International Journal of Engineering Applied Sciences and Technology, 2017
Vol. 2, Issue 4, ISSN No. 2455-2143, Pages 117-120
Published Online February-March 2017 in IJEAST (http://www.ijeast.com)

CRYPTOLOCKER STRATEGY FOR RANSOMEWARE ATTACK – A REVIEW

Vikram Kumar
Department of Computer Science
Gurukul Vidyapeeth Institute of Engineering & Technology

Siddhant Ujjain
Department of Computer Science
Gurukul Vidyapeeth Institute of Engineering & Technology

Abstract - Computer Technology has grown and increased its size and complexity from time to time. In modern era, Computer has become a vital part of our life. We store our critical data and confidential information in Computer system. To secure it we use variety of security measures available to us like Antivirus, Firewall, UTM and similar devices. Even after adopting requisite security measures, we cannot conclude that our data in a system is secure from attackers.

Attackers have developed a way to compromise data on a victim's system by locking their system and prevent them from login into system. For unlocking systems attackers demand money in form of Bit coins. This kind of malware is Ransomware or Cryptolocker.

The paper will discuss about basics of Ransomware, how it works? who all are targets?, prescriptive guidance for Prevention, Mitigation and Recovery from Ransomware attack.

Keywords: - Ransomeware, Bitcoins, Impact of Ransomware

I. INTRODUCTION

The term ransomware is very popular in field of cyber security. The first case of ransomware dates back to 1989, with the appearance of a Trojan called PC Cyborg. This replaced the AUTOEXEC.BAT file, hid the folders and encrypted the names of all the files on the C drive, rendering the system unusable. The user was then asked to "renew their license" by paying $189 to the PC Cyborg Corporation., in order to obtain a repair tool even though the decryption key could be extracted from the code of the Trojan.

Ransomware is a malicious program that infects a computer and then locks it preventing user access to their computer or their data unless a ransom is paid. According to Internet Security Threat Report (2016) by Symantec, it indicates 35% growth in crypto-style ransomwares during the year 2015. Symantec has categorized ransomware as "An extremely profitable type of attack". This profitability is attracting more hackers into this business.

II. RANSOMWARE ATTACK STATEGIES

- Exploit kits are one way to hack users en masse. Criminals will typically purchase advertising space, allowing them to host banner ads on various sites. Advertisements themselves contain exploit kits that execute inside a user's browser when they detect certain vulnerabilities. These then get downloaded and install ransomware in turn. This strategy, known as a drive-by-download, can infect hundreds of people with just a single advertisement.

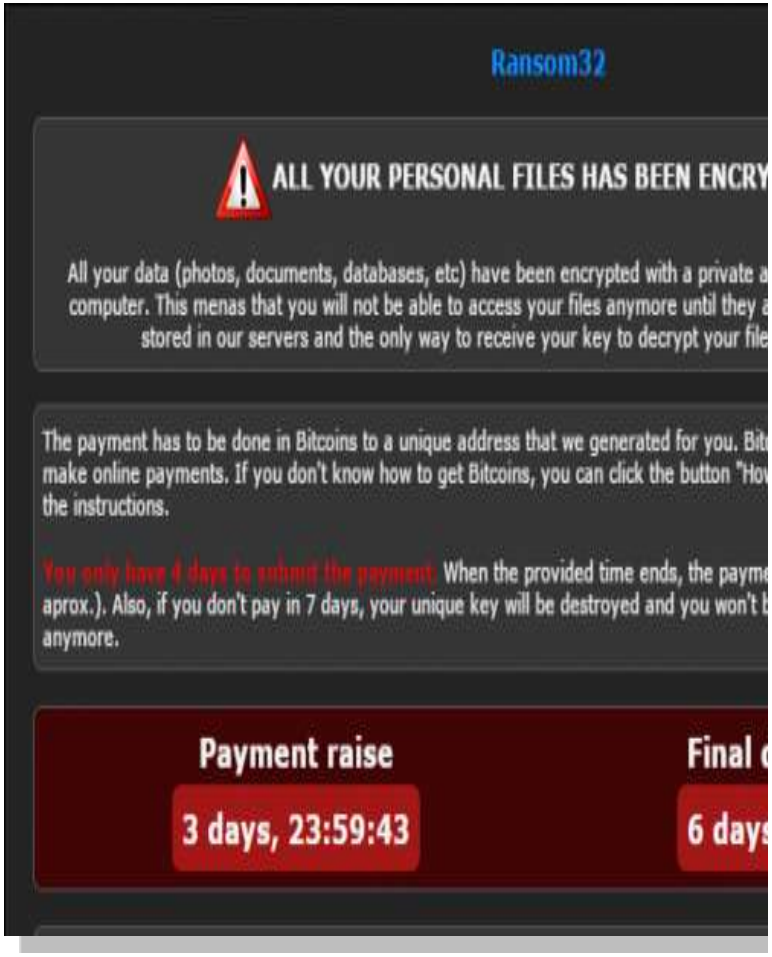
- Spear phishing campaigns are another way to target either individual users, or large classes of users within a single enterprise. This happens because many users will still download and enable macros on suspect Word documents.

- An emerging category of malware, finds specific unpatched vulnerabilities to exploit. They can use penetration testing tools to seek out known vulnerabilities.

- More concerning infection technique is through compromised remote access servers. Hackers can launch brute force attacks to gain access to

International Journal of Engineering Applied Sciences and Technology, 2017
Vol. 2, Issue 4, ISSN No. 2455-2143, Pages 117-120
Published Online February-March 2017 in IJEAST (http://www.ijeast.com)

systems connected to internet, and then use privilege escalation techniques to gain admin rights to servers with sensitive information. Once they have control of these high-profile systems, they can hold data for ransom. It also works as a key logger by capturing all Internet activity, credit card number, net banking password etc.



