© 2019 IJSRST | Volume 6 | Issue 1| Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology
DOI :https://doi.org/10.32628/IJSRST

Ransomware : A Severe Cyber Security Threat in The Digital Era

Satyendra Sharma[1], Prof. (Dr.) Triveni Singh[2]
[1]Senior Manager (IT), Cyber Crime Monitoring Cell, Fraud Risk Management Division, Head Office, Punjab National Bank, New Delhi, India
[2]Indian Police Service, Superintendent of Police, Auraiya District, Uttar Pradesh, India

ABSTRACT
Ransomware is a very severe cyber security threat since its inception. Ransomware has grown to be one of the biggest problems in the era of information technology. It is a type of malware which blocks a computer or encrypts the data and demands money in the form of virtual currency like Bitcoin for restoration of the functionality. Basically, two types of ransomware are found. First is encrypting ransomware which encrypts files using advanced encryption algorithm and another is locker ransomware which locks your computer system. Normally, crypto ransomware uses combination of both encryption techniques symmetric and asymmetric for encrypting the data. Ransomware threats are becoming more prevalent in enterprises. The purpose of these threats is quite simple. They are attempting to extort money from their victims with promises of restoring the functionality or restoring encrypted data whatever. But there is no guarantee that after paying the ransom you will give access to your computer system or restore files again.

Keywords: Ransomware, Bitcoin, Cryptocurrency, Cyber Crime, Cyber Security, Encryption, Public Key, Private Key

I. INTRODUCTION

At present, ransomware is the biggest concern in the digital world. Many countries have been affected by massive ransomware cyber-attack. Ransomware is a type of malware which either blocks a computer system or encrypts the files and demands ransom in the form of virtual currency such as Bitcoin for restoring the functionalities. In some cases, the name or logo of law enforcement agency is appeared so that user can believe that the police are involved.

Ransomware is a type of malware that infects a computer and restricts a user's access to the infected computer. This type of malware, which has now been observed for several years, attempts to extort money from victims by displaying an on-screen alert. These alerts often state that their computer has been locked or that all of their files have been encrypted, and demand that a ransom is paid to restore access [1].
As per Symantec, the concept behind ransomware, a well-known form of malicious software, is quite simple: Lock and encrypt a victim's computer data, then demand a ransom to restore access. In many cases, the victim must pay the cybercriminal within a set amount of time or risk losing access forever. And since we're dealing with criminals here, paying the ransom doesn't ensure access will be restored.

Ransomware is the online form of the bully's game of keep-away. The bully could hold your personal files hostage, keeping you from your documents, photos, and financial information. Those files are still on your computer, right in front of you, but they're encrypted

now, making them unreadable. In 2017, the average ransom demand was US$522 a high price to pay for getting your own property back [2].

They are attempting to extort money from their victims with promises of restoring the functionality or restoring encrypted data whateverRansomware can prevent you from accessing your computer system.

- It holds your computer or files for money (ransom).
- Encrypt files so user cannot use them.
- Prevent certain applications from running (Such as web browser).
- Ransomware demands money (ransom) to get access to your system or files.

Older versions of ransom usually claim (false) that you have done something illegal with your computer system and that you have fined by enforcement agencies like police etc.Newer versions of ransom encrypt the files on your computer system so that you cannot access them, and then demand ransom to decrypt your files.

Types of Ransomware:

There are different types of ransomware. However, all of them prevent you from using your computer system and/or ask you to pay ransom so that you can use your computer system or files.

They can target any computer users (like personal computers, corporate network, servers etc.)

Basically, two types of ransomware are found.

Encrypting ransomware (Data Locker): It incorporates advanced encryption algorithms. Encryption ransomware encrypts your computer files and demand money (ransom) for providing decryption key so that content can be decrypt in readable form.

Examples: CryptoLocker, Locky, CrytpoWall, Cerber, CTB Locker, Cryptodefense, Simplocker.

Fig.1

Locker ransomware (Computer Locker): It locks your computer system due to which you are unable to access desktop and other applications. In this case, data are not encrypted, but the attackers demand for money (ransom) to get access to your computer again. It is also called Lockscreen Ransomware which shows a full-screen message that prevents you from accessing your computer.

Examples: Win locker.

Fig.2

II. METHODS AND MATERIAL

Mode of Payment of Ransom:

Generally, mode of payment is in the form of Bitcoin. Bitcoin is a virtual currency and known as cryptocurrency which is easily convertible into other currencies like dollar, euro etc.

Bitcoin:

Cryptocurrencies have become a global phenomenon, as Thomas Carper, US-Senator said: "Virtual currencies, perhaps notably Bitcoin, have captured the imagination of some, struck fear among others and confused the heck out of the rest of us [3].

