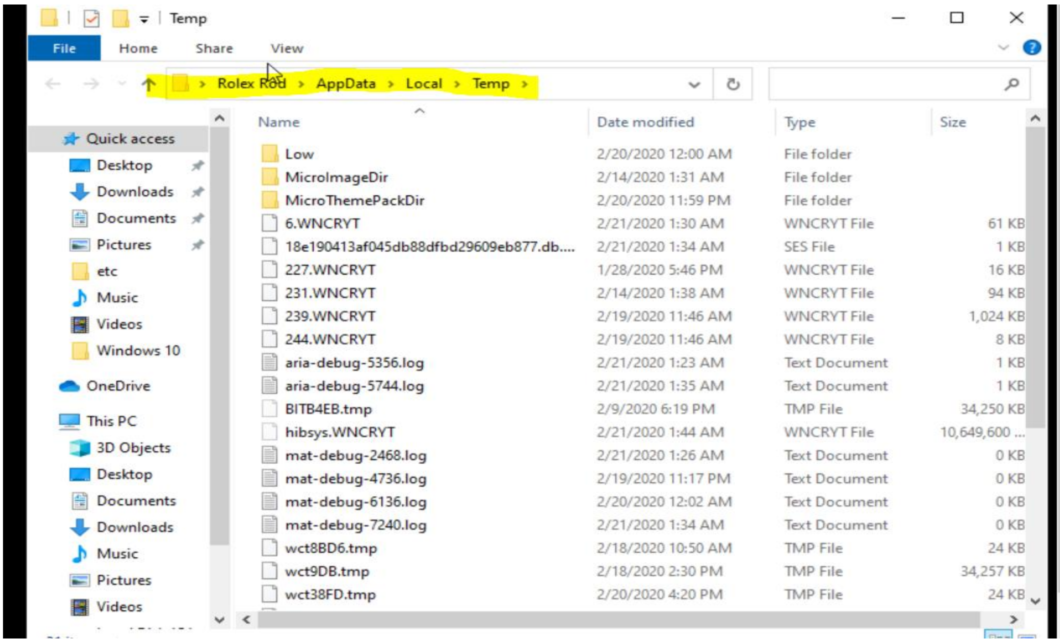
Step 10: Navigate to the path specified in the below fig. Appdata > local and delete all the suspicious files as we see the files in the below image are WannaCry files.



This PC > Local Disk (C:) > Users > naren > AppData > Local >

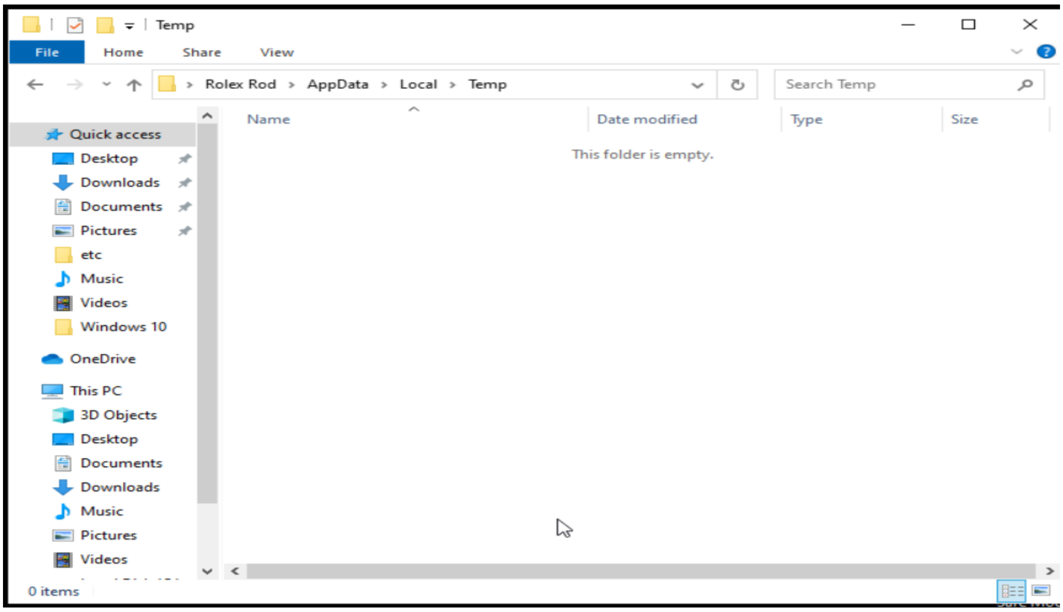
Name	Date modified	Type	Size
Application Data	1/24/2020 7:15 PM	File folder	
Comms	2/21/2020 1:32 AM	File folder	
ConnectedDevicesPlatform	2/21/2020 1:32 AM	File folder	
D3DSCache	2/21/2020 1:32 AM	File folder	
Diagnostics	2/21/2020 1:32 AM	File folder	
ElevatedDiagnostics	1/24/2020 9:22 PM	File folder	
History	1/24/2020 7:15 PM	File folder	
Microsoft	2/21/2020 1:32 AM	File folder	
MicrosoftEdge	2/21/2020 1:32 AM	File folder	
OneDrive	2/21/2020 1:32 AM	File folder	
Packages	2/21/2020 1:32 AM	File folder	
PeerDistRepub	2/21/2020 1:32 AM	File folder	
PlaceholderTileLogoFolder	2/21/2020 1:32 AM	File folder	
Publishers	2/21/2020 1:32 AM	File folder	
Temp	2/21/2020 1:35 AM	File folder	
Temporary Internet Files	1/24/2020 7:15 PM	File folder	
VirtualStore	2/21/2020 1:32 AM	File folder	
@Please_Read_Me@.txt	1/24/2020 8:59 PM	Text Document	1 KB
IconCache.db	2/21/2020 1:44 AM	Data Base File	14 KB
IconCache.db.WNCRY	1/24/2020 8:20 PM	WNCRY File	11 KB

Step 11: In the next step, delete all the temp files and we can see from the below image that we have many files with WannaCry extensions.



