Cosmos Multidisciplinary Research E-Journal
Online Available at www.cmrj.in
Recognized International Peer Reviewed Journal
ISSN No. 2456-1665

Study the Evolution of Ransomware and Future Trends

Prashant L. Chintal
Research Scholar
Department of CSE and IT
Dr. BAMU, Aurangabad (M.S)

Dr. Rajendra Gaikwad
Principal
Ankushrao Tope College,
Jalna(M.S)

Dr. Ratnadeep R. Deshmukh
Head, Department of CSE and IT
Dr. BAMU, Aurangabad

ABSTRACT

Ransomware is a type of malicious software that blocks user access to files or systems, holding files or entire devices hostage using encryption until the victim pays a ransom in exchange for a decryption key, which allows the user to access the files or systems encrypted by the program. This paper aims to review on history of ransomware and the future of this threat in addition this paper gives more emphasis on recently found wannacry ransomeware in general and technical aspects.

Keywords Ransomware, Wannacry, Cybercriminal, Bitcoins

INTRODUCTION

Ransomware has been a prominent threat to enterprises, Small and medium scale businesses, and individuals alike since the mid-2000s. Ransomware has been around for decades, ransomware varieties have grown increasingly advanced in their capabilities for spreading, evading detection, encrypting files, and coercing users into paying ransoms. This paper reviews on evolution and classes of reamsoware from decade and describes general ant technical details of wannacry ransomware.

History of Ransomware

There were more than 7,600 ransomware attacks reported to the Internet Crime Complaint Center (IC3) between 2005 and March of last year. In 2015, IC3 received 2,453 ransomware complaints that cost victims over $1.6 million. Despite the fact that remsomwar were prominently evolving and spreading since last decade and become one of the biggest threat since year 2005, the first ramsomware attack occurred much earlier i.e in year 1989 targeted the health care industry where the attacker carried out the attack by distributing 20,000 floppy disks to AIDS researchers spanning more than 90 countries, claiming that the disks contained a program that analyzed an individual's risk of acquiring AIDS through the use of a questionnaire. However, the disk also contained a malware program that initially remained dormant in computers, only activating after a computer was powered on 90 times. After the 90-start threshold was reached, the malware displayed a message demanding a payment of $189 and $378 for a software lease. This ransomware attack became known as the AIDS Trojan, or the PC Cyborg[1]. This did set the stage for the evolution of ransomware to the sophisticated attacks carried out today.

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. 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 case, 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 case of ransomware prevents access to files to potentially critical or valuable files like documents and spreadsheets. Fig.1 shows the Cryptolocker ransomware message.

Ransom prices vary depending on the ransomware variant and the price or exchange rates of digital currencies. 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 the ransom does not guarantee that users will get the decryption key or unlock tool required to regain access to the infected system or hostaged files.[2]

Financial Aspect :

The ultimate goal of ransomware attacks is to get money from victims, the payment method is an important aspect of the attacks. Cybercriminals continuously strive to find more reliable charging methods by improving two important properties: (1) the difficulty of tracing the recipient of the payments, and (2) the ease of exchanging payments into a preferred currency. Bitcoin provides some unique technical and privacy advantages for miscreants behind ransomware attacks. Bitcoin transactions are cryptographically signed messages that embody a fund transfer from one public key to another and only the corresponding private key can be used to authorize the fund transfer. Furthermore, Bitcoin keys are not explicitly tied to real users, although all transactions are public. Consequently, ran-somware owners can protect their anonymity and avoid revealing any information that might be used for tracing them.[3]

EVOLUTION OF RAMSOMEWARE

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 re 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 note starts.

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 note.

Table 1: Summary of types of charges in 15 ransomware families.

Families	Type of Charge			
	Premium Number	Untraceable Payments	Online Shopping	Bitcoin Transactions
Reveton		✓	✓	
Cryptolocker		✓		✓
CryptoWall				✓
Tobfy		✓		
Sefilad	✓			
Winlock				
Loktrom	✓			
Calelk	✓			
Urausy		✓	✓	
Kroeten		✓		
BlueScreen		✓		
kovter		✓	✓	
Filecoder		✓		
GPcode		✓		
Weelsof		✓		
Number of Samples	132 (9.71%)	1,199 (88.22%)	14(1.03%)	28 (2.86%)
Number of Variants	18 (19.35%)	75 (80.64%)	4 (4.30%)	4 (4.3%)

