Ransomware: A Growing Jeopardy

Shilpa Narula[1] and Anam Afaq[2]

Abstract

In today's technology surrounded world where computer users are increasing at a rapid rate, cybercriminals are also increasing to conduct pernicious activities. In the computer world, on one side, advanced encryption algorithms, can be utilized to protect valuable information. On the other side, they can also be used by the cybercriminals for extortion on a very large scale. Ransomware is an emerging cyber hijacking threat using such encryption technology for extortion. Ransomware locks your system or device and holds your system/device for ransom. The present research paper discusses ransomware extortion scheme, its evolution, factors driving its growth, different types and preventive measures that can be taken.

Keywords: *Bitcoin, CryptoLocker, Cybercrime, Encryption, Ransomware*

Introduction

Ransomware is a type of malicious software which, when run, disables the functionality of a computer in some way. The Ransomware either locks the computer to prevent normal usage or prevent access to the documents and files stored on it by encrypting them. Finally, the people behind this crime demand payment by displaying a message on the computer screen so as to restore functionality of the system. This malware, in effect, is done so as to demand the computer ransom. In other words, ransomware is an extortion racket [1]. They differ from other types of malware as their effects are reversible only via the cryptographic keys held by a remote adversary. The ransom demand is displayed, usually either via a text file or as a webpage in the web browser [18].

Ransomware has evolved over time and users may encounter it in a variety of ways. Innocent users can be a victim of ransomware by visiting malicious or compromised websites. It may arrive as either downloaded payload by other malware or it may arrive as different forms of attachments to a

[1] **Assistant Professor, Asian Business School, Asian Education Group,Plot A-2,Sector-125, Noida. Email: shilpanarula04@gmail.com**

[2] **Assistant Professor, Asian Business School, Asian Education Group,Plot A-2,Sector-125, Noida. Email: anam24afaq@gmail.com**

spammed email. Cybercriminals keep on changing their way of trapping the users. Ransomware attacks often use different tactics like they lock the computer display and do not allow the user to access any program. The Computer screen displays a message that claims to be from a branch of local law enforcement. Messages are usually something like, "You have browsed illicit materials and must pay a fine". The next ransomware variant displays a pornographic image and demand payment to have this image removed[2].These ransomware attacks lock computer or device, preventing victims from using it and hence termed as Locker Ransomware (Computer Locker). Locker Ransomware generally uses payment vouchers for payment. Yet, another category is Crypto Ransomware (Data Locker) which encrypts personal data and files on the computer and generally use Bitcoins for payment [1]&[20]. Figure 1 and Figure 2 shows sample of locker and Crypto Ransomware, respectively.

Figure 1: Example of Locker Ransomware

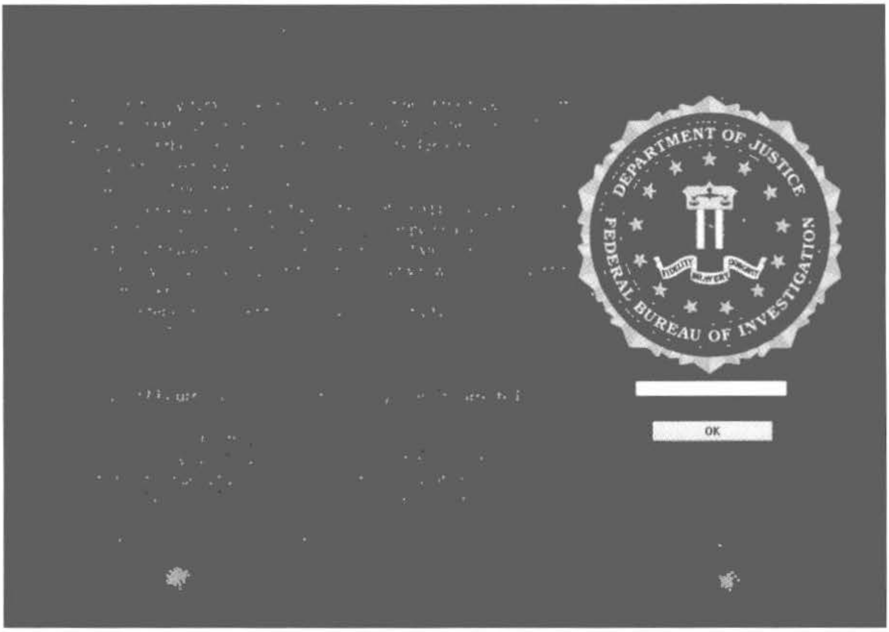
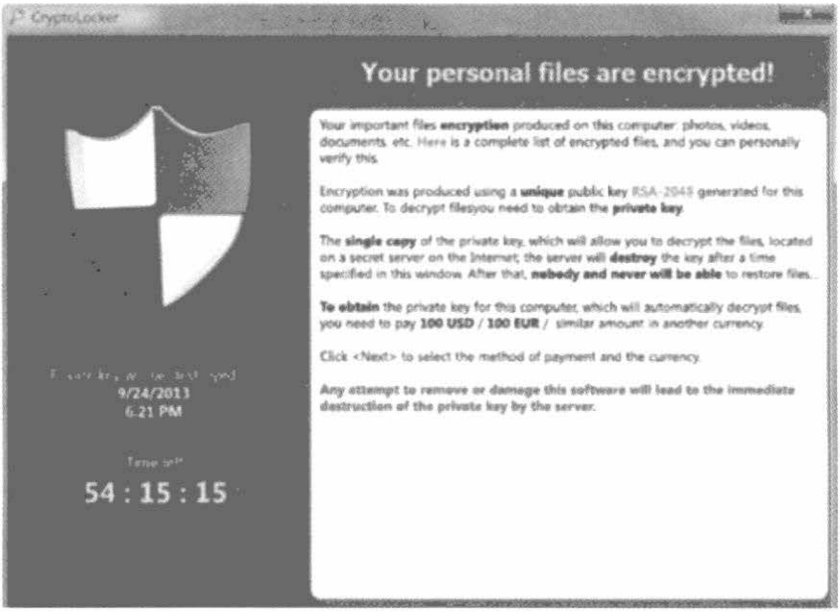


