The Most Dangerous Cyber Security Threat Ransomware Prevention

Swapna Siddamsetti
M.Tech, Sr. Asst. Prof.
Aurora's Technological and Research Institute
vooreswapna205@gmail.com

Naresh Sabavat
M.Tech, Asst Professor
Aurora's Technological and Research Institute

Abstract: Ransomware is a type of malware that can be covertly installed on a computer without knowledge or intention of the user that restricts access to the infected computer system in some way,[1] and demands that the user pay a ransom to the malware operators to remove the restriction. The cryptovirology form of the attack has ransomware systematically encrypt files on the system's hard drive, which becomes difficult or impossible to decrypt without paying the ransom for the decryption key. Other attacks may simply lock the system and display messages intended to coax the user into paying. Ransomware typically propagates as a Trojan, whose payload is disguised as a seemingly legitimate file. This research will protect the system from this dangerous attack by making the operating system very strong.

Keywords:*malware, cryptovirology, ransom, encrypt, Trojan, decryption*

*****

I. Introduction

This research is mainly abot one of the coon threat to cybersecurity threat called “Ransomware” typically propagates as a Trojan, entering a system through, for example, a downloaded file or a vulnerability in a network service. The program then runs a payload, which typically takes the form of a scareware program. Payloads may display a fake warning purportedly by an entity such as a law enforcement agency, falsely claiming that the system has been used for illegal activities, contains content such as pornography and "pirated" media, or runs a non-genuine version of Microsoft Windows.

Some payloads consist simply of an application designed to lock or restrict the system until payment is made, typically by setting the Windows Shell to itself,[11] or even modifying the master boot record and/or partition table to prevent the operating system from booting until it is repaired. The most sophisticated payloads encrypt files, with many using strong encryption to Payment is virtually always the goal, and the victim is coerced into paying for the ransomware to be removed—which may or may not actually occur—either by supplying a program that can decrypt the files, or by sending an unlock code that undoes the payload's changes. A key element in making ransomware work for the attacker is a convenient payment system that is hard to trace.

A range of such payment methods have been used, including wire transfers, premium-rate text messages, pre-paid voucher services such as Paysafecard, and the digital currencyBitcoin. A 2016 census commissioned by Citrix revealed that larger business are holding bitcoin as contingency plans.

The first known ransomware was "AIDS" (also known as "PC Cyborg"), written in 1989 by Joseph Popp. Its payload hid the files on the hard drive and encrypted their names, and displayed a message claiming that the user's license to use a certain piece of software had expired. The user was required the user to pay US$189 to "PC Cyborg Corporation" in order to obtain a repair tool. Popp was declared mentally unfit to stand trial for his actions, but he promised to donate the profits from the malware to fund AIDS research.

The notion of using public key cryptography for such attacks was introduced in 1996 by Adam L. Young and Moti Yung. Young and Yung showed that the AIDS Trojan was ineffective due to its use of symmetric cryptography, since the decryption key can be extracted from its code, and implemented an experimental proof-of-concept cryptovirus on a Macintosh SE/30 that used RSA and Tiny Encryption Algorithm (TEA) to hybrid encrypt the victim's data. Young and Yung also proposed that electronic money could be extorted through encryption as well, so that "the virus writer can effectively hold all of the money ransom until half of it is given to him".[13] They referred to these attacks as being "cryptoviral extortion", an overt attack that is part of a larger class of attacks in a field called cryptovirology, which encompasses both overt and covert attacks.

II. Literature Review

Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid. More modern ransomware families, collectively categorized as crypto-ransomware, encrypt certain file types on infected systems and forces users to pay the ransom through certain online payment methods to get a decrypt key.

Ransom Prices and Payment

Ransom prices vary depending on the ransomware variant and the price or exchange rates of digital currencies. Thanks to the perceived anonymity offered by cryptocurrencies, ransomware operators commonly specify ransom payments in bitcoins. Recent ransomware variants have also listed alternative payment options such as iTunes and Amazon gift cards. It should be noted, however, that paying for the ransom does not guarantee that users will get the decryption key or unlock tool required to regain access to the infected system orhostaged files.

