Ransomware: A Cyber Extortion

Miss. Harshada U. Salvi
Department of MCA,
Finolex Academy of Management & Technology
Ratnagiri, Maharashtra
salvi_harshada@yahoo.com

Mr. Ravindra V. Kerkar
Department of MCA,
Finolex Academy of Management & Technology
Ratnagiri, Maharashtra
ravindra.kerkar09@gmail.com

***Abstract*—**

Life as we know it today would be hampered without computers. They controls just about everything from basic communication, finances and even medical science. As internet technologies are advancing more rapidly, more businesses and individuals are storing sensitive data electronically. Internet has become the hunting ground for criminals to make profit, cause disturbance and bring down organizations and governments. Ransomware is the latest trend that criminals are using for extorting cash from the victims. It is malware that denies you access to your system until you pay ransom.

Keywords*— *Ransomware, Extortion, Malware, Bitcoins, Cryptovirus, Cryptotrojan, Cryptoworm, CryptoLocker, WinLocker, Cryptoviral extortion

I. INTRODUCTION

Big enterprises like Microsoft, Google are designing and building software products that can easily save your files to online storage and users can get to them from any device, like PC, tablet, or phone. Ransomware is malware that keeps you from utilizing your documents or your PC or online storage by locking them up in unbreakable encryption, and after that demands a ransom of $300 to $500 in bitcoins from you in return for a guarantee to open them. It spreads through e-mail attachments, infected programs and websites. A ransomware may also be called a cryptotrojan, cryptovirus or cryptoworm.

Commonly seen ransomware categories are:

- Encrypts personal files/folders – Once the files are encrypted, they are deleted from the folder and generally a text file containing instructions for payment is left behind in the same folder. This type of ransomware is called 'file encryptor'. For example, CryptoLocker.

- 'Locks' the screen – It displays a full screen image that blocks all other windows and demands payment. Personal files are not encrypted. This type of ransomware is called 'WinLocker'.

- “MBR ransomware” – An area in the computer's hard drive that permits the operating system to boot up is called the Master Boot Record (MBR). MBR ransomware changes the computer's MBR which interferes with the ordinary boot procedure. It displays ransom demand on screen [1].

II. BACKGROUND

The first ever recognized ransomware was the "AIDS (Aids Info Desk) Trojan” released in 1989. It is also known as "PC Cyborg Trojan". It was written by Dr. Joseph Popp. It replaced the AUTOEXEC.BAT file and it would then count the number of times the machine had booted. Once this boot count reaches 90, it would then hide directories and encrypt the names of all the files on the C: drive and make the system unusable. To regain access, the user would have to send $189 to PC Cyborg Corp. at a post office box in Panama. Popp was declared mentally unfit to stand trial for his actions [2][3].

In 1996, Adam L. Young and Moti Yung found the fatal weakness in “AIDS" Trojan. They introduced idea of using public key cryptography for such attacks. This attack was referred to as being "cryptoviral extortion". A cryptotrojan, cryptovirus or cryptoworm hybrid encrypts the victim’s files using the public key of the ransomware author and the victim has to pay to obtain the needed session key. This is one of many attacks, both overt and covert in the field known as Cryptovirology [4].

With the Internet making it easier to carry through Popp’s ransom idea, cyber criminals began to realize that they could make a profit from ransomware on a far wider scale. In 2006, criminal organizations began using more effective asymmetric RSA encryption. Trojans such as Archiveus, Gpcode, TROJ.RANSOM.A, Krotten, MayArchive and Cryzip began utilizing more sophisticated RSA encryption schemes, with ever-increasing key-sizes [5].

A brief rundown of various ransomwares that you should know [6]:

- The Archiveus Trojan - It encrypted everything in the My Documents directory and victims are required to purchase items from an online pharmacy to obtain the 30-digit password.

- The GPcode – It is an encryption Trojan, which initially spread via an email attachment professing to be a job application, used a 660-bit RSA public key. Two years later, a variant GPcode.AK using a 1024-bit RSA key was released.

- CryptoLocker – The first versions was posted in September 2013. It usually enters the company by email. If a user clicks on the executable, it immediately starts to scan network drives, renames all the files & folders and encrypts them.

