Ransomware- Its Prevention and Exclusion using Assorted Tools

Dr. T. Venkat Narayana Rao[1], Varsha Challa[2]
Professor[1], Student[2], Department of C.S.E
Sreenidhi Institute of Science and Technology
Yamnampet, Hyderabad, India

Abstract: Ransomware is similar to cyclone that creates data instability. The securely holded user data will be abducted. This has emerged as a malware through which user data is locked or encrypted till the ransom is paid. It is one of the fast evolving malware. Gaining income is the main motive of this ransomware. This paper focuses on various preventive measures to counter malice and can aid in eradicating ransomware. The paper also emphasize on various techniques and tools that can stamp out ransomware.

***Keywords**: Ransomware, cyber, attack, malware, encrypt.*

*****

I. Introduction

Despite the increased efforts of cyber security by the professionals across the world, cyber crimes are on the rise. Among all these, ransomware attacks are gaining more attention**.** Ransomware is a kind of malware or a Trojan that restricts by either preventing or limiting users from accessing their system, either by encypting or locking the system screen or by locking the user's personal files until and unless a ransom is paid. Some ransomwares which lock the screen can be easily unlocked by some knowledgeable person. Advanced malwares uses techniques like cryptoviral extortion which will encrypt user personal files and data.The intention for ransomware attacks is so clear unlike other attacks, victim will be notified regarding attack and the ransom would be demanded as per the attack. Payment demanded would generally be bitcoin so the extortionist identity is not known but it does not restrict only to bitcoin but some other prepaid vouchers like paysafe ,ukash are also demanded. Clear instructions and process is displayed for the user regarding the process of the payment. Bitcoin demanded may vary from some hundreds to thousands as per the attack. The revenue obtained from ransomware is so secure for cyber criminals. Major ransomware will encrypt , deny the access or obfuscate the data, the user will be automatically locked out of the systems themselves[1]. It is a severe online threat . Ransomware is not particular to any geographical location. All operating systems are in endanger of the reansomware .Through a virus, files are infected but through a ransomware files are not infected but blocked. The antivirus can clear the virus but files once encrypted cannot be cleared with antivirus. It is hard to get the files back once encrypted. Attacks by wanna cry ransomware are increasing. 12 May 2017 ,a huge cyber attack has been noticed, it infected more than 230,000 computers over 150 countries all over world and demanded the amount. Recently in January 2018 a new ransomware version of virus named GandCrab was detected.The first ransomware was observed in 1989 by Joseph Popp in his floppy disk by a AIDS Trojan ,he was demanded $189 to provide him with the decryption tool.That Trojan was also named as PC Cyborg. In January 2015 ransomware attacks on linux and web based server were reported. There is an international growth in ransomware, Around 181.5 million attacks of ransomware were noted in starting 6 months of 2018 with a 229% of increase in attacks with respect to the previous year. Ransomware successfully moved from a small floppy disks to advanced techniques, it is not just limited to systems but also phones, tablets, and networks as well. Previously only doc, pdf , jpg , xls extension files were encrypted. The attack on the network linked storages on the synology was observed in the August 2014 with discovery of a new Trojan.

Ransomware earnings

Ransomware easily earns millions of dollars a year. Per month it generates a amount of $90,000 and costing them around $5000 resulting in a profit of $85,000 per one month. Approximately expected to bank a annual revenue of $1m by cyber criminals upon a estimation 0.5% of affected victims pay $300 and the estimation varies till $90,000. Cryptolocker successfully earned an estimation of $3 million before its restriction by authorities and cryptowall and was so successful that it earned $18 million in just a month which was June 2015 according to a report of US FBI. In 2017 the ransomware amount demanded was an average of $522 which is a high amount paid for getting back a one's own property. A globally reported loss amount for ransomware attacks are in $100 millions . In most of cases ransomware demands fine with a range of $100 to $3000 by any prepaid vouchers. Here, bitcoins are not demanded as it forges a law enforcement category. An average ransomware engineer is earning $2500 for a single incident.

