# RANSOMWARE - A GROWING THREAT ON FINANCIAL INSTITUTIONS

**[1]Lucky Narayani, [2]Dr. Priyanka Sharma**

***[1]Student M.Tech(Cyber Security), [2]Professor(IT)***

*[1,2]Department of Information Technology*

*[1,2]Raksha Shakti University, Ahmedabad, India.*

## ABSTRACT

*Ransomware attacks are growing day by day.cyber criminals use this weapon like a money making machine.The Ransomware had targeted many Universities, hospitals, businesses, healthcare and organizations, banking sector and even police departments.Hackers demand the payment in Bitcoin (BTC) because of the decentralized nature of bitcoin and not easily traceable by law enforcement agencies.According to security researchers ransomware will be one of the fastest-growing attacks in cyber crime. Ransomware is more stealthy, with some recent variants completing their dirty work without making a single call to the Internet. The present research paper discusses Ransomware whole round i.e. Ransomware origin, different variants, infection process, Future threats, and Mitigation.*

**Keywords** *: Ransomware, Bitcoin, Variants, Cryptography, Encryption, Payment*

## I. INTRODUCTION :

Ransomware is one of the trending topic in the cyber world. Every day a new variant of ransomware comes into the market. The attackers are making ransomware for windows, android and Linux platforms.
The quick payment system of Ransomware encourages cyber criminals to collect the cash and develop a more tempting framework for the next target. TOX adopted a "ransomware-as-a-service" business model. It allows even inexperienced cybercriminals to create their own customized malware and, using the TOX website (residing on the TOR network), to manage infections and profits[1].

## II. RANSOMWARE ORIGIN AND ITS WORKING PROCESS

The AIDS trojan, The first ransomware was originally developed by biologist Joseph Popp. Popp passed 20,000 infected floppy disks out at the 1989 World Health Organization's AIDS conference. In the attacking phase,the attacker compromised the victim computer using some exposed system vulnerabilities.the attacker uses some kind of trojan and malware to infect the victim system and then find different types of files extension names as .txt, .doc, .rft, .ppt, .cgi, .dsw, .gzip, .zip, .jpg, .key, .mdb, .pgp .pdf. , .chm, .cpp, .asm, .db, .db1, .dbx.after getting these type of important files and encrypt the files. Later, the attacker sends the victim an email ransom or pop-up window demanding for the encryption key that unlocks the frozen files[2].

## III. KNOWN VARIANTS

The malware uses different varieties and new methods to infect the system.the security researchers are continuously upgrading their standards to prevent against these type of attacks.its a cat and mouse game between ransomware developers and security researchers. Some of the known families of Ransomware are discussed used in this section:

**A. Crypto-Locker:** It had been used to distributed through Gameover Zeus Botnet which was isolated in Operation Tovar in late May-2014.this malware encrypts the system using RSA public-key and the private key is stored on malware C & C servers.it propagated via existing botnets and spam emails.

**B. Crypto wall:** It has first appeared in 2013.the variants are delivered through Exploit kits and spam emails.it uses the AES encryption and C&C servers and TOR network for bitcoin payment.it's a file-encrypting ransomware that uses the public key for encryption.

**C. CTB-LOCKER:** CTB-Locker Stands for "Curve-Tor-bitcoin-Locker".it uses Elliptic Curve Cryptography(ECC) similar like RSA encryption to encrypt the files.it is spread through exploit kits like Rig and Nuclear.it does need C & C server to encrypt and decrypt the files.


**FIG-1:** CRYPTO WALL RANSOMWARE PAYMENT PAGE

**D. Spora:** Spora has first appeared in January 2017.it spread through an email attachment which contains HTA files inside.these files use a double extension like PDF or DOC to fool the users.it uses a powerful encryption engine and a payment site which is different from other ransomware.it is an example of ransomware as a service (RaaS).

**E. Mamba:** Mamba is a bit further than Petya ransomware .it is not only encrypts your important files but also encrypts your MFT including each sector, the Operating system, and all application.it install a disk cryptor software in your computer which is a Full Disk Encryption Software that encrypts every sector.

**F. Tesla Crypt:** In earlier, Tesla crypt affect gameplay data for specific computer games like call of duty and Mine craft.it is propagated via Angler Adobe Flash exploit.it uses the assymmetric encryption in its recent variant which is impossible to break.it can also encrypt PDF, JPEG and DOC files.

**G. Locky:** It uses .locky extension to encrypt the files.it scrambles all your personal files and remove any shadow files used for backup and infected any other removable media and servers attached to that system and bad guys have decrypting key on dark web.