Ransomware Infection and Behavior

Users may encounter this threat through a variety of means. Ransomware can be downloaded onto systems when unwitting users visit malicious or compromised websites. It can also arrive as a payload either dropped or downloaded by other malware. Some ransomware are known to be delivered as attachments from spammed email, downloaded from malicious pages through malvertisements, or dropped by exploit kits onto vulnerable systems.

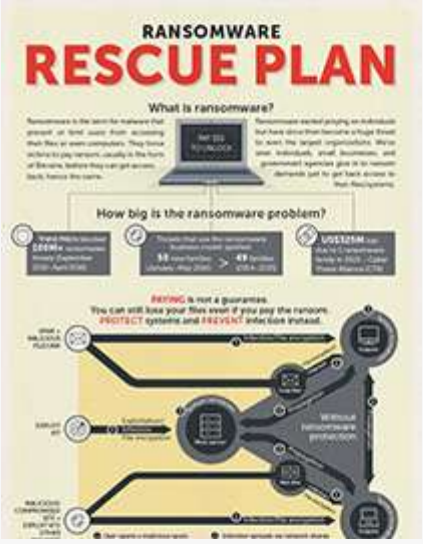
Once executed in the system, ransomware can either lock the computer screen, or, in the case of crypto-ransomware, encrypt predetermined files. In the first scenario, a full-screen image or notification is displayed on the infected system's screen, which prevents victims from using their system. This also shows the instructions on how users can pay for the ransom. The second type of ransomware prevents access to files to potentially critical or valuable files like documents and spreadsheets.

Cases of ransomware infection were first seen in Russia between 2005 – 2006. Trend Micro published a report on a case in 2006 that involved a ransomware variant (detected as TROJ_CRYZIP.A) that zipped certain file types before overwriting the original files, leaving only the password-protected zip files in the user’s system. It also created a text file that acted as the ransom note informing users that the files can be retrieved in exchange for $300.

In its earlier years, ransomware typically encrypted particular file types such as DOC, .XLS, .JPG, .ZIP, .PDF, and other commonly used file extensions.

In 2011, Trend Micro published a report on an SMS ransomware threat that asked users of infected systems to dial a premium SMS number. Detected as TROJ_RANSOM.QOWA, this variant repeatedly displayed a ransomware page to users until they paid the ransom by dialing a certain premium number.

Another notable report involved a ransomware type that infects the Master Boot Record (MBR) of a vulnerable system, preventing the operating system from loading. To do this, the malware copies the original MBR and overwrites it with malicious code. It then forces the system to restart so the infection takes effect and displays the notification (in Russian) once the system restarts.


RANSOMWARE
RESCUE PLAN
What is ransomware?
How big is the ransomware problem?
PAYING is not a guarantee.
You can still lose your files even if you pay the ransom.
PROTECT systems and PREVENT infection instead.

View infographic: Ransomware 101 - What, How, & Why

Ransomware Spreads Outside Russia

Ransomware infections were initially limited to Russia, but its popularity and profitable business model soon found its way to other countries across Europe. By March 2012, Trend Micro observed a continuous spread of ransomware infections across Europe and North America. Similar to TROJ_RANSOM.BOV, this new wave of ransomware displayed a notification page supposedly from the victim’s local police agency instead of the typical ransom.

During this period, different tactics were being used to spread ransomware. A case in 2012 involved a popular French confectionaryshop’s website that was compromised to serve TROJ_RANSOM.BOV. This watering hole tactic resulted in widespread infections in France and Japan, where the shop also had a significant fan-base. Instead of the usual ransom note, TROJ_RANSOM.BOV displayed a fake notice from the French police agency *Gendarmerie Nationale*.

The Rise of Reveton and Police Ransomware

Reveton is a ransomware type that impersonates law enforcement agencies. Known as Police Ransomware or Police Trojans, these malware are notable for showing a notification page purportedly from the victim’s local law enforcement agency, informing them that they were caught doing an illegal or malicious activity online.