Figure 2: Example of Crypto Ransomware



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt filesyou 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...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **100 USD / 100 EUR** / similar amount in another currency.

Click <Next> to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by the server.

Private key will be destroyed on
9/24/2013
6:21 PM

Time left
54 : 15 : 15

Ransomware Evolved: Modern Ransomware

Ransomware is designed for direct revenue generation. The most prevalent revenue-generating risks include misleading apps, fake antivirus scams, locker ransomware, and crypto ransomware etc. The first wave of misleading applications began to appear in 2005. The apps posed as fake spyware removal tools or performance enhancement tools. These fake tools mainly affected Windows computers but also targeted Mac OS X computers. They exaggerated the impact of issues on the computer and said that they would resolve these issues if the user pays for a license. In reality, many of them did not fix anything [3]. Even at this early stage, the first wave of modern crypto ransomware threats appeared. Although malware authors were using custom encryption techniques which were weak but with passage of time they are making refinements at each step as they have learned the lessons from the past failures.

Even at this early stage, the first wave of modern crypto ransomware threats appeared. Initially using custom encryption techniques which were weak and easily overcome. By early 2006, attackers started experimenting with the idea of crypto-ransomware wherein they copied data files into individual password-protected archive files and then deleted the originals. But the password was actually embedded inside the code itself, making it easy to recover the password [3].

In 2008 and 2009, cybercriminals switched to fake antivirus programs. These were misleading applications which copied the appearance and functionality of legitimate security software and performed mock scans, claiming to find large numbers of threats and security issues on the computer. The user was then asked to pay a fee to fix the fake problems. However, some fake antivirus victims chose to ignore the alerts or removed the software, resulting in a lower return on investments for the cyber criminals. Till 2010 Fake antivirus was at its peak trying every best shot to trap the innocent users.

From 2011 onwards Locker Ransomware started spreading its roots with a more determined approach. Actually, locker ransomware emerged a few years before its steep growth between 2011 and 2012. Users encountered first computer-locking malware around the start of 2008. Locker ransomware is typically designed to prevent access to the computer interface, largely leaving the underlying system and files untouched [3].Locker ransomware creators generally use social-engineering techniques to convince users to pay the ransom. After an increased number of attacks, tech savvy made it possible to remove the malware and restore a computer to something close to its original state. This caused sink in attacker's revenue [4].

With each passing year, cybercriminals are bringing innovations and improvements in their extortion schemes. They have polished crypto ransomware technique and have brought a more refined form of it by learning lessons from the mistakes they did in past. From 2013 to the present day, Crypto ransomware trend has shown progression. Crypto Ransomware tends not to use social engineering; instead of being upfront intentions and demands are being kept. It typically displays an extortion message that demands a hefty ransom so as to get the data back [3] & [4]. Crypto ransomware has raised the ransom amounts bar to a new level. Modern crypto ransomware threats are much more capable than its predecessors, with stronger operational and encryption procedures. They also use privacy-enabling services, such as Tor, and favor bitcoins for payment. This is all to play safe and avoid being identified by law enforcement agents [4].