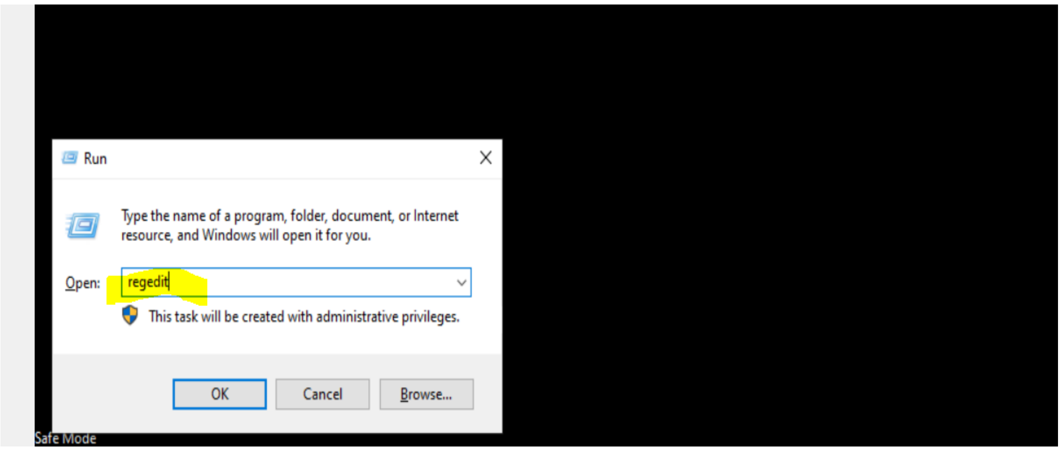
Name	Date modified	Type	Size
Low	2/20/2020 12:00 AM	File folder	
MicroImageDir	2/14/2020 1:31 AM	File folder	
MicroThemePackDir	2/20/2020 11:59 PM	File folder	
6.WNCRYT	2/21/2020 1:30 AM	WNCRYT File	61 KB
18e190413af045db88dfbd29609eb877.db....	2/21/2020 1:34 AM	SES File	1 KB
227.WNCRYT	1/28/2020 5:46 PM	WNCRYT File	16 KB
231.WNCRYT	2/14/2020 1:38 AM	WNCRYT File	94 KB
239.WNCRYT	2/19/2020 11:46 AM	WNCRYT File	1,024 KB
244.WNCRYT	2/19/2020 11:46 AM	WNCRYT File	8 KB
aria-debug-5356.log	2/21/2020 1:23 AM	Text Document	1 KB
aria-debug-5744.log	2/21/2020 1:35 AM	Text Document	1 KB
BITB4EB.tmp	2/9/2020 6:19 PM	TMP File	34,250 KB
hibsys.WNCRYT	2/21/2020 1:44 AM	WNCRYT File	10,649,600 ...
mat-debug-2468.log	2/21/2020 1:26 AM	Text Document	0 KB
mat-debug-4736.log	2/19/2020 11:17 PM	Text Document	0 KB
mat-debug-6136.log	2/20/2020 12:02 AM	Text Document	0 KB
mat-debug-7240.log	2/21/2020 1:34 AM	Text Document	0 KB
wct8BD6.tmp	2/18/2020 10:50 AM	TMP File	24 KB
wct9DB.tmp	2/18/2020 2:30 PM	TMP File	34,257 KB
wct38FD.tmp	2/20/2020 4:20 PM	TMP File	24 KB

Step 12: Deleted all the temp files.



This folder is empty.

Step 13: For the next step, open registry editor from run terminal by entering regedit.

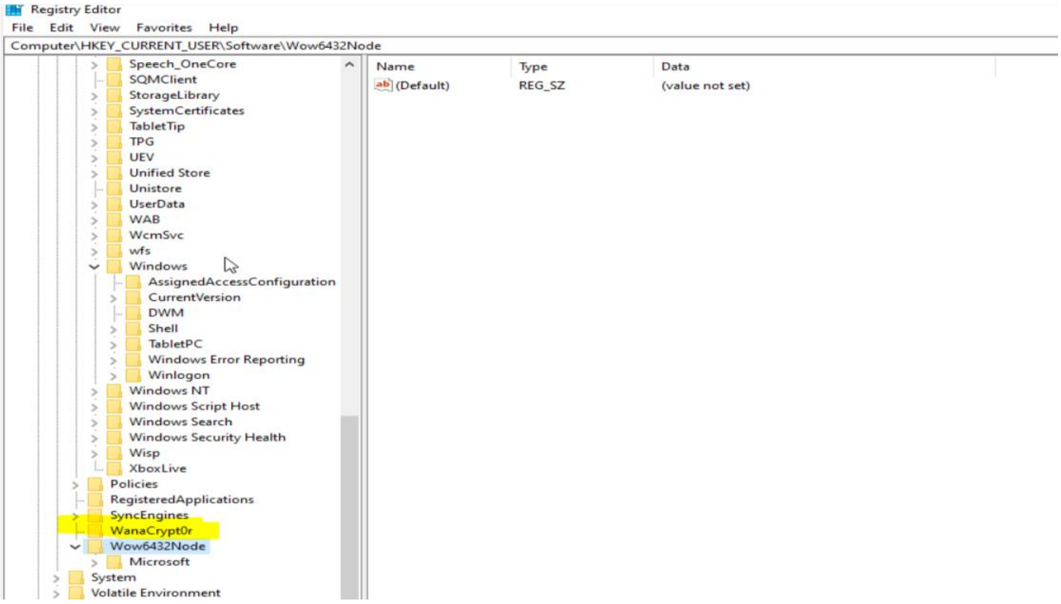


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: regedit

This task will be created with administrative privileges.