To know which local enforcement agency is applicable to users, Reveton variants track the geographical location of their victims. Thus, affected users living in the US receive a notification from the FBI while those located in France are shown a notice from the *Gendarmerie Nationale*.

Reveton variants also employ a different payment method compared to early ransomware attacks. Once a system is infected with a Reveton variant, users are prompted to pay through *UKash*, *PaySafeCard*, or *MoneyPak*. These payment methods afford ransomware perpetrators anonymity, as both Ukash and PaySafeCard have a faint money trail.

In 2012, different types of Reveton variants were seen exhibiting new techniques. During the latter part of that year, Trend Micro reported on variants that played an audio recording using the victim's native language, and another one bearing a fake digital certificate.

Encrypting ransomware

Examples of extortionate ransomware became prominent in May 2005.[24] By mid-2006, Trojans such as Gpcode, TROJ.RANSOM.A, Archiveus, Krotten, Cryzip, and MayArchive began utilizing more sophisticated RSA encryption schemes, with ever-increasing key-sizes. Gpcode.AG, which was detected in June 2006, was encrypted with a 660-bit RSA public key.[25] In June 2008, a variant known as Gpcode.AK was detected. Using a 1024-bit RSA key, it was believed large enough to be computationally infeasible to break without a concerted distributed effort.

Encrypting ransomware returned to prominence in late 2013 with the propagation of CryptoLocker—using the Bitcoindigital currency platform to collect ransom money. In December 2013, *ZDNet* estimated based on Bitcoin transaction information that between 15 October and 18 December, the operators of CryptoLocker had procured about US$27 million from infected users. The CryptoLocker technique was widely copied in the months following, including CryptoLocker 2.0 (though not to be related to CryptoLocker), CryptoDefense (which initially contained a major design flaw that stored the private key on the infected system in a user-retrievable location, due to its use of Windows' built-in encryption APIs), and the August 2014 discovery of a Trojan specifically targeting network-attached storage devices produced by Synology. In January 2015, it was reported that ransomware-styled attacks have occurred against individual websites via hacking, and through ransomware designed to target Linux-based web servers.

Some ransomware strains have used proxies tied to Torhidden services to connect to their command and control servers, increasing the difficulty of tracing the exact location of the criminals. Furthermore. dark web vendors have increasingly started to offer the technology as a service.

Non-encrypting ransomware

In August 2010, Russian authorities arrested ten individuals connected to a ransomware Trojan known as WinLock. Unlike the previous Gpcode Trojan, WinLock did not use encryption. Instead, WinLock trivially restricted access to the system by displaying pornographic images, and asked users to send a premium-rate SMS (costing around US$10) to receive a code that could be used to unlock their machines. The scam hit numerous users across Russia and neighboring countries—reportedly earning the group over US$16 million.

In 2011, a ransomware Trojan surfaced that imitated the Windows Product Activation notice, and informed users that a system's Windows installation had to be re-activated due to "[being a] victim of fraud". An online activation option was offered (like the actual Windows activation process), but was unavailable, requiring the user to call one of six international numbers to input a 6-digit code. While the malware claimed that this call would be free, it was routed through a rogue operator in a country with high international phone rates, who placed the call on hold, causing the user to incur large internationallong distance charges.

In February 2013, a ransomware Trojan based on the Stamp.EKexploit kit surfaced; the malware was distributed via sites hosted on the project hosting services SourceForge and GitHub that claimed to offer "fake nude pics" of celebrities. In July 2013, an OS X-specific ransomware Trojan surfaced, which displays a web page that accuses the user of downloading pornography. Unlike its Windows-based counterparts, it does not block the entire computer, but simply exploits the behavior of the web browser itself to frustrate attempts to close the page through normal means.

In July 2013, a 21-year-old man from Virginia, whose computer coincidentally did contain pornographic photographs of underaged girls with whom he had conducted sexualized communications, turned himself in to police after receiving and being deceived by ransomware purporting to be an FBI message accusing him of possessing child pornography. An investigation discovered the incriminating files, and the man was charged with child sexual abuse and possession of child pornography.