III. IMPACT OF RANSOMWARE

After dipping in the first quarter of 2015, overall ransomware infection numbers began to climb in the fourth quarter, spiking in October and November 2015, and again in March 2016.

Ransomware is designed for direct revenue generation. The four most prevalent direct revenue-generating risks include misleading apps, fake antivirus scams, locker ransomware, and crypto ransomware.The top six countries impacted by all types of ransomware in 2015 are the United States, Japan, United Kingdom, Italy, Germany, and Russia.

The average ransom amount is US$300. The favored payment method for locker ransomware is payment vouchers and for crypto ransomware, it's bit coins. In the past 12 months, 64 percent of binary-file-based ransomware detected have been crypto ransomware while binary-based locker ransomware made up the remaining 36 percent.

IV. RANSOMWARE TYPES

There are two main forms of ransomware in circulation today:

- Locker ransomware(computer locker): Denies access to the Computer or device

International Journal of Engineering Applied Sciences and Technology, 2017
Vol. 2, Issue 4, ISSN No. 2455-2143, Pages 117-120
Published Online February-March 2017 in IJEAST (http://www.ijeast.com)

• Crypto ransomware (data locker): Prevents access to files or Data. Crypto ransomware doesn't necessarily have to use Encryption to stop users from accessing their data, but the vast Majority of it does.
They are designed to deny us access to something we want or need and offer to return what is rightfully ours on payment of a ransom. Despite having similar objectives, the approaches taken by each type of ransomware are quite different

V. PAYMENT OF RANSOMWARE

Ransom payment has always proved a challenge for cybercriminals, who need a method that is easily accessible to victim and easily convertible to cash but also untraceable. Previously attackers relied largely on payment vouchers.

The rise of Bit coin and other crypto currencies provided an alternative that operates outside the traditional financial system.

Although not wholly anonymous, Bit coin movements can be obfuscated by moving through chains of wallets and tumbler services.

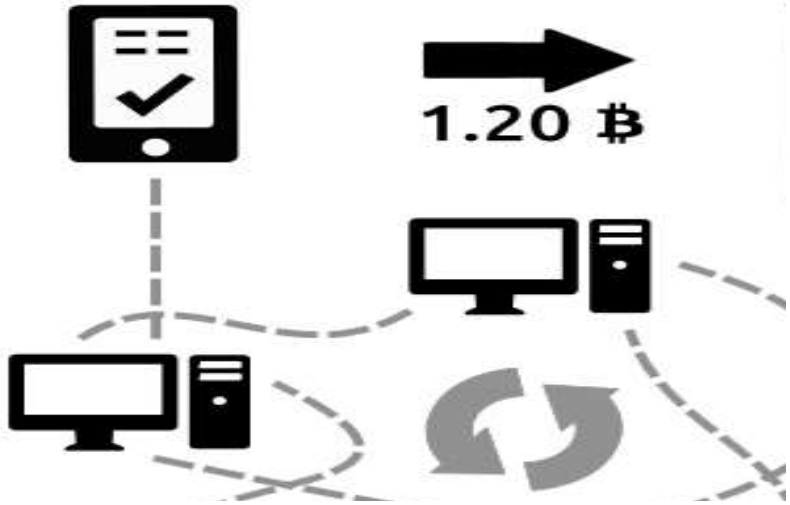
Bit coin wallets are free and disposable, meaning attackers can generate a new, unique wallet for each infection, making it more difficult for law enforcement to follow all earnings. Widespread public awareness of Bit coin also means that victims may be less suspicious of

The **crypto currency**, so are more likely to buy bit coins and pay the ransom.

- ✓ **1 Bit coin = 73938.58 Indian Rupee (According To New Market Report)**

Mechanism of using bit coins

As a new user, one can get started with Bit coin without understanding the technical details. Once you have installed a Bit coin wallet on your computer or mobile phone, it will generate your first Bit coin address and you can create more whenever you need one. You can disclose your addresses to your friends so that they can pay you or vice versa. In fact, this is pretty similar to how email works, except that Bit coin addresses should only be used once.



VI. PREVENTION FROM RANSOMWARE

We can reduce the ransomware attack by applying following measure:-

- The Maximum ransomware attacks are through phishing and spam email. So keep aware on the scam email in the enterprise or government sector where data is very critical network administrator should follow latest trend and technology.
- 44% attacks in last year were due to the unpatched code. So it is require for user to update their system and its application at regular interval.
- Backup your data on the regular basis so that if any attack is launch on the system you can back up your data.

VII. CONCLUSION

Nowadays ransomware attack is affecting user at very high pace, its profitability is attracting more hacker into the business. Cyber criminal now attack smart phones and latest technology like IOT (Internet of Things).In future it will become major threat to privacy and confidential data. Attacker not only encrypts the system but also kept a copy of data which they will be used for blackmail the victim in future. We need to understand the value of our personal data, realize the risk associated with it and actively devise ways to track, monitor and secure personal data interactions and transactions by using Confidentiality, Integrity and Availability principle.

VIII. REFERENCES

- Research paper by Carl Saiyed"cryptolocker"https://issa.org
- Research paper by Shafqat Mehmood "Enterprise Survival Guide for Ransomware Attacks"
- http://www.computerhope.com/jargon/r/ransomwa.htm
- https://support.symantec.com/en_US/article.HOWTO124710.html
- http://www.pcworld.com/article/2084002/how-to-rescue-your-pc-from-ransomware.html
- https://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx
- https://heimdalsecurity.com/blog/what-is-ransomware-protection/
- https://www.theguardian.com/technology/askjack/2016/jul/28/how-can-i-remove-ransomware-infection