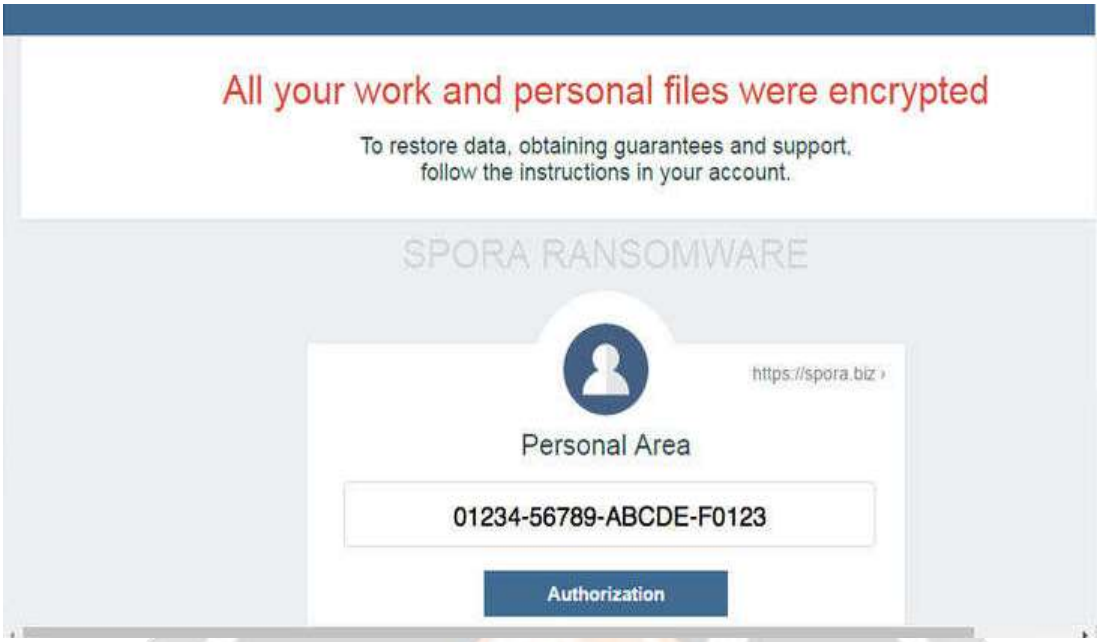


**FIG – 2 :** SPORA RANSOMWARE DISPLAY PAGE

## IV. FINANCIAL LOSSES

The prime target of ransomware is Businesses because it contains sensitive data and other information and so they most likely to pay the ransom demand to resume their operations.In February 2016, Horry County school district in South Carolina paid a big ransom to the attacker to decrypt their files.the further attacks on Hollywood Presbyterian Hospital Medical Center where the hospital paid 40 bitcoins to attackers. Ransomware is spread through established Botnets like Dridex, Dyre and Ramnit Botnet which targeted the Financial Institutions and banking sector. According To the FBI, ransomware is on pace to be a $1 billion a year crime this year. The overall annual cost of global cyber crime was thought to be $3 trillion in 2015 and this is expected to double to $6 trillion a year by 2021[3].

In earlier, the ransomware variants accepted payment through wire transfer and premium rate text messages now they found a new way of cryptocurrencies which is more secure and not easily trackable by law enforcement.the Bitcoin are purchased through the darknet using Tor, it provides anonymity because Bitcoin is a decentralized currency, some variants of ransomware also accept Dogecoin(DOGE) and Litecoins(LTC). According to a report of Kaspersky ransomware attacks on 136,532 Android users which are four times greater than the previous twelve month periods. Both new and old variants caused a total of $209 million in monetary losses to enterprises. Ransomware attacks found in the first half of 2016, such as BEC scams, originated from e-mails 58 percent of the time[4].

## V. TRENDING TARGETS - IOT AND MOBILES DEVICES

The growing risk of ransomware is now targeting the internet of things(IOT) devices. ransomware can modify the physical functions inaccessible. For example, if ransomware attacks on a thermostat it can increase the heat to high level unless a ransom is paid.smart cars and smart cities will be the major target. In the upcoming year, the cybercriminal will threat the medical devices and wearable devices. Ransomware developers are always trying to make the most money for the least effort. they are usually trying to exploit the Windows or Adobe Flash or Internet. But IoT devices are a new challenging area for hackers. According to McAfee Labs reports Consumer electronics