Reveton

In 2012, a major ransomware Trojan known as Reveton began to spread. Based on the Citadel Trojan (which itself, is based on the Zeus Trojan), its payload displays a warning purportedly from a law enforcement agency claiming that the computer has been used for illegal activities, such as downloading unlicensed software or child pornography. Due to this behaviour, it is commonly referred to as the "Police Trojan". The warning informs the user that to unlock their system, they would have to pay a fine using a voucher from an anonymous prepaid cash service such as Ukash or Paysafecard. To increase the illusion that the computer is being tracked by law enforcement, the screen also displays the computer's IP address, while some versions display footage from a victim's webcam to give the illusion that the user is being recorded.

Reveton initially began spreading in various European countries in early 2012. Variants were localized with templates branded with the logos of different law enforcement organizations based on the user's country; for example, variants used in the United Kingdom contained the branding of organizations such as the Metropolitan Police Service and the Police National E-Crime Unit. Another version contained the logo of the royalty collection societyPRS for Music, which specifically accused the user of illegally downloading music. In a statement warning the public about the malware, the Metropolitan Police clarified that they would never lock a computer in such a way as part of an investigation.

In May 2012, Trend Micro threat researchers discovered templates for variations for the United States and Canada, suggesting that its authors may have been planning to target users in North America. By August 2012, a new variant of Reveton began to spread in the United States, claiming to require the payment of a $200 fine to the FBI using a MoneyPak card. In February 2013, a Russian citizen was arrested in Dubai by Spanish authorities for his connection to a crime ring that had been using Reveton; ten other individuals were arrested on money laundering charges. In August 2014, Avast Software reported that it had found new variants of Reveton that also distribute password stealing malware as part of its payload.

CryptoLocker

Encrypting ransomware reappeared in September 2013 with a Trojan known as *CryptoLocker*, which generated a 2048-bit RSA key pair and uploaded in turn to a command-and-control server, and used to encrypt files using a whitelist of specific file extensions. The malware threatened to delete the private key if a payment of Bitcoin or a pre-paid cash voucher was not made within 3 days of the infection. Due to the extremely large key size it uses, analysts and those affected by the Trojan considered CryptoLocker extremely difficult to repair. Even after the deadline passed, the private key could still be obtained using an online tool, but the price would increase to 10 BTC—which cost approximately US$2300 as of November 2013.

CryptoLocker was isolated by the seizure of the GameoverZeuSbotnet as part of Operation Tovar, as officially announced by the U.S. Department of Justice on 2 June 2014. The Department of Justice also publicly issued an indictment against the Russian hacker Evgeniy Bogachev for his alleged involvement in the botnet. It was estimated that at least US$3 million was extorted with the malware before the shutdown.

CryptoLocker.F and TorrentLocker

In September 2014, a wave of ransomware Trojans surfaced that first targeted users in Australia, under the names *CryptoWall* and *CryptoLocker* (which is, as with CryptoLocker 2.0, unrelated to the original CryptoLocker). The Trojans spread via fraudulent e-mails claiming to be failed parcel delivery notices from Australia Post; to evade detection by automatic e-mail scanners that follow all links on a page to scan for malware, this variant was designed to require users to visit a web page and enter a CAPTCHA code before the payload is actually downloaded, preventing such automated processes from being able to scan the payload. Symantec determined that these new variants, which it identified as *CryptoLocker.F*, were again, unrelated to the original CryptoLocker due to differences in their operation. A notable victim of the Trojans was the Australian Broadcasting Corporation; live programming on its television news channelABC News 24 was disrupted for half an hour and shifted to Melbourne studios due to a CryptoWall infection on computers at its Sydney studio.

Another Trojan in this wave, TorrentLocker, initially contained a design flaw comparable to CryptoDefense; it used the same keystream for every infected computer, making the encryption trivial to overcome. However, this flaw was later fixed.[31] By late-November 2014, it was estimated that over 9,000 users had been infected by TorrentLocker in Australia alone, trailing only Turkey with 11,700 infections.