- Locker – The first copycat software emerged in December 2013. Users had to pay $150 to get the key, with money being sent to a Perfect Money or QIWI Visa Virtual Card number.

- CryptoLocker 2.0 – A new and improved version of CryptoLocker was found in December 2013. It was written using C# while the original was in C++. Tor Tor network was used for anonymity and payment methods like Bitcoin were used for extortion. It used 2048-bit encryption. This latest variant is not detected by anti-virus or firewall.

- CryptorBit – A new ransomware was discovered in December 2013. CryptorBit corrupts the first 1024 bytes of any data file it finds. It can bypass Group Policy settings put in place to defend against this type of ransomware infection. It uses social engineering to get end users to install the ransomware using a fake flash update or a rogue antivirus product. It uses Tor and Bitcoin for a ransom payment. It also installs crypto-coin mining software that uses the victim's computer to mine digital currency.

- CTB-Locker (Curve-Tor-Bitcoin Locker) – It was discovered in midsummer 2014. First infections were mainly found in Russia. The developers were thought to be from an eastern European country.

- SynoLocker – It appeared in August 2014. This ransomware attacked Synology NAS devices. It encrypts files one by one. Payment was demanded in Bitcoins and Tor was used for anonymity.

- CryptoWall – It was rebranded from CryptoDefense in April 2014. It exploited Java vulnerability. Malicious advertisements on domains belonging to Disney, Facebook, The Guardian newspaper and many others led people to sites that were CryptoWall infected and encrypted their drives. According to an August 27 report from Dell SecureWorks Counter Threat Unit (CTU): "CTU researchers consider CryptoWall to be the largest and most destructive ransomware threat on the Internet as of this publication, and they expect this threat to continue growing." More than 600,000 systems were infected between mid-March and August 24, with 5.25 billion files being encrypted. 1,683 victims (0.27%) paid a total $1,101,900 in ransom. Nearly 2/3 paid $500, but the amounts ranged from $200 to $10,000.13

- Cryptoblocker – A new ransomware variant emerged in July 2014. It only encrypts the files whose size is less than 100MB and will skip anything in Windows or Program Files. It uses AES rather than RSA encryption.

- OphionLocker – A new ransomware was released in December 2014. It used ECC (Elliptic Curve Cryptography) public-key encryption. If the ransom was not paid within three days, the private key would be deleted.

- Pclock - It was released in January 2015 by imitating CryptoLocker. It encrypts files in a user's profile. It deletes and disables volume shadow copies. It would then set 72-hour countdown timer to pay 1 bitcoin in ransom.

- CryptoWall 2.0 – A new version of CrptoWall ransomware was released in January 2015. It is delivered by means of email attachments, malicious pdf files and various exploit kits. It encrypts the user's data, until a ransom is paid for the decryption key. It uses TOR to conceal the C&C (Command & Control) channel. It incorporates anti-vm and anti-emulation checks to deter identification via sandboxes. It has the ability to run 64-bit code directly from its 32-bit dropper and switch the processor execution context from 32 bit to 64 bit.

- TeslaCrypt – A new CryptoWall variant emerged in February 2015. It targets game files of popular games such as Call of Duty, MineCraft, World of Warcraft, and Steam.

- VaultCrypt – It was released in February 2015. Since then it has been circulated in Russia. It pretended to be customer support. It uses Windows batch files and open source GnuPG privacy software for effective file encryption.

- CryptoWall 3.0 – A new version of CryptoWall was released in March 2015. It uses I2P (Invisible Internet Project) for anonymity. It gains access to privilege escalation on the system by using exploits and disables many security features on a target system.

- CryptoWall 4.0 – A new variant of CryptoWall was unleashed in September 2015. The most important difference between CryptoWall 3.0 and 4.0 is that it re-encrypts filenames of the encrypted files. It becomes more difficult to decrypt the files that need to be recovered.

- LowLevel04 – It is a file-encrypting ransomware that was unleashed in October 2015. It is also known as the Onion Trojan-Ransom. It spreads via with Remote Desktop or Terminal Services by using brute force attacks on machines. The files are encrypted using AES encryption scheme and the encryption key itself is encrypted using RSA algorithm.