Step 14: I have seen WannaCryptor registers in registry editor and have deleted the files.

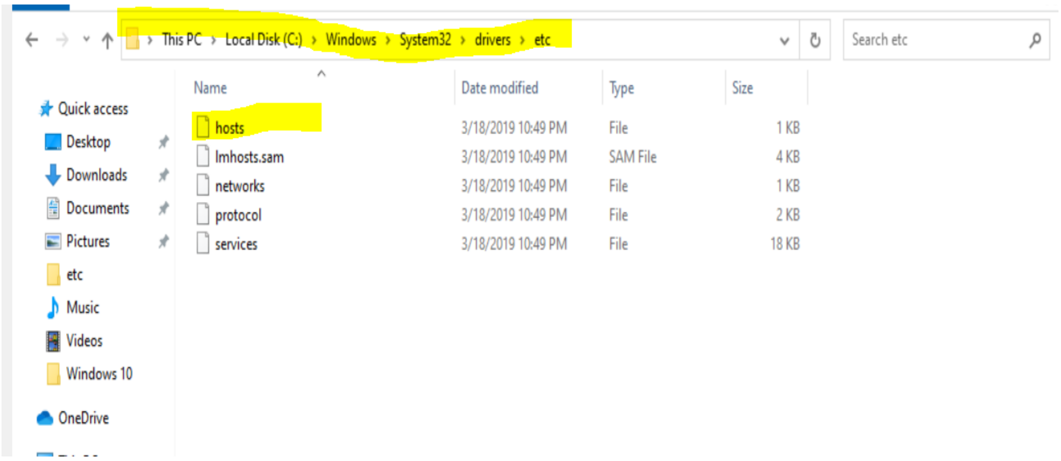


Computer\HKEY_CURRENT_USER\Software\Wow6432Node

```
Speech_OneCore
SQMClient
StorageLibrary
SystemCertificates
TabletTip
TPG
UEV
Unified Store
Unistore
UserData
WAB
WcmSvc
wfs
Windows
  AssignedAccessConfiguration
  CurrentVersion
  DWM
  Shell
  TabletPC
  Windows Error Reporting
  Winlogon
Windows NT
Windows Script Host
Windows Search
Windows Security Health
Wisp
XboxLive
Policies
RegisteredApplications
SyncEngines
WanaCrypt0r
Wow6432Node
  Microsoft
System
Volatile Environment
```

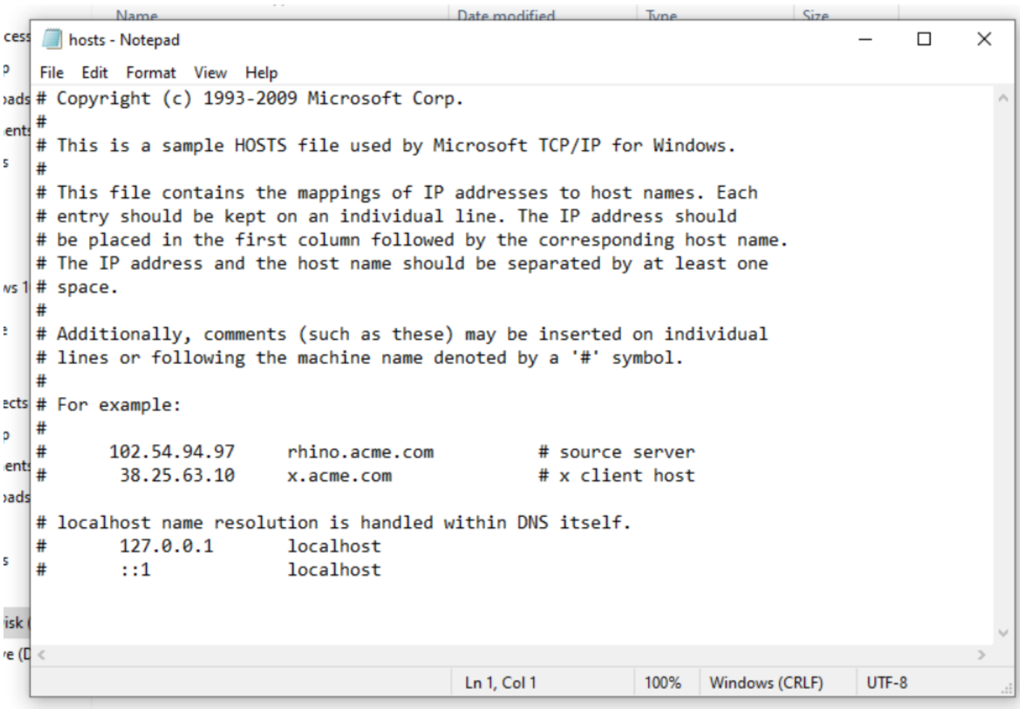
Name	Type	Data
(Default)	REG_SZ	(value not set)