III. Factors driving the growth of Ransomware

Ransomware has become a menace and it is broadening its horizon bringing some new techniques with every passing year. There are many key factors driving the growth of Ransomware. Some of the major factors include:

Advanced Encryption

The most important driving force is strong encryption implementations, which has helped cyber criminals create potent threats. Applying strong and effective encryption was one of the major trouble attackers were facing, and they have made remarkable progress in recent years. A new variant of ransomware uses a combination of symmetric and asymmetric encryption. The idea behind that is to provide advantages of both symmetric and asymmetric scheme [4].

TOR (Anonymity Network)

TOR, which stands for "The Onion Router" is a network and browser developed to enhance and anonymize the Internet. All traffic is encrypted and the network was designed to anonymize and hide the originating and ending destination. TOR network is used to communicate or host websites that cannot be easily tracked by law enforcement or government officials. Since TOR is well crafted for anonymizing activity so ransomware creators use it to interact with their victims without much fear of discovery [14].

Effective Infection Vectors

Cybercriminals exploit one of the unpatched vulnerabilities to install malicious software on a machine. It can be vulnerabilities in an unpatched version of Adobe Flash, a bug in Java or an old web browser and even an unpatched outdated operating system.

There are many ways ransomware can infect a computer like malicious e-mail, Malvertising, SMS messages and third-party app stores etc. An infection may happen by visiting a compromised website with an old browser or software plug-in or an unpatched third party application. The compromised website runs an exploit kit (EK) which checks for known vulnerabilities and in the case of any vulnerability being detected, it allows the execution of malicious code. Several major exploit kits have been observed distributing ransomware. For example, the Angler exploit kit was one of the prominent delivery channels for CryptXXX. The Neutrino exploit kit has been delivering a number of ransomware variants including Locky, Cerber, and CryptoWall [4] & [5]. An effective form of ransomware ensures that it spreads to as many users as possible. Even if only a small fraction became infected, the cybercriminals behind these ransomware would be likely to profit significantly.

Cryptocurrencies

Ransom payment has always proved a challenge for cybercriminals as it should be the one easily accessible to the victim and also untraceable. Earlier attackers relied largely on payment vouchers [4].But due to problems like encashing the vouchers and maintaining the anonymous nature in the case of vouchers, cryptocurrency became prominent driving factor of ransomware. The rise of Bitcoin and other cryptocurrencies provided an alternative that operates outside the traditional financial system. With the rise of Bitcoin has come a rise in ransomware as well. Using or owning Bitcoin is not an inherently criminal activity at all. Bitcoin wallets are free and disposable, meaning attackers can generate a new, unique wallet for each infection, making it more difficult for law enforcement to follow all earnings [5] & [19].

Advanced Attack Techniques

From the last couple of years, ransomware attackers have introduced a wide variety of new techniques for ransomware implementation. A lot of new ransomware types have been coded in different programming languages, such as JavaScript, PHP, PowerShell, or Python. These languages are precautionary being chosen to evade detection.

Ransomware families have also begun to add features beyond the core functionality of locking devices or encrypting files. For example, CryptXXX contains an additional feature that allows it to gather Bitcoin wallet data and send it to the attackers. Cerber is reportedly capable of adding the infected computer to a botnet which can be used to carry out distributed denial of service (DDoS) attacks. Chimera makes an additional threat in its ransom message. In addition to encrypting files, the malware threatens to post the victims files, including pictures and videos, on the internet [4]. The inclusion of these techniques clearly show ransomware attackers are trying their best to play safe and take maximum advantage out of infected computers.

Ransomware-as-a-Service

One of the major factors is growing problem of ransomware-as-a-service (RaaS) platforms. It basically let anyone subscribe to involve in cyber attacks without needing to come up with their own code. This offers the RaaS vendor a better opportunity to get their ransomware to a wider group of potential victims, letting them focus on developing and enhancing the ransomware and leaving the propagation to others. It works as an affiliate scheme where affiliates are responsible for the propagation of ransomware and later ransom money is being divided between ransomware author and affiliate. The rise of ransomware-as-a-service (RaaS) has lowered the barrier to entry and put ransomware in the hands of a wider range of cyber criminals. RaaS is designed to make cybercrime accessible to anyone, irrespective of the level of their programming skills. You don't need to be tech-savvy or have expensive equipment [6]&[7]. The icing on the cake is ransomware is not only cheap to purchase and download; it's also easy to spread. This leads to a higher volume of attacks and higher ransom requests.