- Chimera – It was released in November 2015. The hacker threatens to publish the encrypted files on the Internet if the ransom is not paid.

III. HOW IT WORKS?

PROPAGATION

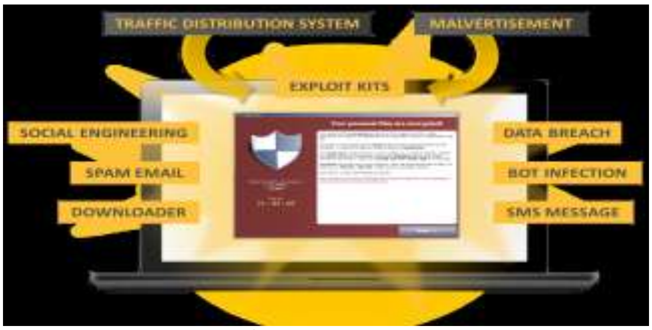


Figure 1 [7]:- Routes for ransomware to arrive on a computer.

The different techniques or services used by ransomware attackers to get their malware onto a victim's computer are as follows [7].

TRAFFIC DISTRIBUTION SYSTEM (TDS)

Attacker buy redirected web traffic from a TDS (Traffic Distribution Service) vendor and direct it to a site hosting an exploit kit. In many cases, the redirected traffic originates from adult content-related websites. If the exploit kit successfully exploits vulnerability in the visiting victims' computer, it leads to the drive-by-download of malware.

MALVERTISEMENT

Malicious advertisements known as malvertisments are pushed onto legitimate websites in order to redirect traffic to malicious website. Click-fraud malware infection, whereby clicking on the malvertisment can also lead to a ransomware infection. By using real-time bidding to purchase traffic or ad space of interest cybercriminals can geographically target victims and operate without borders.

SPAM EMAIL

The spam, a form of an email containing a malicious attachment or a link in the email can lead to a site hosting an exploit kit. The spam may also involve the download of malware through other social-engineering means. The spam emails uses various social engineering and psychological levers to trick user.

The spam emails used to distribute ransomware can have the following themes:
- Mail delivery notification
- Energy bills
- Job seeker resume
- Tax returns and invoices
- Police traffic offense notifications

DOWNLOADERS & BOTNETS

One of the ways to distribute malware is known as downloaders. Once the downloader infects a computer, it downloads secondary malware onto the infected system. The cybercriminals behind downloaders offer a malware-installation service onto already infected computers, at a cost.

Trojan botnets can also download ransomware onto computers they have infected.

SOCIAL ENGINEERING AND SELF-PROPAGATION

Some ransomware also has the functionality to spread. For example, there are some samples on Android that lock the device or encrypt files along with employing worm-like capabilities. They spread to all contacts within the device's address book by sending social-engineering SMS messages.

A ransomware attack goes through five stages: Installation, Contacting headquarters, handshake and keys, encryption, extortion. The five stages are explained as follows [8].

STAGE 1: INSTALLATION

Once a victim's computer is infected, the crypto-ransomware installs itself. It then sets keys in the Windows Registry. So that it starts automatically every time your computer boots up.

STAGE 2: CONTACTING HEADQUARTERS

Before starting to attack your system, it contacts a server operated by the cybercriminals that owns it.

STAGE 3: HANDSHAKE AND KEYS

The ransomware client and server authenticate each other using process called as "handshake". The server then generates two cryptographic keys. One key is kept on victim's computer and the second key is stored on the criminals' server.

STAGE 4: ENCRYPTION

Once the cryptographic keys are established, the ransomware on your computer starts encrypting every file that it finds.

STAGE 5: EXTORTION

The ransomware displays a screen displaying a time limit to pay ransom before the criminals destroy the key to decrypt your files. A typical ransom amount ranges from $300 to $500. It must be paid in Bitcoins or other electronic payments which are untraceble.

IV. RISE OF RANSOMWARE

Today, the ransomware threat has become a global pandemic touching all corners of the world. Even though it is a global problem, certain countries tend to be affected more than others. According to Symantec's report [7], the following countries are most affected by ransomware - USA, Japan, UK, Italy, Germany, Russia, Canada, Australia, India, Netherlands, Brazil, and Turkey.

These countries represent industrialized and developing economies that roughly make up 85 percent of the world's global domestic product (GDP).