Step 15: We also need to check the host files if it is encrypted by WannaCry. We can find the host files by navigating to the below showed path



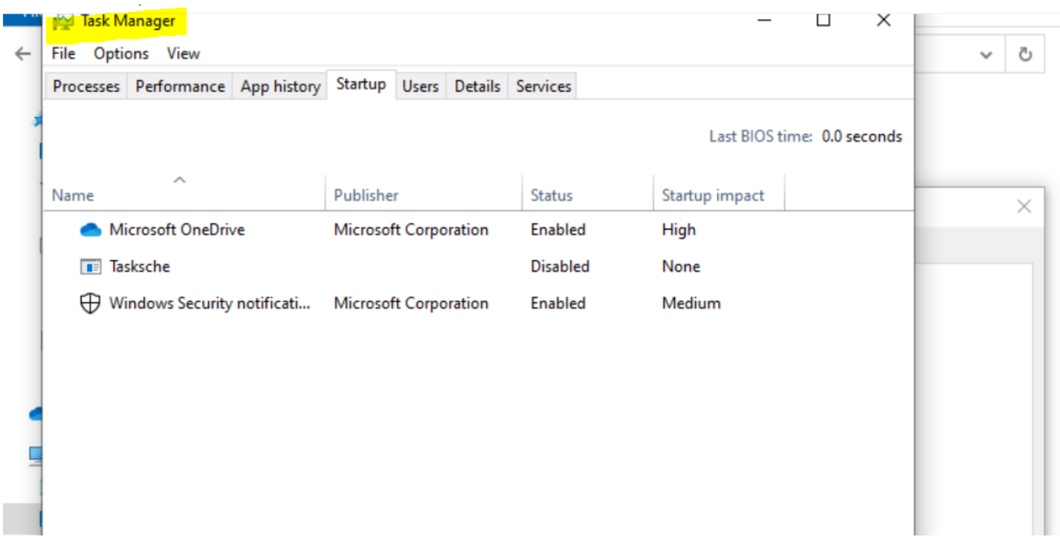
Name	Date modified	Type	Size
hosts	3/18/2019 10:49 PM	File	1 KB
lmhosts.sam	3/18/2019 10:49 PM	SAM File	4 KB
networks	3/18/2019 10:49 PM	File	1 KB
protocol	3/18/2019 10:49 PM	File	2 KB
services	3/18/2019 10:49 PM	File	18 KB

Step 16: After opening the host file, if you find any suspicious/ additional content added to it delete that part. It should be as shown below.



```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#	127.0.0.1       localhost
#	::1             localhost
```

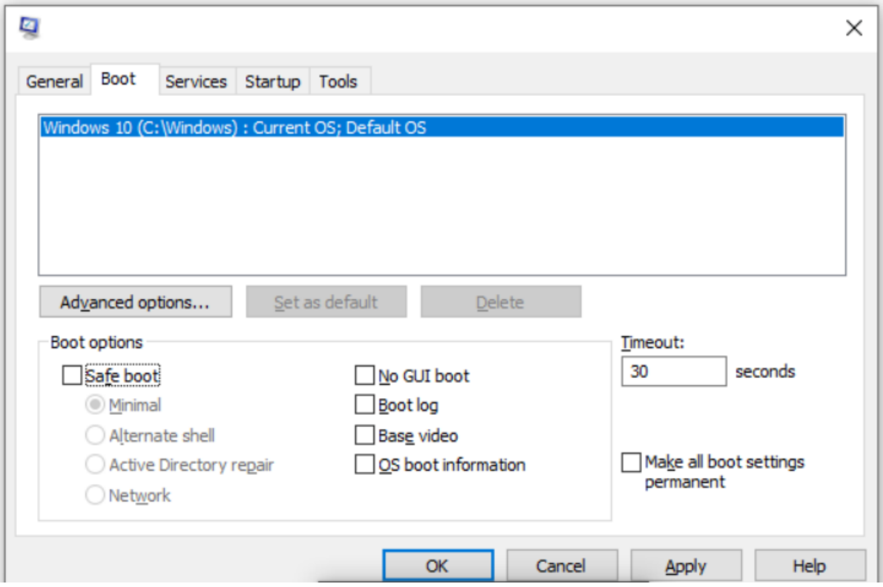
Step 17: Also check the task manager to view all the tasks running in system and delete the suspicious tasks so that we can prevent them by spreading more.



Last BIOS time: 0.0 seconds

Name	Publisher	Status	Startup impact
Microsoft OneDrive	Microsoft Corporation	Enabled	High
Tasksche		Disabled	None
Windows Security notificati...	Microsoft Corporation	Enabled	Medium

Step 18: After doing all the above-mentioned steps, next we need to proceed to normal boot of infected system.