IV. Common Ransomware Types

Ransomware is broadly divided into two types. One is Locker ransomware, which locks the computer or device. Other is Crypto ransomware, which prevents access to files or data, usually through encryption.

Locker Ransomware

Trojan: W32/Reveton

It locks the user system and fraudulently claims to be a legitimate law enforcement authority. The infected computer's machine displays an official-looking message stating that the user had been involved in illegal activity such as child pornography or software piracy and that they could avoid further action and regain normal access to their computers by paying a fine [8]&[10].The threats were very real looking and technique was very convincing. But an increased number of such ransomware helped to raise awareness about them and attackers were bound to bring some innovation to this.

Crypto Ransomware

CryptoLocker

Cryptolocker brought a change in tactics used by cyber criminals. It was the first example of ransomware that used encryption. It was designed to attack Windows operating system by encrypting all the files from the system using RSA[11]&[17]. Each file of user data is encrypted with a different, randomly generated symmetric key. The symmetric key is then encrypted with a public asymmetric key and added to the file [8]. After encryption of all the files, it displays a ransom message demanding payment in return for the private asymmetric key to decrypt the symmetric keys for each encrypted file. The cyber criminals threaten to delete the private keys if payment is not made by a deadline, making data recovery impossible. It also sends a warning that any attempt to remove the ransomware would result in the asymmetric key being deleted.

CryptoWall

Since the time it has come into existence it has appeared in slightly different versions that include CryptoDefense, CryptorBit, CryptoWall 2.0, CryptoWall 3.0 and CryptoWall 4.0. One peculiar feature of CryptoWall is that the

Cybercriminals offer a free single-use decryption key for one file only. It will even delete shadow copies while it encrypts files. CrytpoWall 4.0, released in late 2015, came up with a new feature. It encrypts even the filenames of the files that it encrypts to make it even harder for the victim to know what has been encrypted. Even this makes an antivirus program difficult to detect the malware easily [8]&[16].

Locky

Locky first appeared in 2016, and it usually infects users via malicious Microsoft Office attachments to emails. When the Office file is clicked, the file may prompt the user to enable Office macros, but in fact, it allows the malware to run. After encryption process completes, it displays a ransom note. It instructs users to download the Tor Browser and visit a link specified in the note to pay the ransom. A later version of Locky infects users via a JavaScript attachment that automatically runs malware when clicked, without the need for Office macros to be enabled [8].

WannaCry

This ransomware has shaken a lot of countries by infecting more than 230,000 windows computers in May 2017. It has exploded across 150+ countries. It is also known as Wcry or WannaCrypt or Wcrypt ransomware [9]. It took advantage of an unpatched Microsoft Windows vulnerability in implementations of Server Message Block (SMB). This exploit is referred as Eternal Blue which was apparently stolen and misused by a group called Shadow Brokers. Actually, Eternal Blue is hacking weapons developed by National Security Agency (NSA) to access and hence command the computers running Microsoft Windows. It was specifically designed for the America's military intelligence unit to get an access to the computers used by the terrorists. WannaCrypt first gains access to the computer system via an email attachment and it can spread rapidly through LAN. This ransomware encrypts your system's hard disk and tries to exploit the Server Message Block (SMB) vulnerability. Further it spreads between computers on the same network and it also reaches random computers on the Internet [10].

KeRanger

KeRanger appeared in 2016 and is apparently first ransomware to successfully infect Mac computers running OS X. In 2014, a type of ransomware called FileCoder was discovered, but it did not function properly. KeRanger was injected into the installer of BitTorrent client called Transmission which is an open source. The users who downloaded the infected installer were infected with the ransomware [8] [13].Then after encryption of the files that happens at backend without the user being aware of it, the user gets a ransom note in form of a text file. The ransomware authors offer to decrypt one file for free just to prove that they hold the decryption keys for others files as well.