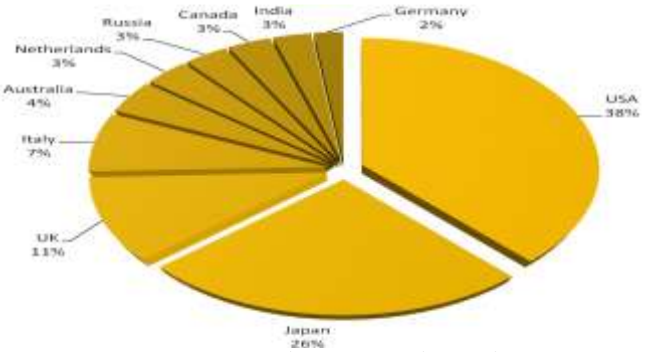


Figure 2 [7]:- Top 10 countries for detections of binary file based crypto ransomware

India is the ninth most affected region in the world by ransomware. India is the third-highest country to report ransomware attacks in Asia with over 60,000 attacks last year. According to Symantec press release, “In India, a staggering 86 percent of all ransomwares was crypto-ransomware posing a threat to consumers and enterprises alike” [9].

Cybercriminals are using ransomware to turn extortion into a profitable venture. They attack big and small targets alike. Ransomware attacks grew 113 percent in 2014, driven by a more than 4,000 percent increase in crypto-ransomware attacks [10].

Two businessmen from Agra were targeted in the first half of 2015, from whom the criminals demanded ransom more than $10,000 to get their machines back [11]. In November 2015, East Delhi-based businessman could not access 500 GB of his company's data and personal files stored on his laptop till he pays ransom of $500 to an unidentified hacker [12].

Recently, the attackers targeted the Indian companies by initially compromising the IT administrators’ computers. They infected the systems using the Le Chiffre ransomware. It is a strain of malware that encrypts targeted files and changes their extensions. It encrypts data and servers with 256-bit public key cryptography. Extortionist keeps the private key in his possession. All targets were infected as soon as the IT administrator opened a faux email disguised as correspondence from senior management. It contained the ransomware which then spread to other computers in the banks’ and company’s network. The ransomware affected thousands of computers at the banks and the pharmaceutical company. The extortionists demanded a bitcoin each for the every decryption key required recover the encrypted computer [13].

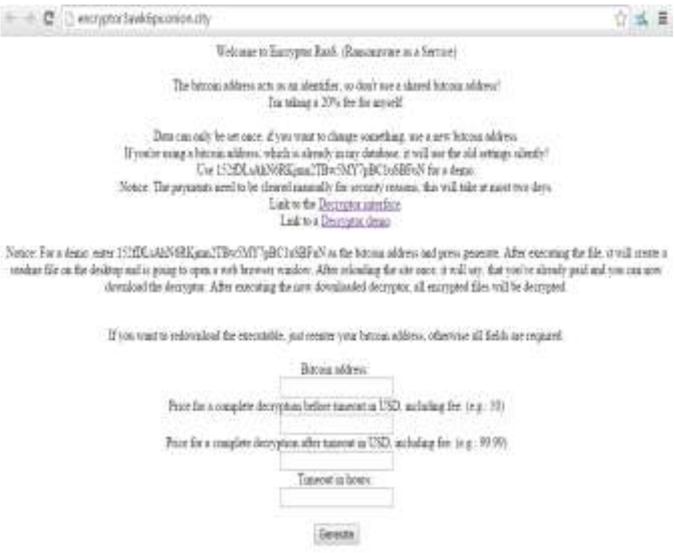
The next most targeted types of devices are tablets and mobile phones. These devices have become ubiquitous worldwide. The studies [14], show that users are spending more time on mobile devices than ever before. Android is a much more open and permissive platform. To take advantage of this growing and potentially profitable user base, ransomware targeting Android devices has already been created. Android.Fakedefender, discovered in June 2013, marked the shift from the standard fake antivirus scam to locker ransomware on the Android platform. Android.Fakedefender professed to be a security scanner but the device interface was locked down to prevent victims from launching other apps or change settings in the operating system.

In 2014, we additionally saw the rise of crypto ransomware for Android devices in the form of Android.Simplocker.