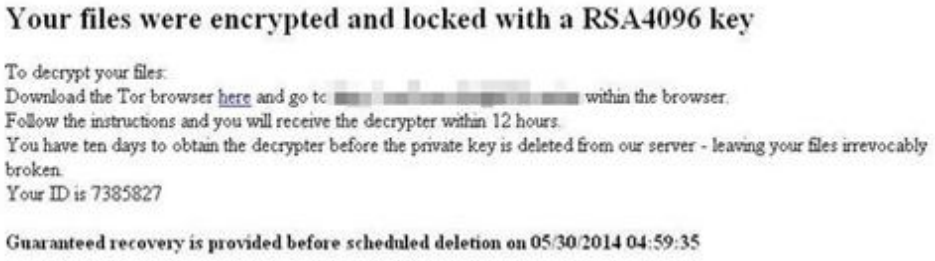
A case in 2012 involved a popular French confectionary shop's website that was compromised to serve TROJ_RANSOM.BOV. This watering hole tactic resulted in widespread infections in France and Japan, where the shop also had a significant fan-base. Instead of the usual ransom note, TROJ_RANSOM.BOV displayed a fake notice from the French police agency *Gendarmerie Nationale*.

In late 2013, a new type of ransomware emerged that encrypted files, aside from locking the system. The encrypted files ensured that victims are forced to still pay the ransom even if the malware itself was deleted. Due to its new behavior, it was dubbed as "**CryptoLocker**". Like previous ransomware types, crypto-ransomware demands payment from affected users, this time for a decrypt key to unlock the encrypted files.

Ransomware soon began to incorporate yet another element: cryptocurrency (e.g., Bitcoin) theft. In 2014, Trend Micro saw two variants of a new malware called BitCrypt. The first variant, TROJ_CRIBIT.A, appends ".bitcrypt" to any encrypted files and displays a ransom note in English. The second variant, TROJ_CRIBIT.B , appends the filename with ".bitcrypt 2″ and uses a multilingual ransom note in 10 languages. CRIBIT variants use the encryption algorithms RSA(426)-AES and RSA(1024)-AES to encrypt the files, and specifies that the payment for unlocking files be made in Bitcoins.

In 2015, the Angler exploit kit was one of the more popular exploit kits used to spread ransomware, and was notably used in a series of malvertisment attacks through popular media such as news websites and localized sites. Angler was constantly updated to include a number of Flash exploits, and was known for being used in notable campaigns such as the Hacking Team leak and Pawn Storm. Because of its easy integration, Angler remains a prevalent choice as a means to spread ransomware.

A new variant of Ransomware and Cryptolocker threats surfaced that leverages the Windows PowerShell feature to encrypt files. Trend Micro detects this as TROJ_POSHCODER.A. Windows PowerShell is a built-in feature in Windows 7 and higher. Cybercriminals often abuse this feature to make threats undetectable on the system and/or network. POSHCODER uses AES encryption and an RSA 4096 public key to encrypt the said AES key. Once all files on the infected system are encrypted, it displays the following image:



particular ransomware different from other police ransomware is that it rides on patched malware to infect systems. Patched malware is any legitimate file that has been modified (via addition or injection) with malicious code. Modifying a legitimate file can be advantageous to cybercriminals as the rate of execution of malicious code will depend on the infected file's frequency of use.

This ransomware is also notable for infecting user32.DLL, a known critical file. Infecting a critical file can be considered an evasion technique as it can help prevent detection by behavioral monitoring tools due to whitelisting. Additionally, cleaning critical files such as user32.DLL requires extra care as one misstep can crash a system, which could be seen as a possible obstacle for cleaning tools.

Earlier crypto-ransomware types targeted .DOC, .XLS, .JPG, .ZIP, .PDF, and other commonly-used files to encrypt. Cybercriminals have since included a number of other file types critical to businesses, like database files, website files, SQL files, tax related files, CAD files, and Virtual desktop files.

Some of the most notable crypto-ransomware families seen in 2016.

LOCKY (RANSOM_LOCKY.A) – Discovered in February 2016, Locky was notable for its distribution methods, first seen arriving as a macro in a Word document, and then spotted being spread via Adobe Flash and Windows Kernel Exploits. One of the most actively-updated ransomware families, Locky ransomware is known for deleting shadow copies of files to make local backups useless, and is notorious for being used in multiple high-profile attacks on healthcare facilities.

PETYA (RANSOM_PETYA.D)– First seen in March 2016, PETYA overwrites the affected system's master boot record (MBR), and is known to be delivered through legitimate cloud storage services such as Dropbox.

CERBER (RANSOM_CERBER.A) – When it was first seen in early March 2016, CERBER was notable for having a 'voice' feature that reads out the ransom message. CERBER was also found to have a customizable configuration file that allows distributors to modify its components—a feature common for malware that's being sold in underground markets. CERBER is also notorious for being used in an attack that potentially exposed millions of Microsoft Office 365 users to the infection.

SAMSAM (RANSOM_CRYPSAM.B) – Discovered in March 2016, SAMSAM is installed after the attackers exploit vulnerabilities on unpatched servers—instead of the usual malicious URLs and spam emails—and uses these to compromise other machines.

