A Dangerous Trend of Cybercrime: Ransomware Growing Challenge

Dr.P.B.Pathak

Assistant Professor & Head, Department of Computer Science & Information Technology

Yeshwant Mahavidyalaya Nanded

Maharashtra, India

***Abstract*— Recently computers are used massively due to advent of the internet and technology, so as cybercriminals also emerged to target innocent users to make money from the victims. People across the globe are subjected to extortion on a very large scale. Ransomware is modern and technology enabled way of extortion. Ransomware stops you from using your system or device and holds your system/device or files for ransom. The present research paper discusses Ransomware all round i.e. What is it? What are various forms of it? How it works? How to prevent it?**

***Index Terms*—Bitcoin, CryptoLocker, Cybercrime, Malware, Ransomware**

I. INTRODUCTION

Ransomware is a kind of malware that attempts to extort money from a computer user by infecting and taking control of the victim's machine, or the files or documents stored on it. Generally, the Ransomware either locks the computer to prevent normal usage, or encrypts the documents and files on it to prevent access to the documents and files. The ransom demand is displayed, usually either via a text file or as a webpage in the web browser. This type of malware exploits the victim's embarrassment or fear to force them pay the ransom demanded. Ransomware may arrive as part of another malware's payload, or may be delivered by an exploit kit to exploit vulnerabilities on the affected computer and it silently installs and executes the malware.[1]

Ransomware is a way of direct and large scale revenue generation using Crypto Ransomware and Locker Ransomware. Crypto Ransomware encrypts personal data and files on computer and Locker Ransomware locks the computer or device, preventing victims from using it. Locker Ransomware use payment vouchers and Crypto Ransomware use it's Bitcoins for payment. Ransomware is considered a Scareware as it scares users to pay a fee or ransom. Paying for the ransom does not guarantee that users can eventually be able to access the infected system.[11]

Users may witness Ransomware threat through a variety of ways. Ransomware can be downloaded by unaware users by visiting malicious or compromised websites. It can also arrive as a either dropped or downloaded payload by other malware. It may arrive as an attachment to a spammed email. Cybercriminals behind Ransomware are ever innovative. Ransomware attacks often use tactics like entrusting pornography on your screen to demand you pay a ransom to remove the pornography.[2]

II. RANSOMWARE AND TYPES

These Ransomware systematically progressed and improved with the technological advances and widespread use of Internet, to make it more scary and powerful over the years. [3,13]

- FAKEAV malware forces users to purchase their bogus antimalware software by showing fake antimalware scanning results.
- A Ransomware zip's certain type of files usually .DOC, .XL, .DLL, .EXE and overwrites these, keeping only the password protected zip files in the user's system along with a ransom note in the notepad.
- SMS Ransomware asks to call a premium SMS number and also displays a Ransomware page continuously to users as long as they do not pay the ransom.
- A Ransomware targets Master Boot Record of a vulnerable system to prevent the operating system from loading and displays its ransom notification.
- Reveton or Police Ransomware impersonates local

Manuscript received Feb, 2016.
***Dr.P.B.Pathak,** Assistant Professor & Head,*
Department of Computer Science & Information Technology
Yeshwant Mahavidyalaya Nanded,Maharashtra, India

police by showing a notification page, informing them that they were caught doing an illegal or malicious activity online. Reveton employ different payment methods.

- Some Ransomware play an audio recording using the victim's native language and some bears a fake digital certificate.
- CryptoLocker Ransomware encrypts files, rather than locking the system to ensure that users will pay though the malware is deleted. The spammed message contain malicious attachment, downloading attachment downloads the CryptoLocker malware.
- CryptoDefense or Cryptorbit, malware demands payment for its decryption services. This can easily spread compared to other via removable drives eliminating need of relying on downloader malware to infect systems. This malware not only encrypts database, web, Office, video, images, scripts, text, and other non binary files but also deletes backup files to prevent restoration of encrypted files. [9,12]
- BitCrypt is more refined Ransomware incorporate Cryptocurrency e.g., Bitcoin theft with two variants first uses an English ransom note and the second uses a multilingual ransom note.
- CRIBIT malware also extorts in the form of Bitcoins for unlocking files.
- FAREIT variant, information stealing malware can steal information from various Cryptocurrency wallets containing important information like transaction records, user preferences, and accounts.
- CryptoLocker variant Ransomware abuse Windows PowerShell feature to encrypt files to make threats undetected on the system and/or network.
- A police Ransomware infects a known critical file, user32.DLL and locks the screen of the infected computer thereby prevents detection by behavioral monitoring tool. The infected user32.DLL will begin a chain of routines that ends with the Ransomware being loaded, locking the computer's screen and projecting a ransom image messages. [10]
- Critroni or Curve-Tor-Bitcoin (CTB) Locker Ransomware uses the Tor network to mask its C&C communications, asks for Bitcoins as ransom. CTB Locker variant TorrentLocker Ransomware adds CAPTCHA code and redirection to a spoofed site.
- Crowti or Cryptowall, and FakeBsod are Ransomware families. FakeBsod uses a malicious piece of JavaScript code to lock your web browser and show a fake warning message when you visit infected or malicious webpage. The warning message tells you to call the phone number in the message and you will be asked to pay money to fix the issue.[4,14]

III. How Ransomware Works

Locker Ransomware denies access to computing resources. This typically locks the computer's or device's user interface and then asks the user to pay a fee to restore access to it. Locked computers will remains with limited capabilities. Locker Ransomware leaves the underlying system and files untouched meaning that the malware can potentially be removed to restore a computer to original state. This dims effectiveness of locker Ransomware at extracting ransom payments compared with its more destructive variants of Crypto Ransomware. This type of Ransomware often impersonate as police authorities and claims to issue fines to users for alleged online imprudence or criminal activities.[5]

