A Brief Study on Ransomware Attacks and Information Security

Paras Vishwakarma[1] Rohit Sharma[2]

[1,2]MS Cyber Law and Information Security, Barkatullah University, Bhopal, Madhya Pradesh, India

Abstract— In recent times, Computer Systems, Mobile devices as well as Internet connectivity have become an indispensable necessity of our daily routine. With the growing use of computer systems, cyber platforms and digital media by individuals and organizations, it is quite common to store important business related documents, company records and personal information in the hard drives or other digital medias (ie. External hard drives, pen drives etc.). On one hand, digital storage of transaction records and information provides us with greater ease of access, revision and manipulation of the information but on the other hand it poses serious threat to the information if a strong security framework is not in place or common security practices are not followed by the user. Figure 1 presents the number of internet users across the globe as per the data from www.internetworldstats.com [1]. Recent attacks of Wannacry, Petya, BadRabbit, DoubleLocker android and NotPetya ransomware brought the attention of the global community towards the rising threat of cyber extortion through the utilisation of ransomwares.

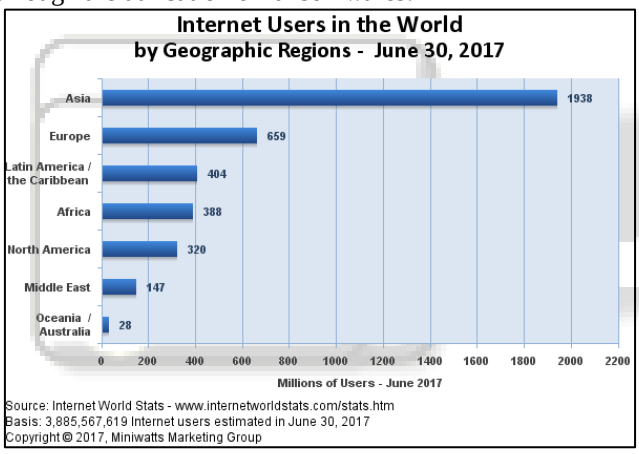

Fig. 1:

Key words: Ransomware, Cybercrime, Crypto Currency, Internet Security, Data Protection, Information Security, Security Techniques

I. INTRODUCTION

Ransomware is a type of malicious programme or malware delivered as a Trojan payload through infected websites, malicious or rogue software or e-mails and prevents or limits access to the data in the victim's computer either by locking the computer system or by encrypting the data or part of information [2]. After attacking the computer system, it flashes a banner demanding a ransom usually in virtual currency (ie. Bitcoin etc.) or prepaid cash vouchers in lieu of decrypting the files and/or unlocking the computer.

In May 2017 Wannacry ransomware attacked computer systems running on Microsoft's Windows Operating System [7]. Severity of this attack can easily be seen through the figures as more than 2,30,000 computer systems throughout the globe got affected by it and consequently in June 2017, many private and government organisations got hit by Petya ransomware which caused severe damage [3]. Computer systems of British Parliamentarians and India's largest container port Jawaharlal Nehru Port Trust (JNPT) also got hit by Petya ransomware. These incidents also highlight the threat to the internal security of the country. According to a report published by Beazley, a provider of data breach response insurance, the attacks of ransomware will double in 2017[6].

There are number of crypto-libraries widely available, so it is relatively easy to produce a ransomware [3]. With the frequent change of attack pattern and deployed algorithms as well as ever evolving methods of delivery, most of the attacks get successful before antivirus companies can analyse the samples and produce update definitions for the malware. Because of this reason, ransomwares now pose a far greater danger to the security of information. Since some data is more important than other, so it can be easily ascertained that attack of ransomwares poses different level of risks to different persons and organisations. According to a study by Bitdefender, half of the victims, depending on the importance of information and the time and resources required to recover the data seized by the attack, resorted to payments to the attackers [2] which even does not guarantee the fulfilment of promise of unlocking/decrypting files by the attacker. This provides the ransomware business with massive amounts of money which further used to fund cybercriminal activities. As per a study conducted by SentinelOne, now the industry spending more on safeguarding their system against attacks from Ransomwares [5].

Rest of this paper is organized in the following manner. Types of ransomewares and its attack methods are briefly described in Section 2. Preventive and curative measures in Section 3. Finally, several concluding remarks are given in Section 4.

II. TYPES AND METHOD OF ATTACK

The methods of Ransomware spreading are similar to those of malicious code Trojan horse [5] which contains malicious routine and present itself as a normal program. Ransomware intrudes into users' devices in the similar manner as Trojan horse. Then it restricts the normal use of the system in various ways such as locking the device or encrypting core system files etc. It is mainly classified into the following three types: Scareware, Device Locker type, and Crypto type [6]. Figure 2 depicts a simple graphical representation of a ransomeware attack as provided in the wall street journal after the attack of Petya ransomeware.

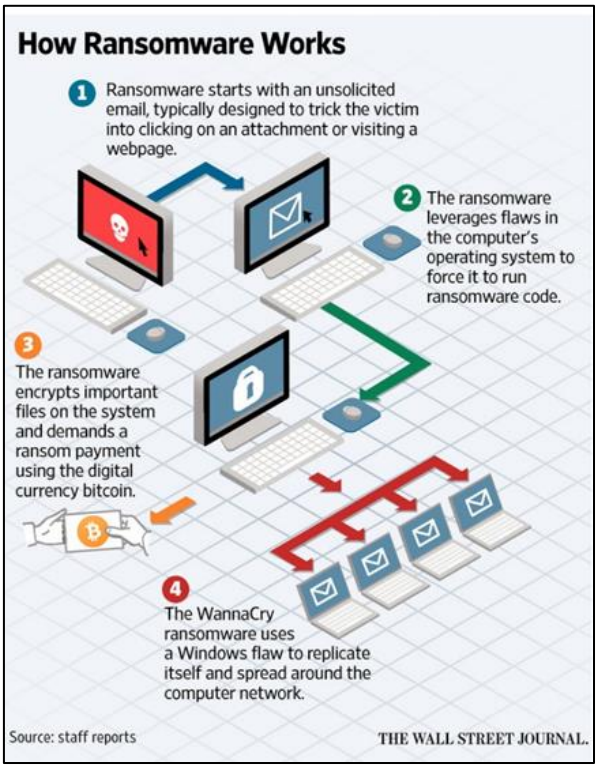

Fig. 2:

Figure 3 shows a basic classification of ransomwares. Based on the attack pattern, Ransomwares can be classified as [2],

a) Scareware
b) Device locker
c) Crypto Ransomware

Scareware intimate users that the device has been infected with malicious codes. It prompts the user to purchase fake antivirus programs to treat them. It finally extorts money from the user.

Lock-Screen or Device Locker Ransomwares attack start with victim downloading the malware through e-mail attachment or by visiting infected websites or through malicious applications which carry the ransomware code as payload. Ones downloaded, the malware, by taking advantage of system security vulnerabilities, executes itself and lock the device and demand payments to unlock the system. Attacker can also masquerade the lock screen message to replicate the warning from a law enforcement agency like Police or FBI.

Crypto Ransomware imitates a similar attack pattern as Device locker type but rather than blocking the access to the computer system, it encrypts all or parts of data stored in the hard drive. It than asks for payment through virtual currency or prepaid vouchers to decrypt the files. Use of virtual currency for the transactions made the attacker anonymous on the network and apprehending the attacker becomes virtually impossible. Crypto variant is the most serious type of ransomware. It prevents the use of important files or access to them in your device through encryption. It then uses encrypted important system resource as the bargaining chips and coerce users to deposit the ransom to a virtual account to decrypt the locked resources.

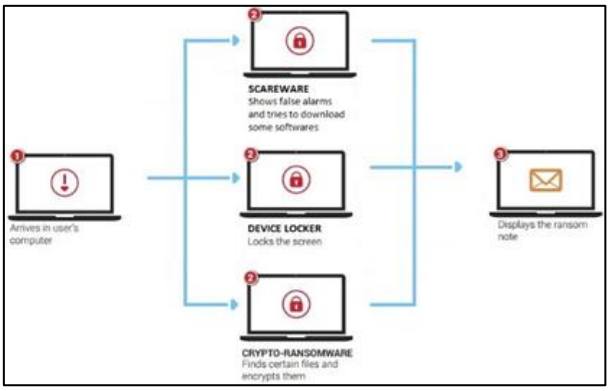

Fig. 3:

Ransomware intrudes into users' system and causes damage to them in various ways. For example, CryptoLocker encrypts files in the PC and makes them inaccessible to the user. Reveton impersonates messages from law enforcement agencies such as FBI. While SimpleLocker targets users with android OS smartphone. This ransomware poses sever security threats to cloud computing environment as it can render the basic infrastructure of information system inaccessible or useless.

Crypto Ransomware imitates a similar attack pattern as Device locker type but rather than blocking the access to the computer system, it encrypts all or parts of data stored in the hard drive. It than asks for payment through virtual currency or prepaid vouchers to decrypt the files. Use of virtual currency for the transactions made the attacker anonymous on the network and apprehending the attacker becomes virtually impossible.

III. So what actions should we take

As we can understand that combating a threat from ransomware is more of a preventive action rather than taking corrective measures afterwards. An attack from a ransomware can be negated by following general security practices such as,

a) Frequent backups.
b) Installing and properly configuring a firewall.
c) Use of security products which also involves internet security and antivirus.
d) Proper browser configuration with link and attachment scanners.
e) Implementation of IDS (Intrusion Detection Systems)
f) Avoid opening attachments from unknown e-mail addresses and visiting websites or links designated as unsafe by link scanner.

IV. Conclusion

The cyber extortion committed using ransomwares now poses a greater risk to the resources, information and reputation of the organisations as well as becoming a hazard to country's internal security. Increasing frequency of attacks using ransomwares only adds to the severity of the same. In this paper we have discussed about the threats presented by Ransomwares to the data resources, the research data available from various sources that exhibits the severity of ransomware attacks and the steps which should be followed in order to protect our personal information from the attacks.

REFERENCES

[1] Interne tworlds tats statistical data of internet users worldwide(http://www.internetworldstats.com/stats.htm)
[2] Bitdefender-Ransomware-A-Victim-Perspective Pg.8 (https://download.bitdefender.com/resources/files/News/CaseStudies/study/59/Bitdefender-Ransomware-A-Victim-Perspective.pdf)
[3] https://en.wikipedia.org/wiki/Ransomware
[4] https://www.symantec.com/connect/blogs
[5] Ransomware research data and summary (https://go.sentinelone.com/rs/327-MNM-087/images/Data%20Summary%20-%20English.pdf)
[6] Beazley breach insights January 2017 (http://www.beazley.com/news/2017/beazley_breach_insights_january_2017.html)
[7] Cyber-attacks Expected to Spread Monday as Europol Fears Computer Systems Simply Won't Start (http://www.zerohedge.com/news/2017-05-14/least-200000-victims-europol-fears-computers-simply-wont-start-monday-after-unrivall)
[8] Symentec white-paper on ransomeware (http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf)
[9] A brief history on wannacry ransomeware attack 2017 by Savita Mahurle and Manisha Patil (http://ijarcs.info/index.php/Ijarcs/article/download/4021/3642)
[10] Ransomeware : A research and personal case study of dealing with this nasty malware by Azad Ali (http://iisit.org/Vol14/IISITv14p087-099Ali3400.pdf)