II. How Does Ransomware Work

Ransomware generally enters the system through Trojan , which is entered via various forms. Email is the easiest for ransomware to enter. A malicious attachment would be embedded in a link and that can be transmitted through a phishing email. Email is chosen as it is simplest and direct way, it works either by opening the infectious link or by directing the victim directly to infected or malicious website. It also targets by using vulnerabilities in the network. Ransomware also enter by downloading malicious documents from drives which is done automatically while a person is surfing the web.Through macros it automatically downloads the malicious code in document and executes to run the ransomware. If macros are disabled by user it obfuscates the document and asks victim to enable macros to see the document clearly then enabling macros downloads the ransomware. In recent days java script files are used as attachments to deliver the ransomware than using word documents.Second major form to attack would be exploit kits. It is a malicious tool used to analyze security and find loop holes in the victims system and to find software that are not updated and the hacker takes advantages of these vulnerabilities to inject ransmware. This code is nicely wrapped in exploit tool to find the particular vulnerabilities and allowing ransomware to download at that particular points.*Wannacryransomware* travels in a automatic way among various computers without the user knowledge and interaction through drive by download where it is installs without user knowledge. *Crypto* ransomware infects through encryption. Encryption takes place in three step process[2].

In the first stage a pair of key is generated by the attacker and the corresponding key required to decrypt is placed in the malware and that malware is released to the victim.This is from attacker to victim stage.

The second stage is from victim to attacker stage where the extortion carries out the crypto viral attack then malware encrypts data using public key present in the malware by generating some random symmetric key. Now encryption is completed and the victim is notified saying files are encrypted.this is a hybrid encryption. Victim requires the decryption key present at attacker to remove the encryption. Thus, victim is left with no other option except to pay the ransom demanded to get the decryption key. Then the amount is transferred from the victim side to the attacker side.

The third stage is from attacker to victim side where the attacker after receiving the payment checks the attacker private key and then releases the symmetric decryption key to the victim which decrypts the files, with this the process is completed. No two randomly generated keys will be the same.

In the deep web the cyber criminals, can purchase ransomware kits and use specific software tools which can create different ransomware with required necessity. This process enables specialized capabilities and provides required malware when paid the required bitcoins to that malware provider in deepweb. In 2016 a different approach called malvertising was popular which is also known as malicious advertising it takes advantage of online advertising and to distribute the malware. While user is using regular or legitimate sites the malware directs the victim to illegal and criminal sites without the interaction of user. The location of the user is traced and accordingly suitable amount is demanded forging the law sections.

Simply, ransomware attacks can be viewed in three stages first is delivery, through various methods ransomware is transmitted. Second is execution where all the files and security issues are studied and decides which data and what extension files to be handled. Third is encryption, this encryption takes place in minutes and sometimes even in seconds *chimera* ransomware just requires 18 seconds to encrypt the data. Encryption will be done as shown in figure 1. Once the ransomware attacks it uses various complex algorithm to encrypt the data various algorithms such as RSA and RC4 etc.

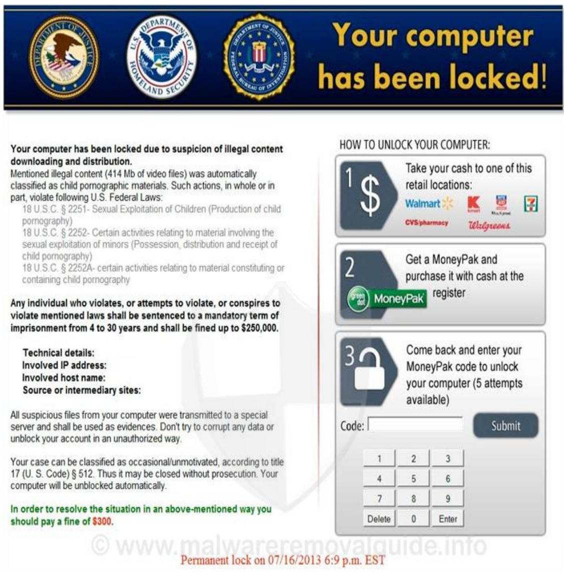
Figure 1: Ransomware attacks stages

There are various reasons why antivirus is not able to detect the ransomware. Antivirus performs normal working methods by routine scanning of files for a search of specific kind of signature with available malwares in the database. This is a perfect method to detect normal virus and malware . But it cannot detect very new malware or the old malware that has changed its signature with repackaged new various signatures. Cyber criminals caught this method of weakness with antivirus. They make variations to malware that could not be understood by antivirus like polymorphic malware where it can change its forms and can be mutable to various signatures. Such malwares slip through antivirus and through obfuscators and there exist certain tools to modify the appearance and make the file unrecognizable and undetectable by the antivirus.