In 2015 new Android ransom-lockers known as *Android/Lockerpin.A* was unleashed by Cyber criminals. Once it infects the system, users cannot regain access to their device without root privileges or without some other security management solution installed, apart from a factory reset which would also delete all their data. Moreover, this ransomware also uses a vicious trick to obtain and maintain device administrator privileges so as to prevent un-installation [15].

Ransomware attacks, both desktop and mobile, have become some of the most determined and damaging scams on the Internet. Researchers at software firm Symantec have revealed a new type of Android ransomware called Android.Lockdroid.E. It imitates the lockscreen user interface to deceive users. It displays a lockscreen with a legal notice that demanded payment of a US$500 fine for accessing “forbidden pornographic sites” and then locked the device while displaying the notice [7].

Cybercriminals have now started to provide services to those who wish to carry out ransomware attacks, by effectively providing ransomware-as-a-service (RaaS). It is designed to be so user-friendly that it could be deployed by anyone with little cyber know-how. The idea is to hire hackers with already operational botnets and campaigns to use the website “Ransomware as a Service”. They would then use that website to create encrypting ransomware binaries to their specifications and then pay 20% of their successful scams to the Encryptor RaaS author. All that hackers have to do is to input the bitcoin wallet address they want the funds to go to. They can modify the price they want for immediate payment, late payment, and finally a timer for what is considered a late payment [16].



Welcome to Encryptor RaaS. (Ransomware as a Service)

The bitcoin address acts as an identifier, so don't use a shared bitcoin address!
I'm taking a 20% fee for myself!

Data can only be set once, if you want to change something, use a new bitcoin address.
If you're using a bitcoin address, which is already in my database, it will use the old settings silently!
Use 152fDLxAhN6RKgma2TBw5MY7pBC1o5BFoN for a demo.
Notice: The payments need to be cleared manually for security reasons, this will take at most two days.
Link to the Decryptor interface
Link to a Decryptor demo

Notice: For a demo, enter 152fDLxAhN6RKgma2TBw5MY7pBC1o5BFoN as the bitcoin address and press generate. After executing the file, it will create a readme file on the desktop and is going to open a web browser window. After reloading the site once, it will say, that you've already paid and you can now download the decryptor. After executing the new downloaded decryptor, all encrypted files will be decrypted.

If you want to redownload the executable, just reenter your bitcoin address, otherwise all fields are required.

Bitcoin address:

Price for a complete decryption before timeout in USD, including fee: (e.g.: 33)

Price for a complete decryption after timeout in USD, including fee: (e.g.: 99.99)

Timeout in hours:

Figure 3 [16]. Encryptor RaaS webpage.

Advancements in the internet technologies and its diversity in the world are the sources of cyber crimes. The increasing use of digital devices like smart phones, tablets, laptops and mobile for online transactions has also increased the vulnerabilities to a great extent. The Internet crimes are committed in diverse fashion and one of the growing cyber-crime is ransomware.

V. STAYING SAFE

Following tips can be used to stay protected from ransomware [8].

- Restrict write permissions on file servers as much as possible.
- Use antivirus to block access to malicious websites and scan all downloads.
- Use advanced endpoint protection that can identify new malware types and detect malicious data.
- Contact concerned authority about suspicious pop-ups.
- Take regular offline backups; test backups to ensure data recoverability.
- Disconnect from networks instantly if you suspect infection.
- Avoid letting websites remember your password.
- Install and enable a firewall.
- Keep Windows / the Operating System up to date.
- Verify the authenticity of the source

VI. FUTURE OF RANSOMWARE

With the expanding spread of Internet of Things (IoT) and connected gadgets like wearable computers, ransomware may be on the threshold of another evolutionary jump forward. As of now we have smart TVs, smart watches, smart locks, smart clothing, smart fridges and internet-enabled cars. This list continues to grow by the day. Cybercriminals could then potentially takeover these devices and held them to ransom [7].

In the wearable market, the smart watch category is gathering momentum. Ransomware can be installed in smart watches by tricking the users using an email or instant messaging notification with a link to download a new app.