Crypto Ransomware finds and encrypts valuable data stored on the computer, making the data useless unless the user obtains the decryption key. The developers of Crypto Ransomware know that data on computers is very important to users and they may be desperate to get their data back, preferring to pay the ransom to restore access and avoid painful consequences. Crypto Ransomware unnoticeably searches for files and encrypts them. Its goal is to stay unnoticed until it can find and encrypt all of the files that could be important and valuable to the user. By this time the victim receives the malware's message that that their data is encrypted. With Crypto Ransomware infections, mostly the affected computer continues to work normally, and users can still use the computer apart from accessing encrypted data. [9]

Police themed Ransomware cleverly present their ransom demands as official looking warning messages from a local police. Ransom message claim that the user's computer is locked after the police identified it as being used to visit illegal websites related to terrorism or abuse and that payment of a fine is required to settle the offense and directions for paying it via anonymous, untraceable disposable cash cards. TorrentLocker and CryptoWall malware variants are difficult to beat and grow their disjointed criminal activity into coordinated, improved stealth and effective business operations. Ransomware attack methods advanced in techniques and increased in profit in past few years. The social engineering has increased infection rates considerably. [15]

TorrentLocker, is successful due to its targeted campaigns. The infection chain involves a three step process:

- URL Redirection,
- Getting on Malicious Page,
- CAPTCHA code Verification.

Attackers compromise web servers and redirect the URL, eventually victim gets on page controlled by cybercriminal, and victim is required to complete simple CAPTCHA code verification test. Immediately after entering the CAPTCHA, the TorrentLocker malware is extracted and executes its commands to encrypt files. CryptoWall has been used to exploit unsuspecting businesses. The timing and design of socially engineered attack keeps recipients clueless to understand that they are attacked. The CryptoWall 3.0 uses AES algorithms to encrypt files and an RSA to encrypt the

key, making it impossible for victim, since the decryption key is with the hacker, to find out a method for decrypting.[6]

IV. How to Prevent Ransomware Attack

Ransomware attack can be prevented by adopting some simple day-to-day regular practices and severity can be reduced if not eliminated. Use reputed antivirus software and a firewall and keep security software up to date. Back up files regularly so that computer can be simply restored to default state and start afresh. Enable popup blocker. One should be always vigilant and cautious when exchanging and opening emails, must know the senders, and should never click on links or download attachments that are not expected and should avoid browsing suspicious websites. If one receives a Ransomware notice, simply disconnect the machine from Internet. Ransomware is a serious form of extortion so alert authorities immediately. Paying ransom sometime may prove to be invitation to further extortion. At first place take at most precautions and maintain continuous vigilance to avoid ransom attack and becoming a victim. Ransomware infections can be prevented potentially by adopting following measures. [7,8]

- Take regular backup of files and data.
- Ransomware may arrive by exploiting vulnerability so keep security software up to date by applying patches regularly.
- IT is good practice to access trusted and bookmarked websites.
- Always be cautious by avoiding downloading email attachments from untrusted sources and clicking on links from email.
- Use reputed antimalware/antivirus and Scan system regularly.
- Use strong firewall.
- Enable popup blocker
- Disconnect from Internet if received Ransom notice.
- If Ransomware infects system, user should do the following:
- Disable System Restore.
- Use antimalware to remove Ransomware files.
- Alert authorities immediately.

V. Conclusion

Cybercriminals are always smart, fast, and unbelievably adaptive and they're always looking for new tricks and techniques, opportunities to make damage and compromise. Ransomware is a type of virus or malware that prevents or limits users from accessing their system resources. Ransomware forces its victims to pay the ransom through certain online payment methods to grant access to their systems, or to get their data back. Cybercriminals primarily focus on refining existing tools and techniques surely Ransomware is evolving progressively. Thus, it is important for users to know how Ransomware functions and best possible ways to protect them from Ransomware threat. Mobile Ransomware attacks are expected to increase due to the migration of business on portable devices and so it becomes essential we should be able to identify how, where, when, and why a threat operates.

REFERENCES

[1] http://www.trendmicro.com/vinfo/us/security/definition/Ransomware
[2] https://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx
[3] http://in.norton.com/yoursecurityresource/detail.jsp?aid=rise_in_ransomware
[4] https://www.f-secure.com/en/web/labs_global/removing-police-themed-ransomware
[5] Kim Boatman, "Beware the Rise of Ransomware", http://in.norton.com/yoursecurityresource/detail.jsp?aid=rise_in_ransomware
[6] CISCO, Inc. Ransomware on Steroids: Cryptowall 2.0. http://blogs.cisco.com/security/talos/cryptowall-2,
[7] SYMANTEC, Inc, "Internet Security Threat Report" http://www.symantec.com/security_response/publications/threatreport.jsp
[8] Krebs on Security, "Inside a Reveton Ransomware Operation" http://krebsonsecurity.com/2012/08/inside-a-reveton-ransomware-operation/
[9] Bowen, B. M., Hershkop, S., Keromytis, A. D., Stolfo, S. J. "Baiting inside attackers using decoy documents", Springer, (2009).
[10] Carrier, B. "File System Forensic Analysis", Addison-Wesley Professional, (2005).
[11] DELL Securityworks , "Cryptolocker Ransomware", https://www.secureworks.com/research/cryptolocker-ransomware
[12] Malware Tips "Your Security Advisor", https://malwaretips.com/
[13] Ajjan, A. "Ransomware: Next-Generation Fake Antivirus", https://www.sophos.com/en-us.aspx
[14] Blockchain.info, "Bitcoin Block Explorer", https://blockchain.info/.
[15] Prince, B. "CryptoLocker Could Herald Rise of More Sophisticated Ransomware", http://www.darkreading.com