CryptoWall

Another major ransomware Trojan targeting Windows, CryptoWall, first appeared in 2014. One strain of CryptoWall was distributed as part of a malvertising campaign on the Zedo ad network in late-September 2014 that targeted several major websites; the ads redirected to rogue websites that used browser plugin exploits to download the payload. A Barracuda Networks researcher also noted that the payload was signed with a digital signature in an effort to appear trustworthy to security software.[67]CryptoWall 3.0 used a payload written in JavaScript as part of an email attachment, which downloads executables disguised as JPG images. To further evade detection, the malware creates new instances of explorer.exe and svchost.exe to communicate with its servers. When encrypting files, the malware also deletes volume shadow copies, and installs spyware that steals passwords and Bitcoin wallets.

The FBI reported in June 2015 that nearly 1,000 victims had contacted the bureau's Internet Crime Complaint Center to report CryptoWall infections, and estimated losses of at least $18 million.

The most recent version, CryptoWall 4.0, enhanced its code to avoid antivirus detection, and encrypts not only the data in files but also the file names.

Mitigation

As with other forms of malware, security software might not detect a ransomware payload, or, especially in the case of encrypting payloads, only after encryption is underway or complete, particularly if a new version unknown to the protective software is distributed.[70] If an attack is suspected or detected in its early stages, it takes some time for encryption to take place; immediate removal of the malware (a relatively simple process) before it has completed would stop further damage to data, without salvaging any already lost.[71][72] Security experts have suggested precautionary measures for dealing with ransomware. Using software or other security policies to block known payloads from launching will help to prevent infection, but will not protect against all attacks. Keeping "offline" backups of data stored in locations inaccessible to the infected computer, such as external storage drives, prevents them from being accessed by the ransomware, thus accelerating data restoration.

The latest notable ransomware analyzed by Trend Micro:

Trend Micro Detection	Notable Features	Month-Year discovered
RANSOM_JOKOZY.A	• Employs RSA 2048 asymmetric encryption	06 2016
RANSOM_JSRAA.A	• Uses Jscript for relatively easy execution in Internet Explorer	06 2016
RANSOM_ZCRYPT.A	• Capable of spreading via USB • Runs on Windows 64-bit operating systems • Increases ransom when not paid during a certain time period	05 2016
RANSOM_TAKALOCKER.A	• Modifies SWIFT bank transactons in PDF format • Displays ransom note in Japanese	05 2016
RANSOM_WALTRIX.C	• Known as CryptXXX • A .DLL file that is capable of locking screens • Distributed by Angler Exploit Kit	05 2016
RANSOM_SHUJIN.A	• Baits Chinese users by using Chinese language in its ransom notes and interface • Deletes itself after execution	05 2016
RANSOM_JIGSAW.A	• Encrypts files on a set time interval if user delays payment • Deletes a larger amount of files with every hour while the amount to be paid also increases	04 2016
RANSOM_SURPRISE.A	• Spreads via TeamViewer, a remote access software • Appends .surprise to encrypted files	03 2016
RANSOM_MAKTUB.A	• Notable for its use of unique graphic designs for its ransom notes	03 2016

RANSOM_KERANGER.A	• Passed off as a legitimate upgrade installer of a known bittorent client • First ransomware to exclusively target OSX machines	