III. Types of Ransomware

Ransomware has various sizes, appearance and shapes and commonly have a same thing that is they demand ransom, but based on their action and performance they are mjorly classified into two categories they are: *Lockscreenransomware* and *Encryption* ransomware

Lockscreenransomware : When an individual view a site and the system issue a notification to confirm regarding any action then all of a sudden the victim screen will be locked and the screen is completely seized and receives a message or notice stating that the screen is locked and a particular amount is to be paid to unlock the screen[3]. This compels in user inability in moving further. User has no other option except to pay the amount as the complete operating system will be locked. Notice is present on the complete screen blocking all other windows. Here, only the screen will be blocked but the files are not encrypted. Lockscreen page looks as shown in figure 2.



Your computer has been locked!

Your computer has been locked due to suspicion of illegal content downloading and distribution.

Mentioned illegal content (414 Mb of video files) was automatically classified as child pornographic materials. Such actions, in whole or in part, violate following U.S. Federal Laws:

18 U.S.C. § 2251- Sexual Exploitation of Children (Production of child pornography)
18 U.S.C. § 2252- Certain activities relating to material involving the sexual exploitation of minors (Possession, distribution and receipt of child pornography)
18 U.S.C. § 2252A- certain activities relating to material constituting or containing child pornography

Any individual who violates, or attempts to violate, or conspires to violate mentioned laws shall be sentenced to a mandatory term of imprisonment from 4 to 30 years and shall be fined up to $250,000.

Technical details:
Involved IP address:
Involved host name:
Source or intermediary sites:

All suspicious files from your computer were transmitted to a special server and shall be used as evidences. Don't try to corrupt any data or unblock your account in an unauthorized way.

Your case can be classified as occasional/unmotivated, according to title 17 (U. S. Code) § 512. Thus it may be closed without prosecution. Your computer will be unblocked automatically.

In order to resolve the situation in an above-mentioned way you should pay a fine of $300.

HOW TO UNLOCK YOUR COMPUTER:

1 $ Take your cash to one of this retail locations:

2 Get a MoneyPak and purchase it with cash at the register

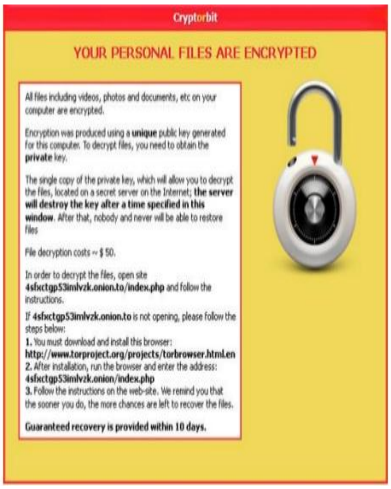
3 Come back and enter your MoneyPak code to unlock your computer (5 attempts available)

Code:

Permanent lock on 07/16/2013 6:9 p.m. EST

Figure 2 : Lockscreen Page view

Encrypting ransomware: Encryption is the process where various important files and documents are altered by the ransomware making the user unable to use those specific data and demanding a particular amount to provide the user with decryption key. A scheduled time will be given to user saying if not paid in that deadline key required to decrypt the data would be deleted. All the potential vulnerabilities are exploited for encryption. All the business information and personal files can be encrypted[4]. Files are deleted and payment note along with instructions to the payment is generally placed in the same folder. The victim cannot access that files which are encrypted but can use various other windows unlike lockscreenransomware. Encryption page looks similar as shown in figure 2.1.



Cryptorbit

YOUR PERSONAL FILES ARE ENCRYPTED

All files including videos, photos and documents, etc on your computer are encrypted.

Encryption was produced using a **unique** public key generated for this computer. To decrypt files, you need to obtain the **private** key.

The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; **the server will destroy the key after a time specified in this window**. After that, nobody and never will be able to restore files

File decryption costs ~ $ 50.

In order to decrypt the files, open site **4sfxctgp53imlvzk.onion.to/index.php** and follow the instructions.

If **4sfxctgp53imlvzk.onion.to** is not opening, please follow the steps below:
1. You must download and install this browser: **http://www.torproject.org/projects/torbrowser.html.en**
2. After installation, run the browser and enter the address: **4sfxctgp53imlvzk.onion/index.php**
3. Follow the instructions on the web-site. We remind you that the sooner you do, the more chances are left to recover the files.