continues to grow at a rapid pace. One area in particular is the consumer element of the Internet of Things, which is expected to hit roughly 1.8 billion devices by 2019[5]. In the rising popularity of android devices, the attackers are trying to develop malicious apps and infecting the android devices for making money. there are a number of ransomware attacks are rising in recent years on android devices. Ericsson, predicts there could be as many as 6.4 billion smartphone subscriptions by the end of 2020, almost one per person[6]. The majority of both locker and crypto ransomware are a big concern for mobile users. Most of the Mobile ransomware shows a screen that claims to come from the FBI and NSA and demands ransom — from $50 to $300. Some variants can capable stealing money, modify data, and, of course, locking the device. A new variant of Cyber Police ransomware which shows a lock screen of American national security agency in the popup display and shows a note to pay $100 USD in violation of rules. it is propagated via malicious apps and spam emails. Another ransomware like Porn ransomware which is spread through fake text messages that contain a malicious link of adult website which contains a malicious video file. when the user clicks on that link the ransomware compromised that device and shows fake alerts of child pornography related messages.

## *VI.* RANSOMWARE REMEDIATION STRATEGIES

The first step to mitigating a ransomware threat is to implement a comprehensive cybersecurity.There are some following steps can be taken to prevent from ransomware threat.

- Do not click on any link that contains some malicious app.
- Do not try to open any download attachment from an unknown email.
- Keep your Backup data on multiple devices.
- Use some good antivirus and update it regularly
- Do not click on any greedy Advertisement on websites.
- Awareness and information security training among users should be first and foremost.
- Patch your operation system vulnerabilities and application versions to reduce the attack surface.
- Download the apps from trusted place like google play store and ios store.
- Turn off the Unknown sources option of the device.
- Install a good firewall and IDS/IPS in your company

The Ransomware growth is rising exponentially so The European Police agency Europol has joined forces with police and cyber security and Europol announced the initiative, dubbed NO More Ransom, Which is backed by technology giant Intel, Kaspersky Lab and the Netherlands police to mitigate the ransomware threat.

## VII. FUTURE THREATS

The next generation of ransomware will be highly sophisticated.Ransomware developers are trying to make crypto worm which is similar like SQL SLAMMER and Conficker.In fact, according to security researchers at Cisco Talos, today's newest ransomware, SamSam, is a harbinger of a new wave of more malicious, tenacious and costly ransomware to come[7]. Crypto worm contains self-propagating nature of worms and malware of the past.The new ransomware like Ransom32 which is programmed in Powerware(Powershell) and javascript have capabilities to evade detection of many antivirus products by using the legitimate process on the system. The attackers behind ransomware use the many spam evading techniques to bypass spam filtering system. The attackers next target will be Supervisory Control and Data Acquisition (SCADA) systems, home routers, traffic lights, web cameras and IOT devices. We will see new attacks in 2017 like a Mirai-style botnet installing ransomware on all of CCTV cameras and home internet routers.

## VIII. CONCLUSION:

Every day now we hear the news describing enterprise or organization hacked by ransomware attacks. The reason behind growing threat of ransomware is the lack of security awareness among IT staff and users. It is difficult to recover data from the system which is encrypted with strong cryptography.Availability of easily getting Ransomware like TOX which is freely available on the dark web to download opens the gate for script kiddies to making money.there is no currently a bullet proof solution is available for ransomware prevention even FBI said

just pay the ransom. Ransomware will be a challenging for both researchers and security professionals.Clearly, the ransomware is profitable for cyber criminals and it will continue to grow in future.

## . IX. REFERENCES:


1. Krzysztof Cabaj and Wojciech Mazurczyl,"Using Software-Defined Networking for Ransomware Mitigation : the Case of Cryptowall",Proc. Of the IEEE Network 30(6) August 2016 (https://www.researchgate.net/publication/306474307_Using_Software Defined_Networking_for_Ransomware_Mitigation_The_Case_of_CryptoWall).

2. Qinyu Liao,"Ransomware: A Growing Threat To SMES" (http://www.swdsi.org/swdsi08/paper/SWDSI%20Proceedings%20Paper%20S400.pdf).

3. The Cost Of Ransomware Attacks:$1 Billion This Year (http://www.zdnet.com/article/the-cost-of-ransomware-attacks-1-billion-this-year).

4. Ransomware-Causes-3Billion-Worth-Of-Losses-In-H1 (http://khaleejtimes.com/technology/ransomware-causes-3billion-worth-of-losses-in-h1).

5. Intel Corporation. "McAfee Labs 2017 Threat Predictions" ( https://www.mcafee.com/us/resources/reports/rp-threats-predictions-2017.pdf).

6. Symantec Corporation. "Intel Security Threat Report."Volume 21,April 2016. **(**https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf**).**

7. Meet-The-CryptoWorm-The-Future-Of-Ransomware **(**https://threatpost.com/meet-the-cryptoworm-the-future-of-ransomware/117330**).**