Windows 10 (C:\Windows) : Current OS; Default OS

Boot options

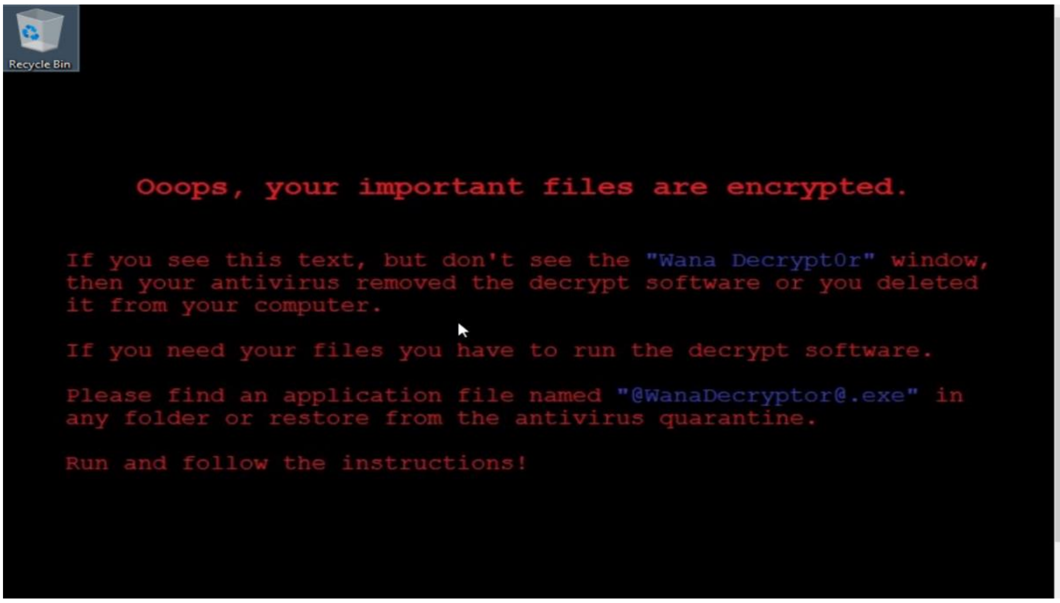
□ Safe boot
○ Minimal
○ Alternate shell
○ Active Directory repair
○ Network

□ No GUI boot
□ Boot log
□ Base video
□ OS boot information

Timeout: 30 seconds

□ Make all boot settings permanent

Step 19: From the below image, we can see that we are in our windows mode and we need to personalize the desktop image.



Ooops, your important files are encrypted.

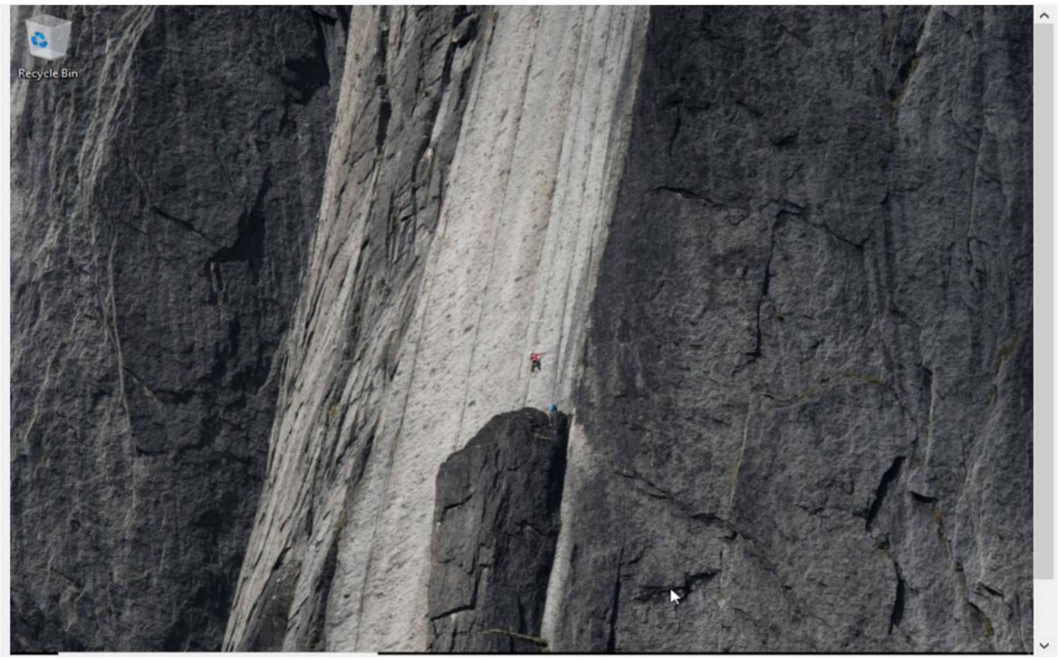
If you see this text, but don't see the "Wana Decrypt0r" window, then your antivirus removed the decrypt software or you deleted it from your computer.

If you need your files you have to run the decrypt software.

