Survey on Ransomware: A New Era of Cyber Attack

Gandhi Krunal A.
Assistant Professor, I.T Department
Laxmi Institute of Sarigam, Valsad

Patel Viral Kumar D.
Assistant Professor, I.T Department
Laxmi Institute of Sarigam, Valsad

ABSTRACT
In today's world, a most popular crime is Cybercrime. In this paper through a literature study, effect of ransomware is discussed. In this needy internet world, how crucial is to use a non-secure connection and how it will track a normal user or unaware user into the trap of hacker and after that losing money in terms of bit-coins. At last, with the damage cause by the latest attack of ransomware around the world is proved that there is lacks of awareness among the company professionals is confirmed and pay a high amount of money in bit-coins.

Keywords
Ransomware, bitcoins, TOR, wannacry 2.0, payment, education.

1. INTRODUCTION
1) Ransomware
It is a malware which is used by attackers by covertly installing into victim's system through mail attachment (most of the time) and after installation it will encrypt all the files of the victim's system and then demands a ransom payment (in bit-coins) in return for the decryption key which is required to decrypt the encrypted file. Not only can encrypt the files on victim's system but it is smart enough that it will travel across the network and encrypt any files which are located both on mapped and unmapped drive. This can lead to critical situation whereby one user's infection brings entire department or an organization to a halt. The first known ransomware was written in 1989. Thus, this paper main objective is to aware all the peoples who uses internet nowadays and maybe they might encounter it in future [1].

2) Bit-Coins
It is the form of crypto-currency; it means they do not have any physical representation. The main benefits of bit-coins are they are stored in anonymous digital wallets. It can be transferred anywhere in the world via the Internet. It can be paid from anywhere, to anywhere with total anonymity. It is commonly abbreviated as BTC [1].

3) TOR
It is an anonymity network, which stands for "The Onion Router". It is developed by considering the anonymity over internet traffic as prime objective. It uses a special browser that is configured to use a worldwide connected network of relays. All traffic is encrypted and the network was designed to hide the origin and ending destination of the traffic. It also using onion domain. You need TOR browser to use onion domain websites [2].

2. TYPES OF RANSOMWARE
1) Reveton
It is known as Trojan:W32/Reveton an application of the ransomware. It will claim fraudulently to be from a legitimate authority and prevents users from accessing their infected machine, demanding a 'fine' to restore normal access [3].

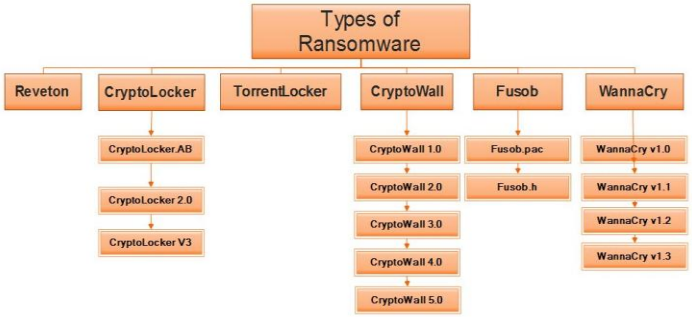

Fig 1. Types of Ransomware

2) CryptoLocker
It is a file-encryption ransomware, which encrypts the personal documents with the help of RSA-2048 key and then displays a message which offers to decrypt the data if a payment is paid through bit-coins only [3].

3) CryptoLocker.F and TorrentLocker
Ransom.Cryptolocker.F and TorrentLocker is a Trojan horse that encrypts files on the compromised computer and then prompts the user to purchase a key in order to decrypt them [3].

4) CryptoWall
It used a JavaScript code as part of an email attachment, which will download executable JPG files to disguise the victim. It will also create a new instance of EXPLORER.EXE AND SVCHOST.EXE to make communication with their server. In addition of it, at the time encryption it will deletes the volume shadow copies and installs spyware that steals passwords and BITCOIN wallets [5].