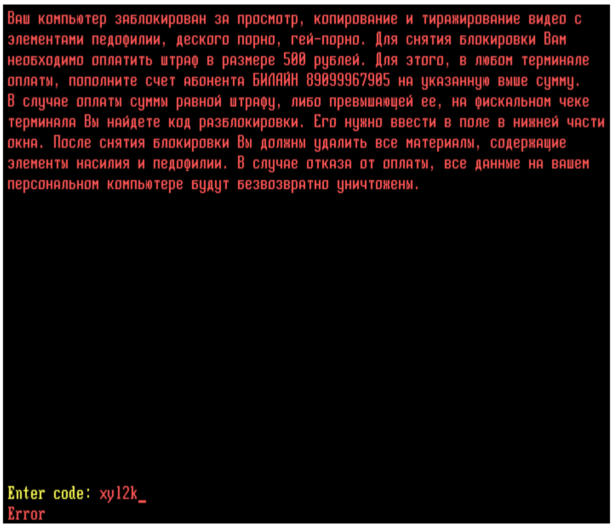
Guaranteed recovery is provided within 10 days.

Figure 2.1 : Encryption page view

Type of ransomwares

A) Master Boot Record (MBR) Ransomware

This ransomware affects the hardware and interrupts the normal boot process by loading the malicious code in the original operating system and do not allow normal operating system to execute. By this the system forcibly restarts by taking the infection and the note regarding payment details would be displayed on the screen after the reboot process. After the payment the ransomware would be removed and previous settings would be restored. Master boot Record ransomware attacked page looks similar as shown in figure 2.2.



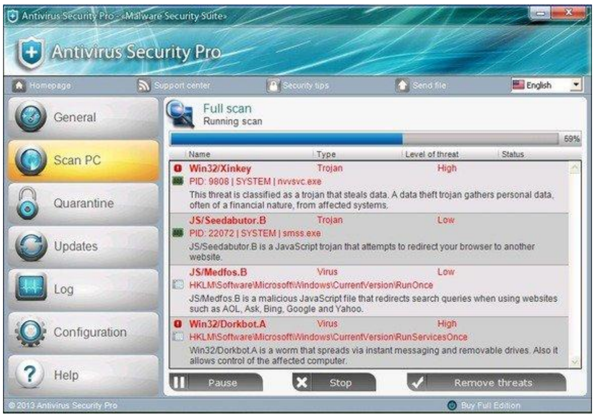
```
Ваш компьютер заблокирован за просмотр, копирование и тиражирование видео с
элементами педофилии, деского порно, гей-порно. Для снятия блокировки Вам
необходимо оплатить штраф в размере 500 рублей. Для этого, в любом терминале
оплаты, пополните счет абонента БИЛАЙН 89099967905 на указанную выше сумму.
В случае оплаты суммы равной штрафу, либо превышающей ее, на фискальном чеке
терминала Вы найдете код разблокировки. Его нужно ввести в поле в нижней части
окна. После снятия блокировки Вы должны удалить все материалы, содержащие
элементы насилия и педофилии. В случае отказа от оплаты, все данные на вашем
персональном компьютере будут безвозвратно уничтожены.

Enter code: xyl2k_
Error
```

Figure 2.2: Master Boot Record ransomware

B) Scareware

It is bogus software containing fake antivirus and other security tools, it pretends to be a real antivirus. Scareware informs user that it had found few issues in the system and demands an amount to rectify the issue. Even if the payment is not done all the files and documents in the system are safe. Some can also lock the screen and some flood may pop ups , alerts and many messages . The above are easy ransomware to be removed. Scareware page consists of all fake tools as shown in figure 2.3.