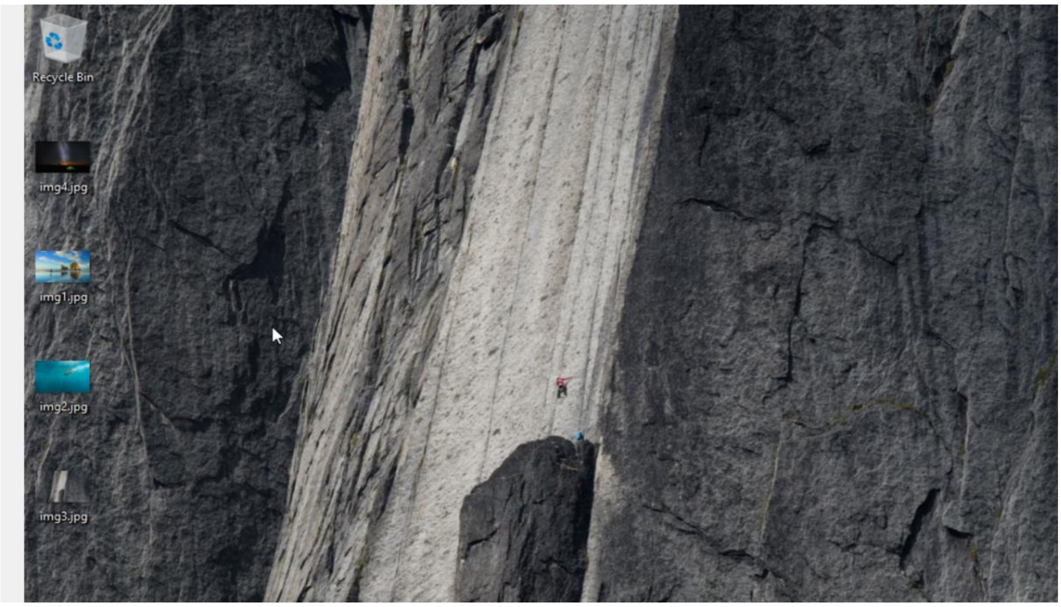
Please find an application file named "@WanaDecryptor@.exe" in any folder or restore from the antivirus quarantine.

Run and follow the instructions!

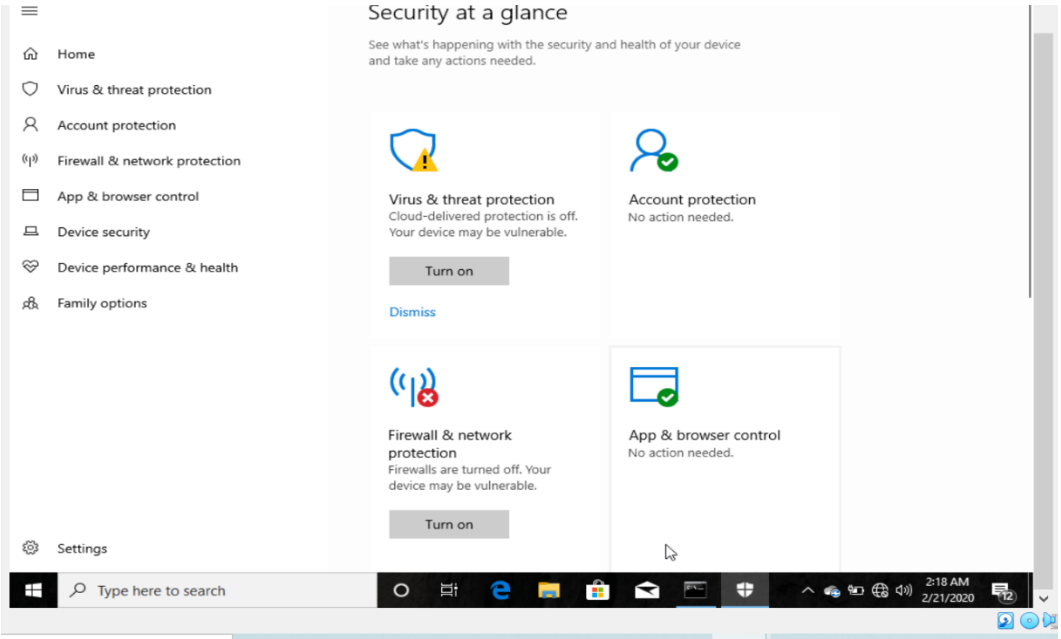
Step 20: After changing the desktop screen and we could see that there are no WannaCry files.



Step 21: Finally, after removing WannaCry Ransomware from the infected system we can restore our data from backups.



Step 22: It is always recommended to turn on the windows firewall defender and virus and threat protection on to prevent the multiple patterns of virus.



Security at a glance

See what's happening with the security and health of your device and take any actions needed.

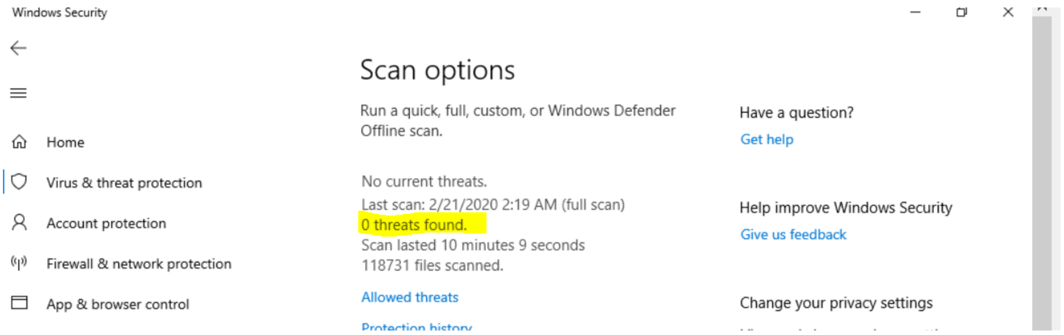
Virus & threat protection
Cloud-delivered protection is off. Your device may be vulnerable.

Account protection
No action needed.

Firewall & network protection
Firewalls are turned off. Your device may be vulnerable.

App & browser control
No action needed.

Step 23: In order to make sure that all system files are free from WannaCry I have performed the full scan of all my files, and it displayed no threats found as shown below.



Scan options

Run a quick, full, custom, or Windows Defender Offline scan.

No current threats.
Last scan: 2/21/2020 2:19 AM (full scan)
0 threats found.
Scan lasted 10 minutes 9 seconds
118731 files scanned.