Bitcoin is an innovative payment network and a new kind of money. Bitcoin uses peer-to-peer technology to operate the payment network. There is no central regulatory authority or banks are involved in payment process. Bitcoin payment network manages transactions including issuing of Bitcoin. Bitcoin is open source and its design is public. Nobody owns or controls Bitcoin payment network but everyone can take part.

Fig.3

Bitcoin is a digital cryptocurrency made up of processed data blocks used for online and brick-and-mortar purchases. Because bitcoins are limited and their value is determined by market forces, bitcoins are also traded like stocks on various exchanges. Relatively new and experimental, bitcoin is described as "the first decentralized digital currency [4]."

Sources of Ransomware:

- Visiting unsafe or suspicious websites.
- Opening email attachments from unknown sources.
- Opening of spam email.
- Clicking on malicious links at web like emails, social sites etc.
- Using external drive.
- Using outdated anti virus
- Non updated security patches

File Encryption Techniques:

Normally, crypto ransomware uses combination of both encryption techniques symmetric and asymmetric.

Symmetric Key Encryption (Private Key Encryption):

In symmetric encryption technique, a single key which is called private key (secret key) is used to encrypt and decrypt the data. Using symmetric key encryption technique, ransomware can generate a key on the infected computer system and send this key to the command and control server (attacker's system). Ransomware also can request a private key from the command and control server (attacker's system) before encrypting the files on victim's computer. In this technique of encryption attacker needs to ensure that the private key is not available on the victim's computer after encrypting the files, otherwise the victim might be able to decrypt the files himself without paying the money (ransom).

Symmetric encryption technique is faster than asymmetric encryption and typically uses 256-bit AES key.

The main problem with symmetric key encryption is how to securely get the secret key (private key) from the message sender in secured way and keep them securely. For this reason, an asymmetric key encryption is now often used which is popularly known as the public key infrastructure (PKI).

Asymmetric Key Encryption (Public Key Encryption):

In asymmetric key encryption technique, two keys are used. One is public key and another is private key which is used to encrypt and decrypt the data respectively. In this technique, anyone can encrypt the data using the public key (which is made public and distributed widely and freely) but only the holder of the paired private key can decrypt the data.

Using asymmetric encryption algorithm, Crypto ransomware may encrypt the files on victim's computer system with the public key and attacker may keep the private key for himself. The attacker does not need to worry for the protection of public key because for decrypting the files related private key is required.

Asymmetric encryption is slower than symmetric key encryption.

More advanced crypto ransomware typically uses a combination of both symmetric and asymmetric encryption techniques. The variants that use asymmetric encryption may also generate specific public-private key pairs for each infected computer.

Different Approaches of Crypto Ransomware for Data Encryption:

Downloaded Public Key Approach: Cryptodefense ransomware (Encrypts the file with extension .cryptodefense) uses combination of both encryption techniques symmetric and asymmetric. Cryptodefense ransomware uses AES (Advanced Encryption Standard) which is a symmetric encryption algorithm to encrypt the victim's data. The 256-bit AES key is generated on the victim's computer system which encrypts the file. After that the AES key is itself encrypted with a 2048 bit RSA asymmetric public key (Public key is downloaded from the command and control server of attacker). Subsequently, encrypted AES key (secret key) is stored in each encrypted files on the computer of victim. Whereas attacker controls the RSA private key on the command and control server. This private key is required to decrypt the file on victim's computer.

Weakness of this approach is that if command and control server (attacker) is unable to reach for downloading the RSA public key, in this case the encryption processes will not success.

Advantage of this approach is that the attacker can use a different RSA asymmetric key pair for each infection. Exposure of a single RSA private key will not allow any other victims to unlock their files.

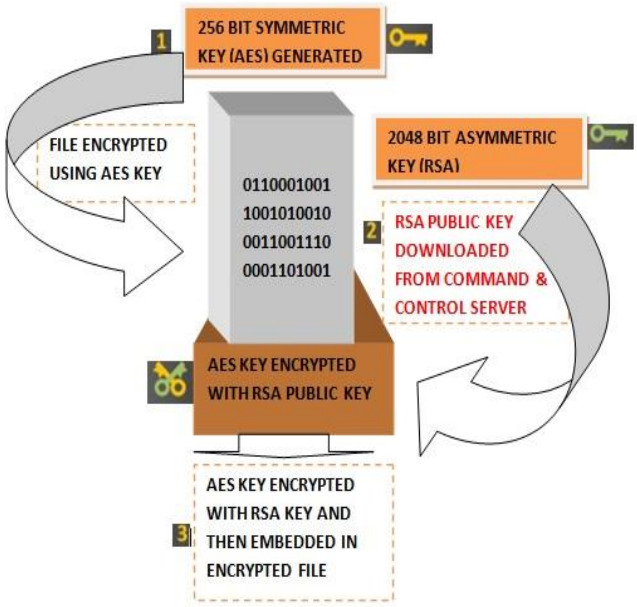

Fig.4

Embedded Public Key Approach:

CTBLocker ransomware (Encrypts the file with extension .CTBL or .CTB2 or other ransom extensions) also uses combination of both encryption techniques symmetric and asymmetric with different approach. An embedded public key is included in CTBLocker ransomware for RSA asymmetric encryption process. The command and control server (attacker) keeps the corresponding private key. CTBLocker ransomware

uses AES (Advanced Encryption Standard) which is a symmetric encryption algorithm to encrypt the victim's data. The 256-bit AES key is generated on the victim's computer system which encrypts the file.. After that the AES key is itself encrypted with a 2048 bit RSA asymmetric public key (Public key is embedded in CTBLocker ransomware). Subsequently, encrypted AES key (secret key) is stored in each encrypted files on the computer of victim. Whereas attacker controls the RSA private key on the command and control server. This private key is required to decrypt the file on victim's computer.

Weakness of this approach is that if attacker uses the same public key for encryption, then if the first user obtains the private RSA key, he could be share the private key with other victims for decrypting their files.

Advantage of this approach is that the ransomware can start its file encryption process without internet access.

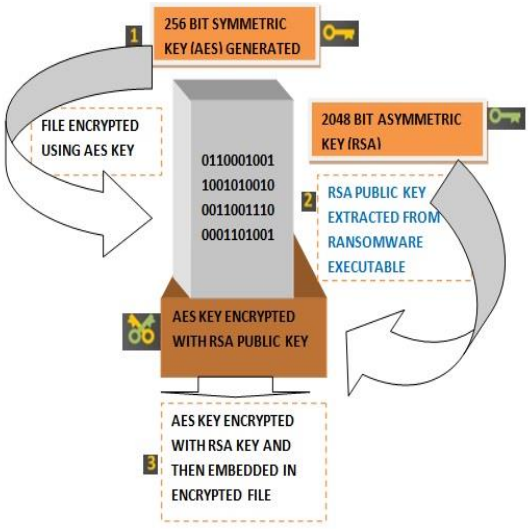

Fig.5

III. RESULTS and DISCUSSION

Report: 99% of ransomware targets Microsoft products

The explosive growth of ransomware is bad news for Windows users. Some 99% of ransomware attacks are targeting Microsoft products, according to a report from security firm Carbon Black

The report was conducted by Carbon Black's Threat Analysis Unit (TAU). The team looked at more than 1,000 ransomware samples, which they then split into 150 families. Essentially, they found that most attackers were looking for a way to make fast money with a combination of relatively unsophisticated tools delivered in a sophisticated way, the report said.

Attacks like WannaCry and NotPetya definitely brought more attention to the rising ransomware threat. However, the report said, many organizations are distracted by these major threats, to the point that they are forgoing basic cybersecurity measures that defend against smaller, more common attacks.

"Businesses appear to be focusing too greatly on next-generation threats while being unable to defend against the current era of basic malware. What's more, the public attention to new threats distracts many organizations from the ability to tool their environments and train their staff to respond to basic attacks," the report said [5].

Recognizing the warning signs: Ransomwareand email phishing:

Email still remains the top attack vector for all malicious activity, says Adenike Cosgrove, cybersecurity strategist, EMEA, Proof point. She says the easiest route for cyber criminals is to exploit the vulnerability of humans "through simple yet sophisticated social engineering tactics". She explains: "Cybercriminals have found new ways to exploit the human factor — the instincts of curiosity and trust that lead well-intentioned people to play into the hands of the attacker. This could be in the form of a disguised URL or seemingly benign attachment, but

all it takes is one click and the ransomware can take hold immediately."

The majority of ransomware is spread via massive spam campaigns involving hundreds of thousands of emails sent daily, says Dick O'Brien, threat researcher at Symantec [6].

Case Study:

The WannaCry attack put ransomware, and computer malware in general, on everyone's map, even those who don't know a byte from a bite. Using exploits from the Equation Group hacking team that were made publicly available by the Shadow Brokers, the attackers created a monstrosity - a ransomware encryptor able to spread quickly over the Internet and local networks.

The four-day WannaCry epidemic knocked out more than 200,000 computers in 150 countries. This included critical infrastructure: In some hospitals, WannaCry encrypted all devices, including medical equipment, and some factories were forced to stop production. Among recent attacks, WannaCry is the most far-reaching [7].

In March 2018, the computer network of the City of Atlanta was hit by the SamSam ransomware, for which the city projected costs of $2.6 million dollars to recover from. Rendition Infosec founder Jake Williams noted that the city's infrastructure had fallen victim to the NSA-developed DoublePulsar backdoor in late April to early May 2017, which ZDNet notes was over a month after Microsoft released patches for the vulnerabilities. Although the City of Atlanta did not pay a ransom, the attackers behind the SamSam malware netted nearly $6 million since the attack began in late 2015, according to a July 2018 report at ZDNet. That report also indicates that the attackers continue to gain an estimated $300,000 per month [8].