Full scan
Running scan
59%

Name	Type	Level of threat	Status
Win32/Xinkey PID: 9808 | SYSTEM | nvvsvc.exe This threat is classified as a trojan that steals data. A data theft trojan gathers personal data, often of a financial nature, from affected systems.	Trojan	High	
JS/Seedabutor.B PID: 22072 | SYSTEM | smss.exe JS/Seedabutor.B is a JavaScript trojan that attempts to redirect your browser to another website.	Trojan	Low	
JS/Medfos.B HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce JS/Medfos.B is a malicious JavaScript file that redirects search queries when using websites such as AOL, Ask, Bing, Google and Yahoo.	Virus	Low	
Win32/Dorkbot.A HKLM\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce Win32/Dorkbot.A is a worm that spreads via instant messaging and removable drives. Also it allows control of the affected computer.	Virus	High	

Figure 2.3: Scareware page

C) Doxware

It is also known as leakware, it has a different kind of approaches. Doxware threatens the user by stealing the personal data , images and sensitive data saying if specific ransom is not paid all those information would be published online. With this the user gets panic about their privacy and pay the amount when the files are stolen.

D) Android MobileRansomware

Ransomware is not restricted to systems and networks even the android mobiles are not safe from this ransoware. Android is infected by wannacry through gaming forums. The ransomware enters the mobile through third party applications and the malware is distributed in the form of apkfile [5]. Since synchronization is easily possible in android mobiles there is no point of encrypting the data, hence the criminals lock the screen of mobile or steals the sensitive data and demands the specific amount to unlock the screen.

E) IOTRansomware

In this the attackers are not interested in either locking or encrypting the data, but they try to take the control of various things that are operated through internet by the particular user.

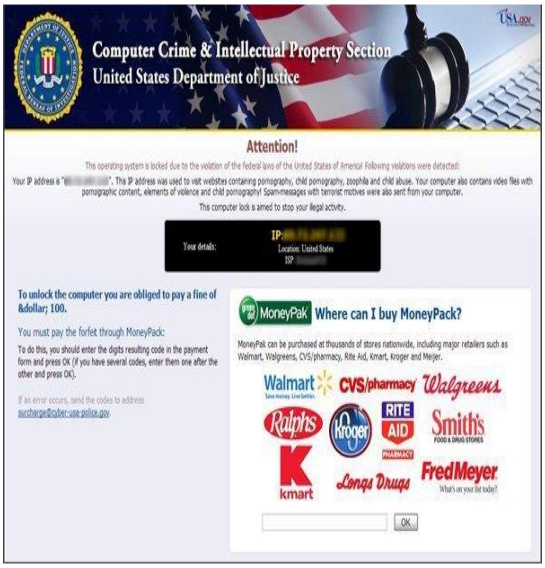
F) Macransomware

Inspite of high security provided the mac is still in danger of ransomware. It enters the mac either by email or by directing to malicious websites. Initially ransomware targeted OS X, but later apple released XProtect and it was cleared. The icloud accounts are often targeted by criminals. By using find my iphone option they try to lock the mobile.

IV. Some Major Ransomwares

A. Reveton

In 2012, raveton began to spread by a major ransomware Trojan. This displays a fake and severe warning saying that a notice from law agency and states that the system was used for criminal and illegal activities like using or downloading. It further indicates that private software or any unlicensed software is in use and performing activities such as encouraging terrorism and child pornography. The user is then asked to pay the specific fee to unlock the system thinking it is from the real law agency, the user pays the specific amount with fear to get the system unlocked. Since the criminals pretend as law enforcement agency and lock system they generally ask only prepaid vouchers. To increase the illusion the user that it is really from the law agency the ip address of the system will be hacked and displayed and footages. The pictures and logos of the law are presented on the screen to make the victim believe. Password stealing makware is also distributed by raveton in 2014. The fraud law page from police looks as shown in figure 4.


USA.gov
Computer Crime & Intellectual Property Section
United States Department of Justice
Walmart
Save money. Live better.
CVS/pharmacy
Walgreens
Ralphs
Kroger
RITE AID PHARMACY
Smith's FOOD & DRUG STORES
kmart
Longs Drugs
FredMeyer
What's on your list today?
OK

Attention!

This operating system is locked due to the violation of the federal laws of the United States of America! Following violations were detected:

Your IP address is "[redacted]". This IP address was used to visit websites containing pornography, child pornography, zoophila and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.

This computer lock is aimed to stop your illegal activity.

Your details: IP:[redacted]
Location: United States
ISP [redacted]

To unlock the computer you are obliged to pay a fine of &dollar; 100.

You must pay the forfeit through MoneyPack:

To do this, you should enter the digits resulting code in the payment form and press OK (if you have several codes, enter them one after the other and press OK).

If an error occurs, send the codes to address surcharge@cyber-usa-police.gov.