5) FuSob
After successful encryption of data of the system with above techniques which are successful for big machines, it is the time for Mobiles the smaller ones. The Fusob is the malware which will infect the mobile phones. It pretends to be an authority and for example it will suggest using Play-Store gift cards for payment. Also, a timer clicking down on the screen to make sure user is anxious. In addition, it will masquerade as a pornographic video player and appears on the user's screen to download. When it is downloaded and installed, it first checks the language used in the device. If it uses Russian or some similar language, Fusob does nothing. Otherwise, it puts lock on the screen and demand ransom [6].

6) WannaCry
It is the latest ransomware which is implemented in May 2017, and mainly it targets Microsoft Windows Operating Systems.

Now, after types there is a big question how you would know that you are affected by one of this or not. For that there are few **symptoms**:

- You suddenly cannot open normal files and get errors such as file is corrupted or has the wrong extension.
- An alarming message has been set to your desktop background with instructions on how to pay to unlock your file.
- The program warns you that there is a countdown until the ransom increases or you will not be able to decrypt files.
- A window has opened to a ransomware program and you cannot close it.
- You see files in all directories with names such as HOW_TO_DECRYPT_FILES.TXT_or DECYPT_INSTRUCTIONS.HTML

3. WORKING OF RANSOMWARE

There are steps of being affected by the one of the six ransomwares .

How Ransomwares Works?

1. End user receives an email that appears to be from their boss.

➢ It contains a URL to a SaaS application such as Salesforce, Workday or ZenDesk.

2. The link opens a browser window and directs the user to a website that seems legitimate.

➢ It's actually a landing page for an exploit kit hosted in a.co.cc top level domain (TLD).

3. Upon loading the page, the web server hosting the exploit kit begins communicating with the victim machine.

➢ The server sends requests about versions of software such as Java to find a vulnerable version for which the kit has an exploit.

4. When a vulnerable version is confirmed, the kit attempts to exploit the vulnerability.

➢ Once successful, the exploit kit pushes down a malicious .EXE file – let's call it "ransomware.exe." The malicious binary on the victim machine then attempts to execute.

5. From this beachhead, the binary spawn's child processes, including vssadmin.exe (shadow copy), to delete existing shadows on the victim machine and create new ones to hide in.

➢ The attacker does this to limit the possible recovery of files by the victim using Shadow Copies that Windows stores on a system.

6. The binary uses a PowerShell executable to propagate copies of itself throughout the filesystem.

➢ The executable also searches the filesystem for files of specific extensions and begins to encrypt those files.

7. The powershell.exe child process creates three copies of the originating malware binary, first in the AppData directory, next in the Start directory, and finally in the root C:\ directory.

These copies are used in conjunction with the registry modifications to restart the malware upon reboot and login events.

8. After encrypting the victim's files, the malware sends the encryption key and other host- specific information back to the command-and-control server.

9. The server then sends a message to the victim.

This could be a simple "alert user of encryption and directions on paying us." It could also include directions that result in downloading additional malware, which enables the attacker to steal credentials from the victim as well.

To amplify the victim's distress, ransomware often includes a countdown clock with a deadline for paying the ransom – or else the decrypt key will be destroyed, eliminating any chance of recovery.

Paying the ransom often means the attacker will unlock the victim's machine or provide the key to decrypt files. However, it rarely means the originating malicious binary, "ransomware.exe" in the case above, has been removed. That will require IT and SecOps support.

And the attack doesn't necessarily end there. Attackers often load additional malware on a user's machine, allowing them to harvest personal information, intellectual property, and credentials to sell for additional revenue.