Family Name	Aliases	Description
ACCDFISA	Anti Cyber Crime Department of Federal Internet Security Agency Ransom	First spotted early 2012; Encrypts files into a password-protected; Cybercriminals behind this ransomware asks payment thru *Moneypak*, *Paysafe*, or *Ukash* to restore the files and unlock the screen; Known as a multi-component malware packaged as a self-extracting (SFX) archive; May come bundled with third party applications such as *Sdelete* and *WinRAR*
ANDROIDOS_LOCKER		First mobile ransomware spotted; Uses Tor, a legitimate service that allows anonymous server connections; Users with mobile devices affected by this malware may find the files stored in their mobile device rendered useless and held for ransom
CRIBIT	BitCrypt	Similar to CRILOCK with its use of RSA-AES encryption for target files; Version 1 uses RSA-426; Version 2 uses RSA-1024; Appends the string *bitcryp1* (for version 1) and *bitcrypt2* (for version 2) to the extension name of the files it encrypts
CRILOCK	CryptoLocker	Employs Domain Generation Algorithm (DGA) for its C&C server connection; October 2013 - UPATRE was found to be the part of the spam mail that downloads ZBOT, which further downloads CRILOCK
CRITOLOCK	Cryptographic locker	Uses advanced encryption standard (AES-128) cryptosystem; The word *Cryptolocker* is written in the wallpaper it uses to change an affected computer's wallpaper
CRYPAURA	PayCrypt	Encrypts files and appends the corresponding email address contact for file decryption; PayCrypt version appends .id-{victim ID}-paycrypt@aol.com to files it encrypts
CRYPCTB	Critroni, CTB Locker, Curve-Tor-Bitcoin Locker	Encrypts data files; Ensures there is no recovery of encrypted files by deleting its shadow copies; Arrives via spam mail that contains an attachment, actually a downloader of this ransomware; Uses social engineering to lure users to open the attachment; Uses Tor to mask its C&C communications
CRYPDEF	CryptoDefense	To decrypt files, it asks users to pay ransom money in bitcoin currency

CRYPTCOIN	CoinVault	Encrypts files and demands users to pay in bitcoin to decrypt files; Offers a one-time free test to decrypt one file
CRYPTFILE		Uses unique public key generated RSA-2048 for file encryption and also asks users to pay 1 bitcoin to obtain private key for decrypting the files
CRYPWALL	CryptoWall, CryptWall, CryptoWall 3.0, Cryptowall 4.0	Reported to be the updated version of CRYPTODEFENSE; Uses bitcoin currency as mode of payment; Uses Tor network for anonymity purposes; Arrives via spam mail, following UPATRE-ZBOT-RANSOM infection chain; CryptoWall 3.0 comes bundled with FAREIT spyware; Cryptowall 4.0 encrypts file name of files it encrypts and follows an updated ransom note, it also comes from spam as a JavaScript attachment, and may be downloaded by TROJ_KASIDET variants
CRYPTROLF		Shows troll face image after file encryption
CRYPTTOR		Changes the wallpaper to picture of walls and asks users to pay the ransom
CRYPTOR	batch file ransomware	Arrives thru DOWNCRYPT; A batch file ransomware capable of encrypting user files using GNU Privacy Guard application
DOWNCRYPT	batch file ransomware	Arrives via spam email; Downloads BAT_CRYPTOR and its components such as a decoy document
VIRLOCK	VirLock, VirRansom	Infects document files, archives, and media files such as images
PGPCODER		Discovered in 2005; first ransomware seen
KOLLAH		One of the first ransomware that encrypts files using certain extension names; Target files include Microsoft Office documents, PDF files, and other files deemed information-rich and relevant to most users; Adds the string *GLAMOUR* to files it encrypts
KOVTER		Payload of the attack related to YouTube ads that lead to the Sweet Orange exploit kit
MATSNU		Backdoor that has screen locking capabilities; Asks for ransom
RANSOM		Generic detection for applications that restrict the users from fully accessing the system or encrypts some files and demands a *ransom* in order to decrypt or unlock the infected machine
REVETON	Police Ransom	Locks screen using a bogus display that warns the user that they have violated federal law; Message further declares the user's IP address has been identified by the Federal Bureau of Investigation (FBI) as visiting websites that feature