Protection against Ransomware

Adopting a multilayered approach to security minimizes the chance of infection. First and the foremost thing should be spreading effective security awareness amongst users especially the employees of organizations who are handling critical data of the company. Use up to date antivirus software and firewall. Enable popup blocker. Implement a highly effective patch procedure that updates all applications that have vulnerabilities. Implement a backup solution that too on regular basis: Software-based, hardware based, or both. Ensure your data is safe, redundant and easily accessible in case ransomware. Be vigilant and extra cautious when exchanging and opening emails, and never click on links or download attachments that seem to be malicious and should avoid browsing suspicious websites. If one receives a Ransomware attack, simply unplug the computer from the network. Turn off wireless functionalities like Wi-Fi, Bluetooth, NFC, etc. Ransomware is a serious issue so alert authorities immediately. Paying ransom sometimes may prove to be an invitation to further extortion [15], [5]&[18].

Conclusion

Ransomware is a type of malware that prevents or restricts users from accessing their system resources. Ransomware is a product of cyber criminals who seek to create a reliable source of direct income from victims worldwide. Since the time ransomware has come into existence it has evolved with each passing year and has many twists and turns in its history. Cyber criminals are very smart, fast, and innovative. Starting from misleading applications such as PC performance tools, cybercriminals learned and iterated over the years and with each step, raised the levels of aggression. They progressed from misleading apps to fake antivirus scams and then later moved onto pure ransomware in the form of locker and crypto ransomware threats that are so prevalent today. There are different factors that are contributing in the growth of ransomware Ransomware is evolving rapidly. Thus, it is important for users to know how Ransomware functions, its different forms and best possible ways for prevention and protection. Attention to security is paramount for all. Battling ransomware is a major task and we all have a role to play in it. The growth of the Internet of Things (IoT) has multiplied the range of devices that could potentially be infected with ransomware. With growing awareness about prevalent ransomware attacks, attackers may turn to IoT to find new targets.

References

1. (Undated). Retrieved from www.trendmicro.com: http://www.trendmicro.com/vinfo/us/security/definition/Ransomware
2. (Undated). Retrieved from www.esecurityplanet.com: http://www.esecurityplanet.com/malware/types-of-ransomware.html
3. (Undated). Retrieved from www.securityjar.com: https://securityjar.com/types-of-ransomware-attacks
4. (Undated). Retrieved from www.microsoft.com: https://www.microsoft.com/security/portal/threat/encyclopedia/Entry
5. (Undated). Retrieved from www.bitdefender.com: https://www.bitdefender.com/support/cryptolocker-ransomware---details-and-prevention-1204.html
6. (Undated). Retrieved from www.thewindowsclub.com: http://www.thewindowsclub.com/what-is-wannacrypt-ransomware
7. (Undated). Retrieved from www.symantec.com: https://www.symantec.com/connect/blogs/keranger-first-mac-os-x-ransomware-emerges
8. (Undated). Retrieved from www.torproject.org: https://www.torproject.org/about/overview.html.en
9. (Undated). Retrieved from www.trendmicro.com: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats
10. (2017). Retrieved from www.forbes.com: https://www.forbes.com/sites/forbestechcouncil/2017/03/17/ransomware-as-a-service-the-next-great-cyber-threat
11. (2017). Retrieved from www.nytimes.com: https://www.nytimes.com/2017/05/15/technology/personaltech/heres-how-to-protect-yourself-from-ransomware-attacks.html?_r=0
12. Alessandrini, A. (2016). *Ransomware: Hostage Rescue Manual.* Technical Report, KnowBe4 Human error conquered.
13. Boatman, K. (Undated). *Threats: Beware the Rise of Ransomware.* Retrieved from in.norton.com: https://in.norton.com/yoursecurityresource/detail.jsp?aid=rise_in_ransomware
14. *CISCO, Inc. Ransomware on Steroids: Cryptowall 2.0.* (n.d.). Retrieved from blogs.cisco.com: http://blogs.cisco.com/security/talos/cryptowall-2

15. *DELL Security works , "Cryptolocker Ransomware".* (n.d.). Retrieved from www.secureworks.com: https://www.secureworks.com/research/cryptolocker-ransomware

16. Fraga, B. (2013). The Herald News. *Swansea police pay $750 "ransom" after computer virus strikes. The Herald News, 2013.*

17. *Industry News- Technology.* (2014). Retrieved from www.bizjournals.com: http://www.bizjournals.com/memphis/blog/2014/11/tennessee-sheriff-pays-ransom-to-cybercriminals-in.html

18. McDonald, G. & Gorman, G. (2012). *Ransomware: A growing menace.* Technical report, Symantec Corporation.

19. (2016). *Ransomware and Businesses.* Technical report, Symantec Corporation.

20. Savage, K., Coogan, P. & Lau, H. (2015). *The Evolution of Ransomware.* Technical report, Symantec Corporation.