In September 2018, Ransomware attacks forced gate information screens offline at Bristol Airport for two days. Airport officials decline to pay ransom demand and manually restore all affected systems. Functionality has been restored to all screens after two days.

Flight information screens were blacked out over the weekend at the Bristol Airport in the UK.

Airport officials blamed the incident on a ransomware infection that affected the computers running the airport's in-house TV screens displaying arrival and departure flight information.

The infection appears to have taken root on Friday morning, local time, according to the Bristol Airport's social media accounts, who warned passengers all weekend to arrive early and allot extra time for the check-in process.

For all Friday, Saturday, and the subsequent night, airport officials have been using paper posters and whiteboards to announce check-in and arrival information for flights going through the airport.

Speaking to local press over the weekend, airport officials said they did not intend to pay the attacker's ransom demand and opted to take down their systems while they serviced affected computers.
No flight delays have been reported because of the cyber-attack, officials said.

Functionality to affected systems was restored on Sunday morning, local time. Airport screens worked on Sunday [9].

Preventive Steps from ransomware:

- Do not click on a link on a webpage or in an email or in a chat message unless you absolutely trust the page or sender.

- Do not open email attachments from unknown sources.
- Delete any suspected spam immediately.
- Keep your spam filter on.
- Do not click on the link unsolicited advertising and offers.
- Wireless network should be encrypted.
- Do not visit unsafe or suspicious websites.
- Check the URL in the browser address bar and look for any spelling mistakes or unexpected names.
- Before giving any personal or financial details, check that you are on a secure link like https.
- Firewall should be on.
- Update Anti-virus regularly.
- Update windows for security patches and bug fixes on regular basis.
- Update your browser on regular interval.
- Install Anti-spyware tools.
- Block browser pop ups.
- Keep your passwords strong and secret.
- Keep backup of important files in a separate disk/DVD.
- Create restore point in your computer system.

IV. CONCLUSION

- A number of ransomware groups are using advanced attack techniques which are similar to the many cyber-attacks.
- The ransomware-as-a-service (RaaS) means their own ransomware can be obtained by the cyber criminals.
- New ransomware families are discovered and gradually increasing
- According to Kaspersky's Ransomware and Malicious Cryptominers 2016-2018 report, ransomware infections have fallen 30% over the past 12 months as cryptominers infections have increased 44.5% over the same time period.

In this research, it is found that the interest of cyber criminals is increasing in hitting businesses with targeted attacks using ransomware.

V. ACKNOWLEDGEMENT

Disclaimer: "All content presented in this paper is personal view of authors. This content cannot be treated as an official view of the authors."

VI. REFERENCES

[1]. United States Computer Emergency Response T eam (October 2014) "Crypto Ransomware" https://www.us-cert.gov/ncas/alerts/TA14-295A

[2]. Symantec (2018) "What is ransomware? And how to help prevent it" https://us.norton.com/internetsecurity-malware-ransomware-5-dos-and-donts.html

[3]. Thomas Carper, US-Senator (January 2019) "What is Bitcoin Cryptocurrency" https://www.openaccessgovernment.org/what-is-bitcoin-cryptocurrency/42401/

[4]. Techopedia "Bitcoin (BTC)" https://www.techopedia.com/definition/27193/bitcoin-btc

[5]. Conner Forrest "Report: 99% of ransomware targets Microsoft products" (Sep. 2017) https://www.techrepublic.com/article/report-99-of-ransomware-targets-microsoft-products/

[6]. Kate O'Flaherty (Aug. 2018) "How To Survive A Ransomware Attack -- And Not Get Hit Again" https://www.forbes.com/sites/kateoflahertyuk/2018/08/17/how-to-survive-a-ransomware-attack-and-not-get-hit-again/#46a0ec926cd3

[7]. John Snow (Nov. 2018) "Top 5 most notorious cyberattacks" https://www.kaspersky.com/blog/five- most-notorious-cyberattacks/24506/

[8]. James Sanders (Oct. 2018) "Ransomware: A cheat sheet for professionals" https://www.techrepublic.com/article/ransomware-the-smart-persons-guide/

[9]. Catalin Cimpanu (Sep. 2018) "Ransomware attack blacks out screens at Bristol Airport" https://www.zdnet.com/article/ransomware-attack-blacks-out-screens-at-bristol-airport

Cite this article as :

Satyendra Sharma, Prof. (Dr.) Triveni Singh, "Ransomware : A Severe Cyber Security Threat in The Digital Era", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 6 Issue 1, pp. 211-218, January-February 2019. Journal URL : http://ijsrst.com/IJSRST196120