		illegal content
VBUZKY		64-bit ransomware; Attempts to use *Shell_TrayWnd*injection; Enables TESTSIGNING option of Windows 7
CRYPTOP	Ransomware archiver	Downloads GULCRYPT and its components
GULCRYPT	Ransomware archiver	Archives files with specific extensions; Leaves a ransom text file containing the instructions on who to contact and how to unpack the archives containing user's files
CRYPWEB	PHP ransomware	Encrypts the databases in the web server making the website unavailable; Uses HTTPS to communicate with the C&C server; Decrypt key is only available in the C&C server
CRYPDIRT	Dirty Decrypt	First seen in 2013 before the emergence of Cryptolocker
CRYPTORBIT		Detection for images, text, and HTML files which contain ransom notes that are indicators of compromised (IOC)
CRYPTLOCK	TorrentLocker	Poses as CryptoLocker; newer variants display*crypt0l0cker* on the affected computer; uses a list of file extensions that it avoids encrypting, compared to usual ransomware that uses a list of file extensions to encrypt - this allows CRYPTLOCK to encrypt more files while making sure the affected computer still runs, ensuring users know that their files are encrypted and access to the Internet to pay the ransom is still present
CRYPFORT	CryptoFortress	Mimics TorrentLocker/CRYPTLOCK user interface; Uses wildcards to search for file extensions; encrypts files in shared folders
CRYPTESLA	TeslaCrypt	User interface is similar to CryptoLocker; encrypts game-related files; Versions 2.1 and 2.2 appends encrypted files with .vvv and .ccc; Version 3.0 has an improved encryption algorithm and appends .xxx, .ttt, and .mp3 to files it encrypts
CRYPVAULT	VaultCrypt	Uses GnuPG encryption tool; downloads hacking tool to steal credentials stored in web browsers; uses sDelete 16 times to prevent/hinder recovery of files; has a customer support portal; is a batch script crypto-ransomware
CRYPSHED	Troldesh	First seen in Russia; added English translation to its ransom note to target other countries; aside from appending .xtbl to the file name of the encrypted files, it also encodes the file name, causing affected users to lose track of what files are lost
SYNOLOCK	SynoLocker	Exploits Synology NAS devices' operating system (DSM

		4.3-3810 or earlier) to encrypt files stored in that device; has a customer support portal
KRYPTOVOR	Kriptovor	Part of a multi-component infection; aside from its crypto-ransomware component, it has an information stealing component that steals certain files, processes list, and captures desktop screenshot; uses an open source Delphi library called *LockBox 3* to encrypt files
CRYPFINI	CryptInfinite, DecryptorMax	Arrives via spam with macro attachment, the spam mail usually pretends to be a job application linked to a Craigslist post; Appends .crinf files
CRYPFIRAGO		Uses Bitmessage for communication with its creators; Appends .1999 or .bleep to files it encrypts
CRYPRADAM	Radamant	May arrive via exploit kits; Appends .rdm to files it encrypts
CRYPTRITU	Ransom32	Known as the JavaScript ransomware
CRYPBOSS	CrypBoss	Appends .crypt to files it encrypts
CRYPZUQUIT	Zuquitache, Fakben	Known as the ransomware-as-a-service (RaaS) malware
CRYPDAP	PadCrypt	Has live chat support for affected users; Arrives via spam
CRYPHYDRA	HydraCrypt	Based on leaked source code of CrypBoss; Arrives via spam
LOCKY	Locky	Renames encrypted files to hex values; Appends .locky to files it encrypts; Arrives via spam with macro-embedded .DOC attachment, similar to the arrival of DRIDEX malware
CERBER	Cerber	Encrypts the file name and appends it with .cerber; Drops a .VBS file that makes the computer speak to the victim
CRYPSAM	SAMSAM	Uses exploits on JexBoss open source server application and other Java-based application platforms to install itself in targeted Web application servers
PETYA	Petya	Causes blue screen and displays its ransom note at system startup
WALTRIX	CRYPTXXX, WALTRIX, Exxroute	Arrives as a .DLL file; Distributed by the Angler Exploit Kit; Locks screens and encrypts all files; Appends the extension .crypt
CRYPSALAM	Salam	Encrypts files and drops a ransom note formatted as {month}-{day}-{year}-INFECTION.TXT; Asks the users to contact the ransomware creator via email to decrypt the files

Anti-Ransomware Tools and Solutions

Trend Micro offers free tools such as the Trend Micro Lock Screen Ransomware Tool, which is designed to detect and remove screen-locker ransomware. The Trend Micro Crypto-Ransomware File Decryptor Tool can decrypt files locked by certain variants of crypto-ransomware without paying the ransom or the use of the decryption key.