Above all the mentioned steps and images gives the idea about how the system will behave once it gets infected with WannaCry and how we can recover the system from WannaCry and restoring the data from the backups.

8. CONCLUSION

When it comes to any kind of malicious software or malware attacks, knowledge to users about malware attacking vectors and behaviour when infected, is the best possible prevention technique to help eradicate it.

Among all the malware types, Ransomware is the most dangerous kind of malware and its use has been increasing significantly. Preventive measures should be taken before Ransomware takes strong hold and starts to spread across the network from an infected system.

Some of the best prevention techniques are keeping data backups up to date, ensure that systems are up to date with current patches and installing anti-malware solutions with updated signature files would help to prevent from infecting with Ransomware.

Creating software restriction policies is also a good method to prevent infections from attacks like those implemented by malware such as CryptoLocker.

8.1 RECOMMENDATIONS

Use of anti-malware solutions and keeping the backups of data up to date is highly recommended to prevent from infecting systems and from paying ransom to get the encrypted data back.

Other recommendations need to be considered to prevent the infection of dangerous malware either to individual systems or critical systems like servers in the organization, are to install host based IDS/IPS systems that monitors the network activity and alert security experts in case of intrusions. It is also recommended to use firewalls to monitor the complete network activity and performing the deep inspection of packet content for malware patterns.

Providing security awareness training to personnel in the organizations about the social engineering techniques, about threat actors, about performing actions when infected with malware and finally about the persons they need to contact when they have seen any suspicious activities happing on systems, is highly recommended.

ALWAYS BE CAREFUL WHAT YOU CLICK!!

REFERENCES

[1] "Proofpoint,"[Online]. Available: https://proofpoint.com/us/threat-reference/ransomware

[2] K. LAFFAN.[Online]. Available: https://www.varonis.com/blog/a-brief-history-of-ransomware/

[3] K. Zetter, "A Guide to the Global Cyberattack's Scary Method,"[Online]. Available: https://www.wired.com/2017/05/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/

[4] K. C. P. &. L. H. Savage, *The Evolution of Ransomware.* Available: https://its.fsu.edu/sites/g/files/imported/storage/images/information-security-and-privacy-office/the-evolution-of-ransomware.pdf

[5] Rosenberg, "Q&A about the malicious software known as ransomware,"[Online]. Available: https://www.salon.com/test/2015/04/08/a_qa_about_the_malicious_software_known_as_ransomware/

[6] S. Sjouwerman, "History and evolution of Ransomware,"[Online]. Available: https://www.knowbe4.com/ransomware#ransomwaretimeline

[7] C. Cawley, "A History of Ransomware: Where It Started & Where It's Going,"[Online]. Available: https://www.makeuseof.com/tag/history-ransomware-russia-reveton/

[8] J. Segura, "A cyber-criminal's ultimate weapon,"[Online]. Available: https://blog.malwarebytes.com/threat-analysis/2012/11/citadel-a-cyber-criminals-ultimate-weapon/Sheridan

[9] J. Cannell, "Cryptolocker ransomware: what you need to know,"[Online]. Available: https://blog.malwarebytes.com/101/2013/10/cryptolocker-ransomware-what-you-need-to-know/

[10] K. Townsend, "History and Statistics of Ransomware,"[Online]. Available: https://www.securityweek.com/history-and-statistics-ransomware

[11] Kirk, "Apple shuts down first-ever ransomware attack against Mac users,"[Online]. Available: https://www.pcworld.com/article/3040987/apple-shuts-down-first-ever-ransomware-attack-against-mac-users.html

[12] Kirk, "A new Android trojan steals your banking info and holds your files ransom,"[Online]. Available: https://www.pcworld.com/article/3035106/a-new-android-banking-trojan-is-also-ransomware.html

[13] Constantin, "New Locky ransomware version can operate in offline mode,"[Online]. Available: https://www.pcworld.com/article/3095865/new-locky-ransomware-version-can-operate-in-offline-mode.html

[14] J. 2. McAfee Labs Threats Report.[Online]. Available: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-may-2016.pdf

[15] R. Lemos, "How greed could destroy the ransomware racket,"[Online]. Available: https://www.pcworld.com/article/3083772/how-greed-could-destroy-the-ransomware-racket.html

[16] F. Y. Rashid, "4 reasons not to pay up in a ransomware attack,"[Online]. Available: https://www.infoworld.com/article/3043197/4-reasons-not-to-pay-up-in-a-ransomware-attack.html.

[17] S. o. R. 2016, Understanding the Depth of the Ransomware Problem in the United States.[Online]. Available: https://www.malwarebytes.com/pdf/white-papers/UnderstandingTheDepthOfRansomwareIntheUS.pdf

[18] R. Richardson, "Ransomware: Evolution, Mitigation and prevention,"[Online]. Available: https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=5312&context=facpubs

[19] GALLAGHER, "newly evolved ransomware is bad news for everyone,"[Online]. Available: https://arstechnica.com/information-technology/2016/04/ok-panic-newly-evolved-ransomware-is-bad-news-for-everyone/.

[20] J. Albors.[Online]. Available: https://www.welivesecurity.com/2016/05/04/jigsaw-ransomware-becoming-aggressive-new-capabilities/

[21] Timothy Gallo, A. L. (December 2016). *Ransomware.* ISBN: 9781491967881: O'Reilly Media, Inc.