MoneyPak Where can I buy MoneyPack?

MoneyPak can be purchased at thousands of stores nationwide, including major retailers such as Walmart, Walgreens, CVS/pharmacy, Rite Aid, Kmart, Kroger and Meijer.

Figure 4 : Fraud law page view

B. CryptoLocker

In September 2013 encryption ransomware reappeared with a Trojan known as cryptolocker. Distributed through email and gameoverzeus. In this the command control server is uploaded with a 2048 bits of RSA key pair and then encrypts the data with specific file extensions. Later it threatens the user to pay the amount else the key required to decrypt data will be destroyed in particular time. As a large key it is difficult to repair in that specific deadline. Later the online tools would be available to obtain the key which would demand even higher amount than the extortionist. It came to an end when the gameoverzeusbotnet was isolated in june 2014

C. CryptoWall

Cryptowall was first appeared in 2014. This ransomware targets windows. It is part of propagation through malvertising at zedo advertising network and later various websites were targeted which directs the user to nasty websites and downloads the payload using the browser plugin exploits. Cryptowall 3.0 as part of email attachment uses payload that was in the form of java script and downloads jpg images. It also installs spyware by deleting volume shadow and then steals bitcoin wallets passwords.

D. WannaCry

Wannacry started spreading through internet in may 2017. The eternalblue exploit vector leaked from national security agency of united states it was in rise and in a unpredictable manner infected over 230,000 computers in more than 150 countries in various languages for sake of bit coins. Asymmetric encryption is the method used by wannacry to attack the users that the victim cannot easily find the key.

E. Petya

It was first found in march 2016.it is also a kind of encryption ransomware, it is targeted for master boot record .it encrypts the NTFS files by installing a payload, blocking the windows booting and demands the payment. these are reported in fewer number of cases than other ransomwares.a global cyber attack mainly targeting Ukraine was found on june 2017 by using eternalblue exploit, due to some change in design even after the payment they were unable to unlock systems.security analysts confirmed that this was occurred to create a disruption but not for sake of payment.

V. The Victims Of Ransomware

The initial stage of ransomware attacks was on individual persons that is on a single system. However, now the cybercriminals has analyzed and its productivity and potential has shifted been to business and targeted global entrepreneurs. 35% small and medium business and 12.3% large businesses were targeted. Majorly western part was focused with Canada US and UK as main target as their target is generally based on population and income earned by people. The ransomware shifted the target from individuals to organizations. Anyone holding the important files and data in the system or network are at risk of ransomware. Many government sectors or law enforcement agencies and hospitals stored their reputed data and would not take any chance to lose any data. The government sectors, hospital and firms pay the fine immediately for their access since they need immediate access on their files and keep this information private for reputation sake, though there is no guarantee that the data is secured. A person working more on mails, surfing with sensitive data is usually at a risk. Location of a famous person can be traced and a ransom could be demanded. Ransomware can also target an individual who's OS and softwares are not updated. If not under any of these categories are also in a risk of ransomware since it spreads easily through internet.

VI. Signs Of Ransomware

- If the user is unable to open a file.
- Various messages on desktop that are alarmed.
- Count down for a warning messages.
- Pop up with the message of payment with instructions to pay.
- Automatic downloads and mismatched file Extensions.
- Corrupted data.
- Messages once opened and that cannot be Closed.
- Names of the directories are changed Automatically.
- Files unable to open[6].
- Data lost.

Dos and don'ts of ransomware

Ransomware is a high profit market and that is difficult to stop so it is better to have knowledge on ransomware and to know do's and dont's to prevent ransomware

Do's:

- A security tools and softwares must be used.
- All security essentials must be updated.
- All operating systems must be updated.
- Always have a good backup system.
- Use cloud services for storing the data

Don't's:

- Open a spam mail.
- Download a suspicious attachment.
- Visit malicious websites.
- Enable macros.
- Open link in emails.
- Pay amount.

VII. How to Prevent Ransomware

It is better to prevent the ransomware before attack rather than to remove it after the files are deleted or encrypted. The ransomware prevention is similar to other kinds of malware as given below.

i. Back up your important files: The best defence for ransomware would be backing up the useful data with external sources like pen drive , SD card, various cloud storages like Google drive and drop box etc.[7]. If the data is stored in external drives make sure that the external drives must not be connected to the device as malware might even spread to the external drives. Back up data into various clouds as shown in figure 7.1.