Research Objectives and Approach

The main objective of the research is to find the better solution to the problem by avoiding the attacker not to attack the system.

There are Anti-Ransomware tools but these may or may not decrypt the files.This tools also take more time to decrypt because the attacker uses 1024 bit RSA algorithm to encrypt the system files.

The main approach of this research is to study about the attacker carefully how he is going to attack the system though we are having soo many security layers in the transmission system.

Then how he is going to attack each and every layer of the network system so that we can stop him by making more strong and secure layers.

If the attacker even attacks the system by attacking each and every layer, we will find one method in which he cannot encrypt the system files.

Then we select one security algorithm in such a way that the data stored on the system will be in the form of encrypted data and when attacker tries to encrypt it further cannot be possible.

Usefullness of Research:

“Prevention is better than cure” ,This solution will avoid the hackers to attack the system because the previous solutions are only after the attacker attack the system but not before that.To protect the system from any type of hacking is the main goal of this research.

Work Plan:

1. The first step is to study about the ransomware in depth.
2. Then identifying how he is going to attack each and every layer of transmission system.
3. Which algorithm is used by him and what is the key size.
4. Analyzing on which criteria he is choosing the systems to attack.
5. Protecting each and every layer of the network system , by using secure socket layer.
6. Inorder to transmit the data also we can also make use of https rather than http protocol.
7. After this also we can make the operating system in such a way that no one can access the files of it.
8. Atlast we implement this method which is very strong enough to protect the system.

III. Conclusion:

Ransomware is one of the cyber security threat which will attack the system by either encrypting or blocking the system and demanding the user some money to decrypt it.The solution is to find method which will not make the attacker to attack the system , by making the operating system soo strong and secured by using security algorithms.

References:

[1] *Mehmood, Shafqat (3 May 2016).* "Enterprise Survival Guide for Ransomware Attacks".*SANS Information Security Training | Cyber Certifications | Research. www.sans.org*. Retrieved 3 May 2016.

[2] *Dunn, John E.* "Ransom Trojans spreading beyond Russian heartland". *TechWorld*. Retrieved 10 March 2012.

[3] "New Internet scam: Ransomware...". *FBI. 9 August 2012.*

[4] "Citadel malware continues to deliver Reveton ransomware...". *Internet Crime Complaint Center (IC3). 30 November 2012.*

[5] "Update: McAfee: Cyber criminals using Android malware and ransomware the most".*InfoWorld*. Retrieved 16 September 2013.

[6] "Cryptolocker victims to get files back for free". *BBC News. 6 August 2014*. Retrieved 18 August 2014.

[7] "FBI says crypto ransomware has raked in >$18 million for cybercriminals". *Ars Technica*. Retrieved 25 June 2015.

[8] "Ransomware squeezes users with bogus Windows activation demand". *Computerworld*. Retrieved 9 March 2012.

[9] "Police warn of extortion messages sent in their name". HelsinginSanomat. Retrieved 9 March 2012.

[10] *McMillian, Robert.* "Alleged Ransomware Gang Investigated by Moscow Police". *PC World*. Retrieved 10 March 2012.

[11] "Ransomware: Fake Federal German Police (BKA) notice". *SecureList (Kaspersky Lab)*. Retrieved 10 March 2012.

[12] "And Now, an MBR Ransomware". *SecureList (Kaspersky Lab)*. Retrieved 10 March2012.

[13] *Young, A.; M. Yung (1996). Cryptovirology: extortion-based security threats and countermeasures. IEEE Symposium on Security and Privacy. pp. 129–140.*doi:10.1109/SECPRI.1996.502676. ISBN 0-8186-7417-2.