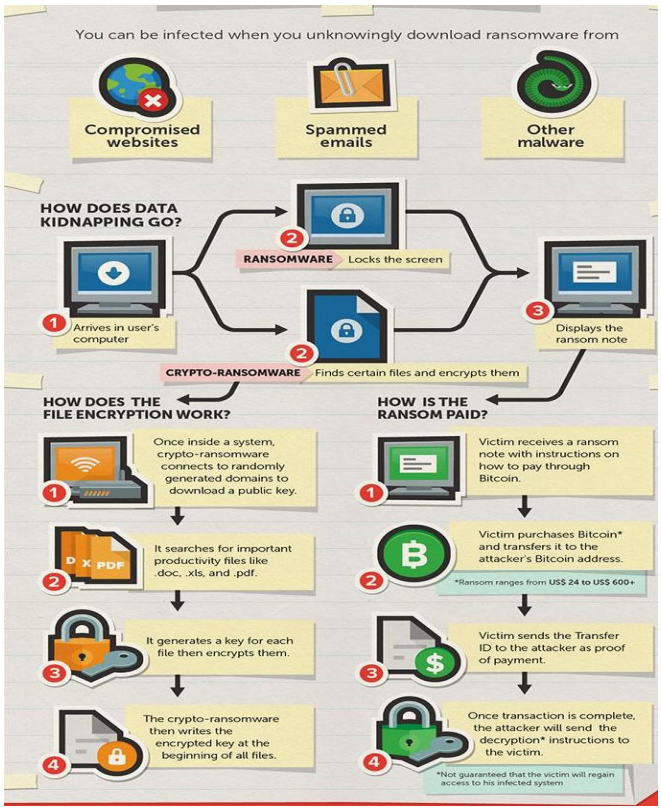

Fig 2. Working of Ransomware

4. RANSOMWARE TRICKS

Ransomware authors have developed a number of clever tricks to make it hard to undo their work, but following are some tricks from you can check whether you are proceeding towards infection or not [14].

Name encryption: The latest version of ransomware now encrypts names of files along with each files' data. encrypted files have names made up of random numbers and letters.

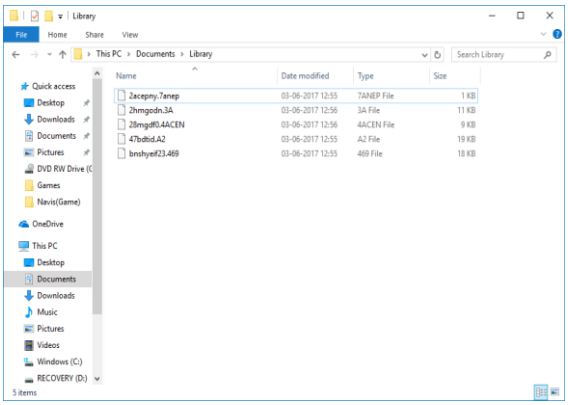

Fig 3. Encrypted File names

Backup and Publish: Some ransomware now claims that copies of the files have been moved to the attackers' servers and, if you don't pay, they will publish the files on the internet.

PCs, and windows, and websites: Ransomware such as Linux Encoder. It will inject itself into websites with known vulnerabilities such as shopping cart programs and once on the host machine will encrypt all the files in the home directories and many of the directories referenced by typical websites.

5. PROTECTION AGAINST RANSOMWARE

There are few Techniques to protect IT infrastructure from the damage of Ransomware.

1) Make regular backups of your all sensitive data and systems and store them offline.
2) Always keep your antivirus databases and software updated.
3) Block unknown ransomware extensions via FSRM. If ransomware cannot create files with those extensions on your server, it cannot encrypt your files.

Make the most of Group Policy:
Set up Group Policy to show up hidden file extensions on all working systems so users can see the double file extensions (such as filename.doc.exe) that attacker use to disguise malware.

Configure the application control policy to blacklist everything and whitelist only needed software.

Use group Policy to disable Autoplay and Autorun on all workstations.

Either disable file execution in e-mail attachments, or quarantine all attachments using your spam filter.

Configure your firewall to whitelist only the specific ports and hosts you need.

Limit user access to shared drives by assigning NTFS permissions via security groups.

Maintain a complete and current inventory of all your equipment and its network addresses so you can quickly find the source of a ransomware attack and take it offline immediately.

And for latest Wannacry 2.0 as it is targeting the Microsoft operating system, update your Operating System and install released patch for SMB. After installation disable the SMB service in your system, enable firewall and block SMB port's until it's all over.

6. ANALYSIS

1) PAYMENT
From the survey results and the literature, it can be concluded that only a very small portion of the victims actually pays the attacker. There are most likely multiple reasons for this, such as a deep distrust of the instructions to download the TOR browser [REF] and buy Bitcoins (both technologies with a seedy reputation). Furthermore, it seems likely that a significant portion of the victims do not possess the necessary technical skills to install and manage these technologies, even if they did have the intention to pay.