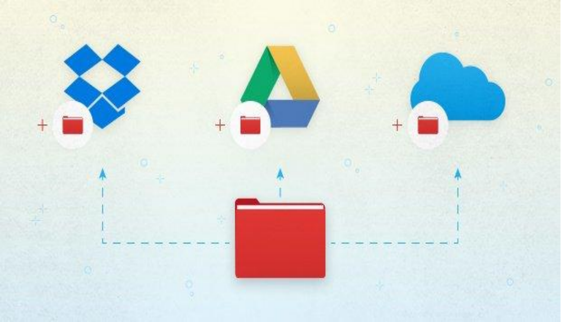


Figure 7.1: Back up process

ii. Update antivirus: A proper antivirus is essential for the prevention of any virus and malware. A free antivirus named AVG antivirus does a lot of malware prevention. Another software named AVG Internet Security that gives protection for the system from ransomwares, and blocks applications that modify the user files and that are suspicious. There is a security solution called InterScan Web Security that do not allow ransomware to reach the user system through emails and web pages. Trend Micro Security 10 also provides protection for the user data by blocking various malwares attacking through malicious websites and various threats associated with these sites.

iii. Operating system must be updated: The operating systems that are not updated are more likely to be attacked by ransomware. WannaCry takes advantage of vulnerabilities in softwares that are not updated. Thus, all the operating systems must be updated and all the patches in the OS must be rectified.

Iv. Browser must be clean: Adware invasions must be prevented by avoiding add-ons and junk toolbars. The stages of attacks and corresponding security solution are shown in figure 7.2.

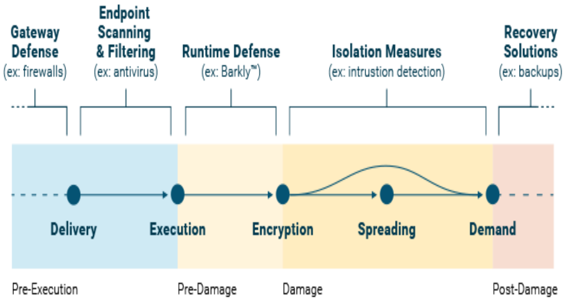

Gateway Defense (ex: firewalls)
Endpoint Scanning & Filtering (ex: antivirus)
Runtime Defense (ex: Barkly™)
Isolation Measures (ex: intrustion detection)
Recovery Solutions (ex: backups)
Delivery
Execution
Encryption
Spreading
Demand
Pre-Execution
Pre-Damage
Damage
Post-Damage

Figure 7.2 : Stages of attacks

E-mails play a major role in transmitting the malware , user must always be careful with the suspicious and spam mails especially that contain attachments. Email spoofing and phishing must be prevented by enabling strong spam filters. Unless sure that the mail is official the user must not enable the macros. Whitelistening software must be installed to prevent third party applications that are unauthorized. Ransomware has a malware that is complicated so the protection used must be in a multiple layers to avoid threats. Firewalls must be configured in such a way that atleast known IP addresses of malicious websites must be blocked. The firewall must be up to date. User must be aware of the malware and its detection. Many extortionists take the advantage of weaknesses of users. All the users must be educated regarding the attacks , prevention and removal methods. In an organization, just a individual knowledge regarding the cyber security is not enough and the personals working in the organization must also have the knowledge in lines of various attacks, spam mails and also phishing attacks. Removing the ransomware is not possible all the times so it is better to prevent than removing the ransomware and other reasons like backup is not always efficient as only 42% of organizations that were attacked with ransomware were able to recover the full data. Time is valuable in IT industry as it eats lot of time once ransomware attacks.

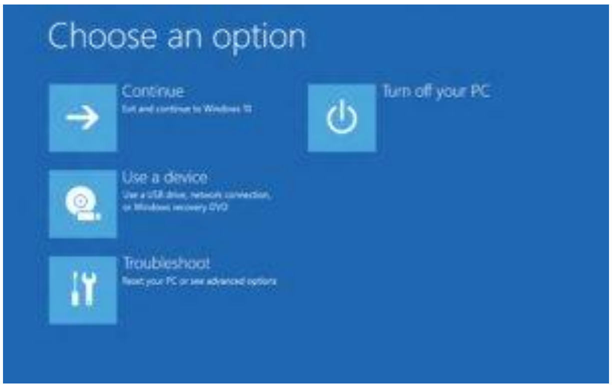
VIII. Removing Ransomware

If the user is locked or prevented from entering windows by a ransomware, a option called system restore can be used to roll back windows in time this is not going to affect personal files but just return to a previous state of programs that system had a certain time, system restore option should be enabled prior to using this option.