[22] KnowBe4.[Online]. Available: https://blog.knowbe4.com/anatomy-of-a-ransomware-attack-infographic

[23] Aaron Zimba, L. S. (2017). Demystifying Ransomware Attacks: Reverse Engineering and Dynamic Malware Analysis of WannaCry for Network and Information Security. *ZAMBIA INFORMATION COMMUNICATION TECHNOLOGY (ICT) JOURNAL*, pp. 35-40.

[24] "Nakedsecurity,"[Online]. Available: https://nakedsecurity.sophos.com/2016/02/17/locky-ransomware-what-you-need-to-know/

[25] T. Meskauskas.[Online]. Available: https://www.pcrisk.com/removal-guides/9807-locky-ransomware

[26] "Kaspersky,"[Online]. Available: https://www.kaspersky.com/resource-center/threats/ransomware-wannacry

[27] "Wikipedia,"[Online]. Available: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

[28] "Wired,"[Online]. Available: https://www.wired.co.uk/article/bad-rabbit-ransomware-flash-explained

[29] A. I. Fedor Sinitsyn.[Online]. Available: https://securelist.com/bad-rabbit-ransomware/82851/

[30] "Malwarebytes,"[Online]. Available: https://blog.malwarebytes.com/threat-spotlight/2019/12/threat-spotlight-the-curious-case-of-ryuk-ransomware/.

[31] "Malwarebytes,"[Online]. Available: https://blog.malwarebytes.com/threat-analysis/2019/03/spotlight-troldesh-ransomware-aka-shade/

[32] J. Ransomware.[Online]. Available: https://www.knowbe4.com/jigsaw-ransomware

[33] Avast.[Online]. Available: https://www.avast.com/c-cryptolocker

[34] MCafee.[Online]. Available: https://www.mcafee.com/enterprise/en-ca/security-awareness/ransomware/petya.html

[35] "Malwarebytes,"[Online]. Available: https://blog.malwarebytes.com/threat-analysis/2016/12/goldeneye-ransomware-the-petyamischa-combo-rebranded/

[36] "Malwarebytes,"[Online]. Available: https://www.malwarebytes.com/gandcrab/

[37] BlackBlaze.[Online]. Available: https://www.backblaze.com/blog/complete-guide-ransomware/

[38] Hassan, N. A. (November 2019). *A Beginner's Guide to Protecting and Recovering from Ransomware Attacks.* ISBN: 9781484242551: Apress.

[39] Malwarebytes,[Online]. Available: https://www.malwarebytes.com/ransomware/

[40] "Synology,"[Online]. Available: https://www.synology.com/en-us/solution/ransomware?utm_medium=cpc&utm_source=google&utm_campaign=sac--usca-google-search-ransomware--032020&utm_content=general-search&gclid=Cj0KCQjw0pfzBRCOARIsANi0g0vKTthaOfbZw-qX0thdy6VnFIuzl6u1OD6J8ejaQoMY2tIsjX45xkkaAp

[41] "Zdnet,"[Online]. Available: https://www.zdnet.com/article/windows-10-tip-turn-on-the-new-anti-ransomware-features-in-the-fall-creators-update/

[42] TrustedSec.[Online]. Available: https://www.trustedsec.com/blog/incident-response-ransomware-series-part-3/

[43] "GeeksForGeeks," [Online]. Available: https://www.geeksforgeeks.org/types-of-firewall-and-possible-attacks/

[44] "Comodo",[Online]. Available: https://www.comodo.com/resources/home/how-firewalls-work.php

[45] A. D. Ray Blair, "Types of Firewalls," [Online]. Available: https://www.networkworld.com/article/2255950/chapter-1--types-of-firewalls.html

[46] T. HEER and O. KLEINEBERG, "Firewall functions and roles for company security," SEPTEMBER 13, 2017. [Online]. Available:

https://www.controleng.com/articles/firewall-functions-and-roles-for-company-security/

[47] C. RUDIN, "SIKICH," [Online]. Available: https://www.sikich.com/insight/does-a-firewall-protect-against-malware-and-ransomware/

[48] K. S. Murugiah Souppaya, "Guide to Malware Incident Prevention and handling for Desktops and Laptops," National Institute of Standards and Technology , July 2013.

[49] G. S, "Intrusion Detection System (IDS) – A Detailed Guide & Working Function - SOC/SIEM," [Online]. Available: https://gbhackers.com/ids/

[50] I. G. P. V. &. J. K. Ansam Khraisat, "Survey of intrusion detection systems: techniques, datasets and challenges," Available: https://cybersecurity.springeropen.com/articles/10.1186/s42400-019-0038-7, 2019.

[51] Tyra, "Phishing Definition, Prevention, and Examples," [Online]. Available: https://resources.infosecinstitute.com/category/enterprise/phishing/#gref

[52] E. B. Joxean Koret, *Antivirus Hacker's Handbook,* https://repo.zenk-security.com/Magazine%20E-book/Antivirus%20hackers%20handbook.pdf

[53] Y. D. Erdal Ozkaya, Cybersecurity – Attack and Defense Strategies - Second Edition, ISBN: 9781838827793: Packt Publishing, December 2019.

[54] J. Kirk, "PCWorld," [Online]. Available: https://www.pcworld.com/article/3054591/with-few-options-companies-increasingly-yield-to-ransomware-demands.html

[55] L. Abrams, "BLEEPINGCOMPUTER," New Scheme: Spread Popcorn Time Ransomware, get chance of free Decryption Key, 2016. [Online]. Available: https://www.bleepingcomputer.com/news/security/new-scheme-spread-popcorn-time-ransomware-get-chance-of-free-decryption-key/