JIGSAW (RANSOM_JIGSAW.I) – The first JIGSAW variant seen in April 2016 mixed effective scare tactics with an innovative routine. Featuring imagery from the *Saw* movie

franchise, Jigsaw's ransom note features a countdown timer to pressure its victims into paying—with a promise to increase the ransom amount while deleting portions of the encrypted files every time the timer runs out. Recent Jigsaw variants also featured a chat support feature that allows victims to contact the cybercriminal.[2]

WANNACRT RANSOMWARE :

The WannaCry ransomware attack was a worldwide cyberattack by the WannaCry ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency.

The attack began on Friday, 12 May 2017, and within a day was reported to have infected more than 230,000 computers in over 150 countries. Parts of Britain's National Health Service (NHS), Spain's Telefónica, FedEx and Deutsche Bahn were hit, along with many other countries and companies worldwide.[4] The WannaCry ransomware attack has quickly become the worst digital disaster to strike the internet in years, crippling transportation and hospitals globally.

One of WannaCry's ransom notes

WannaCry ransomware targets and encrypts 176 file types. Some of the file types WannaCry targets are database, multimedia and archive files, as well as Office documents. In its ransom note, which supports 27 languages, it initially demands US$300 worth of Bitcoins from its victims—an amount that increases incrementally after a certain time limit. The victim is also given a seven-day limit before the affected files are deleted—a commonly used fear-mongering tactic. WannaCry leverages CVE-2017-0144, a vulnerability in Server Message Block, to infect systems. The security flaw is attacked using an exploit leaked by the Shadow Brokers group—the "EternalBlue" exploit, in particular. Microsoft's Security Response Center (MSRC) Team addressed the vulnerability via MS17-010 released March, 2017.

WannaCry's has worm-like behavior allows WannaCry to spread across networks, infecting connected systems without user interaction. All it takes is for one user on a network to be infected to put the whole network at risk. WannaCry's propagation capability is reminiscent of ransomware families like SAMSAM, HDDCryptor, and several variants of Cerber—all of which can infect systems and servers connected to the network.

PREVENTIONS FROM WANNACRT RANSOMWARE :

Here are some of the solutions and best practices that organizations can adopt and implement to safeguard their systems from threats like WannaCry:

- Avoid opening unverified emails or clicking links embedded in them.
- Back up important files using the 3-2-1 rule—create 3 backup copies on 2 different media with 1 backup in a separate location.

- Regularly update software, programs, and applications to protect against the latest vulnerabilities.
- The ransomware exploits a vulnerability in SMB server. Patching is critical for defending against attacks that exploit security flaws. A patch for this issue is available for Windows systems, including those no longer supported by Microsoft. When organizations can't patch directly, using a virtual patch can help mitigate the threat
- Deploying firewalls and detection and intrusion prevention systems can help reduce the spread of this threat. A security system that can proactively monitor attacks in the network also helps stops these threats
- Aside from using an exploit to spread, WannaCry reportedly also uses spam as entry point. Identifying red flags on socially engineered spam emails that contain system exploits helps. IT and system administrators should deploy security mechanisms that can protect endpoints from email-based malware
- WannaCry drops several malicious components in the system to conduct its encryption routine. Application control based on a whitelist can prevent unwanted and unknown applications from executing. Behavior monitoring can block unusual modifications to the system. Ransomware uses a number of techniques to infect a system; defenders should do the same to protect their systems
- WannaCry encrypts files stored on local systems and network shares. Implementing data categorization helps mitigate any damage incurred from a breach or attack by protecting critical data in case they are exposed
- Network segmentation can also help prevent the spread of this threat internally. Good network design can help contain the spread of this infection and reduce its impact on organizations
- Disable the SMB protocol on systems that do not require it. Running unneeded services gives more ways for an attacker to find an exploitable vulnerability[5]

FUTURE OF RANSOMWARE

With the advent in the field of internet and IoT Everything is becoming a computer. Your microwave is a computer that makes things hot. Your refrigerator is a computer that keeps things cold. Your car and television, the traffic lights and signals in your city and our national power grid are all computers. This is the much-hyped Internet of Things (IoT). It's coming, and it's coming faster than you might think. And as these devices connect to the Internet, they become vulnerable to ransomware and other computer threats. It's only a matter of time before people get messages on their car screens saying that the engine has been disabled and it will cost $200 in bitcoin to turn it back on. Or a similar message on their phones about their Internet-enabled door lock: Pay $100 if you want to get into your house tonight. Or pay far more if they want their embedded heart defibrillator to keep working.

REFERENCES

[1] https://factly.in/cyber-crimes-in-india-which-state-tops-the-chart/
[2] http://www.cyberlawsindia.net/
[3] Amin Kharraz, William Robertson "Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks"
[4] https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
[5] https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time
[6] https://www.trendmicro.com/vinfo/us/security/definition/ransomware