"Digital India", a flagship programme of Government of India has garnered the maximum attention of IT sector. The vision of Digital India programme is to transform India into a digitally empowered society and knowledge economy [17]. But this programme has also drawn attention of cybercriminals. Indian firms are going to be targeted by malware-authors frequently.

It is never easy to anticipate the way the ransomware scene will advance in the future. We can study the patterns of the past and try to guess about what might happen in the future. The concept of ransomware has reached a high level of maturity now. Given nature of these threats and the emergence of many new ransomware families, it is dubious that ransomware-type scams will decline anytime soon, with future growth being more likely.

VII. CONCLUSION

In this paper we have looked at the origins, history and evolution of Ransomware. It has become a lucrative business for cybercriminals. The majority of the countries that make up the G20 group are hit by ransomware. Technological trends such as IoT and the growth in the wearable market allow cybercriminals to target new areas with ransomware. It has shown that attention to security is supreme concern for all. Fighting ransomware is a challenging and we all have a role to play in it. While designing, creating new technology or products, considering the normal use cases is not enough anymore. The major challenge for product designers is to improve security and take malicious operations and scenarios into consideration. We need to practice basic security practices to protect our data, such as avoiding clicking malicious links or attachments and patching exploitable software vulnerabilities. We need to gain knowledge about the threat of ransomware and accordingly take steps to prepare for and minimize hazard from these ransomware attacks.

REFERENCES

[1] Sophos.com, "Information on malware known as Ransomware", 2015. [Online]. Available: https://www.sophos.com/en-us/support/knowledgebase/119006.aspx.

[2]J. Bates, "Trojan Horse: AIDS Information Introductory Diskette Version 2.0", Virus Bulletin Ltd, England., 1990.

[3]M. Kassner, "Ransomware: Extortion via the Internet - TechRepublic", *TechRepublic*, 2010. [Online]. Available: http://www.techrepublic.com/blog/it-security/ransomware-extortion-via-the-internet/.

[4]A. Young and M. Yung, "Cryptovirology: extortion-based security threats and countermeasures", in *IEEE Symposium on Security and Privacy*, Oakland, CA, 1996, pp. 129 - 140.

[5]J. Leyden, "Ransomware getting harder to break", *Theregister.co.uk*, 2006. [Online]. Available: http://www.theregister.co.uk/2006/07/24/ransomware/.

[6]K. Laffan, "A Brief History of Ransomware", *Varonis: The Inside Out Security Blog*, 2015.

[7]K. Savage, P. Coogan and H. Lau, "The evolution of ransomware", Symantec Security Response Publications, 2015.

[8]J. Zorabedian, "Anatomy of a ransomware attack: CryptoLocker, CryptoWall, and how to stay safe (Infographic)", *Sophos*, 2015.

[9] Symantec, "Rise in Targeted Attacks Aimed At Indian Businesses Dealing With Critical Infrastructure", 2015.

[10]"Internet Security Threat Report, Volume 20", Security Response Publications, 2015.

[11]A. Chauhan, "Notorious computer virus attacks users' files", *The Times of India*, 2016.

[12]S. Shekhar, "Delhi businessman hacked, asked to pay $500", *Mail Today*, 2015.

[13]S. Das, "Indian Banks & Big Industry Targeted in Ransomware Racket Demanding Bitcoin - CCN: Financial Bitcoin & Cryptocurrency News", *CCN: Financial Bitcoin & Cryptocurrency News*, 2016. [Online]. Available: https://www.cryptocoinsnews.com/indian-banks-big-industry-targeted-in-ransomware-racket-demanding-bitcoin/.

[14]"Mobile Internet - Statistics & Facts", 2015. [Online]. Available: http://www.statista.com/topics/779/mobile-internet/.

[15]L. Stefanko, "Aggressive Android ransomware spreading in the USA", *Welivesecurity.com*, 2016. [Online]. Available:http://www.welivesecurity.com/2015/09/10/aggressive-android-ransomware-spreading-in-the-usa/.

[16]R. Dela Paz, "Encryptor RaaS: Yet another new Ransomware-as-a-Service on the Block", *Fortinet Blog*, 2015.

[17] Digitalindia.gov.in, "Vision and Vision Areas | Digital India Programme". [Online]. Available: http://www.digitalindia.gov.in/content/vision-and-vision-areas.