To remove ransomware on windows 7, Open advanced boot options and then select repair your computer and select enter Advanced boot options in windows 7 by pressing F8 in the booting. The restoration process would be started by following these steps:

1. Shut down and turn on the system then as something appears on the screen start pressing F8 key in a repeated manner,then the user is taken to advanced boot options menu as shown in figure 8.
2. Repair your computer must be selected followed by enter.
3. Login as user, select the account name of windows and then enter the password.
4. After logged on select the system restore.

Windows 8, 8.1, or 10. The advanced boot option are shown in figure 8.



Choose an option

Continue
Exit and continue to Windows 10

Turn off your PC

Use a device
Use a USB drive, network connection, or Windows recovery DVD

Troubleshoot
Reset your PC or see advanced options

Figure 8: Advanced boot options

1. Recovery option here can be obtained by selecting shift while rebooting the login screen of windows then click power button then restart
2. This will reboot and direct to the recovery screens.
3. Go to troubleshoot then select the advanced options and then click on system restore.

Before restoring the system windows 10 must be rebooted to safe mode, software anti-malware must be installed, system must be scanned for ransomware programs and then the system settings must be restored to previous state. Following the above steps the malware can be removed but the files cannot be decrypted[8][9].
Even if this system restore is not helping to get back into windows by removal of ransomware then try to run a virus scanner through a USB drive or a bootable disc , this refers to scanning of virus through offline means such as nortan , avast and sophos etc. If this booting doesnot help then open folder options and select show hidden files and which takes few couple of seconds. After selecting this if the data reappears then it is easy to fix the problem, open the file explorer of computer then go to c drive select users then open windows account name folder apply right click on the folders that are hidden then uncheck the hidden attributes from the properties then select OK. This would remove the ransomware. If the data is backed up then directly we can sync the data without all above steps.
What must be done even if data is not able to be accessed? The user must try to recover the data that was encrypted from various forms, there are three major methods to recover the data:
1. Recovery of deleted data through Backup: it is the easiest way to recover all the files that were damaged through ransomware. Data can be restored through external backup devices[8]. This option can be used if and only if the user backed up data from time to time in external sources like SD card,hard disk , pen drive or cloud storages.
2. Recovery of deleted data through data recovery software: if the victims data is not backed up in any of the external sources then the user can retrieve the data through data recovery software.
3. Recovery of deleted files through services of ransomware data recovery. This option is helpful when the above two measures doesnot work, this takes the help of services from ransomware virus .

IX. Conclusion

Ransomware attacks have a devastating effect on small scale organizations i.e. not only small scales but also various individuals. In spite of high cyber security the attacks of ransomware are increasing constantly, none of the data is safe. When it comes to ransomware knowledge, the best possible weapon is to prevent it. The various preventive actions must be taken to withstand the high attacks. Even the paying of demanded amount does not guarantee the user data. Various kinds of bitcoins and blockchains must be banned so that the rate of ransomware would be decreased.

References:

[1]. Dr. Wajeb GHARIBI, Computer Science & Information Systems College, JazanUniversity,Jazan, KSA.
[2]. 2016 IEEE 36th International Conference on Distributed Computing Systems.
[3]. International Journal of Computer Applications (0975 – 8887) Volume 164 – No 7, April 2017.
[4]. International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 6 Issue 4 April 2017, Page No. 20915-20919 Index Copernicus value (2015): 58.10 .
[5]. Hindawi Publishing Corporation Mobile Information Systems Volume 2016, Article ID 2946735, 9 pages
[6]. International Journal of Engineering Research and Technology. ISSN 0974-3154 Volume 10, Number 1 (2017).
[7]. AlexanderAdamov, «Computer Threats: Methods of Detectionand Analysis», Kaspersky Lab, Moscow 2009.
[8]. International Journal of Scientific & Engineering Research Volume 4, Issue 1, January-2013.
[9]. Volume 14, 2017 Ransomware: A research and a personal case study of dealing with this nasty malware.