2) TRANSFER
Victims which can, from the attacker's point of view, be seen as viable targets are a small subset of the total group of victims. Viable targets are victims who have lost important data, require the technical skills to make a payment and are also willing to do so. It can therefore be assumed that most ransomware distributors use a 'shotgun approach' in the hope of reaching some viable targets and, in process, create a lot of collateral damage. The role of Internet is also a pressing threat for easier spread of ransomware.

7. CONCLUSION

This paper will provide the awareness of ransomware, especially for older peoples. With the increasing use of internet, transfer of ransomware is easy. In company environments, the lack of awareness among the employees is confirmed because of latest attack. Lastly, from the possible solutions will ensure that an internet user will be stay safe and far away from ransomware.

8. FUTURE SCOPE

As this paper will provide enough countermeasures for the ransomware, but in this fast internet world new attack may introduce at any moment. So, in future as the new attack introduces we will back with the countermeasures of it too.

9. REFERENCES

[1] Chris Moore, "Detecting Ransomware with Honeypot techniques," *2016 Cybersecurity and Cyberforensics Conference*

[2] Rhythima Shinde, Pieter Van der Veeken, Stijn Van Schooten, Jan van den Berg. "Ransomware: Studying Transfer and Mitigation," *2016 International Conference on Computing, Analytics and Security Trends (CAST)*

[3] L. Kelion, "Cryptolocker ransomware has 'infected about 250,000 PCs'," BBC News techology, 2013. [Online]. Available: http://www.bbc.com/news/technology-25506020. [Accessed 2016].

[4] G. O'Gorman and G. McDonald, "Ransomware: a growing menace," Symantec Corporation, 2012.

[5] B. N. Giri, N. Jyoti and M. AVERT, "The Emergence of Ransomware," AVAR, Auckland, 2006.

[6] J.-L. Richet, "Extortion on the internet: the rise of crypto-ransomware.," Harvard , 2016.

[7] A. Bhardwaj, G. Subrahmanyam, V. Avasthi and H. Sastry, "Ransomware: A rising threat of new age digital extortion.," in *arXiv* preprint arXiv:1512.01980, 2015.

[8] X. Luo and Q. Liao, "Awareness education as the key to ransomware prevention.," *Information Systems Security*, vol. 16, no. 4, pp. 195-202, 2007.

[9] A. Gazet, "Comparative analysis of various ransomware virii," *Journalin computer virology*, vol. 6, no. 1, pp. 77-90, 2010.

[10] M. Fossi, G. Egan, K. Haley, E. Johnson, T. Mack, T. Adams, J.Blackbird, M. Low, D. Mazurek, D. McKinney and P. Wood, "Symantec internet security threat report trends for 2010," Symantec, 2011.

[11] B. Foster and Y. Lejins, "Ehealth security Australia: The solution lies with frameworks and standards.," 2013.

[12] J. C. a. E. A. B. Hernandez-Castro, "UK has little to be proud of assurvey reveals sorry state of European cybersecurity," University of Kent, 2015. [Online]. Available: https://kar.kent.ac.uk/51071/1/uk-haslittle- to-be-proud-of-as-survey-reveals-sorry-state-of european cyber security-37505. [Accessed 2016].

[13] K.-K. R. Choo and R. G. Smith, "Criminal exploitation of online systems by organised crime groups," *Asian journal of criminology*, vol. 3, no. 1, pp. 37-59, 2008.

[14] K. Gradon, "Crime science and the internet battlefield: Securing the analog world from digital crime.," *Security & Privacy, IEEE*, vol. 11, no. 5, pp. 93-95, 2013.

[15] T. Zhang, H. Antunes and S. Aggarwal, "Defending connected vehicles against malware: Challenges and a solution framework.," *Internet of Things Journal, IEEE*, vol. 1, no. 10, pp. 10-21, 2014.

[16] https://www.wired.com/.../wannacry-ransomware-hackers-made-real-amateur-mistake...