IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.11481

THE GROWTH OF TERRORISM FUNDING WITH THE HELP OF RANSOMWARE ATTACKS AND THE RATE OF INCREASED CRIME WITH IT.

Palash T. Sole[1], Sheetal A. Wadhai[2]

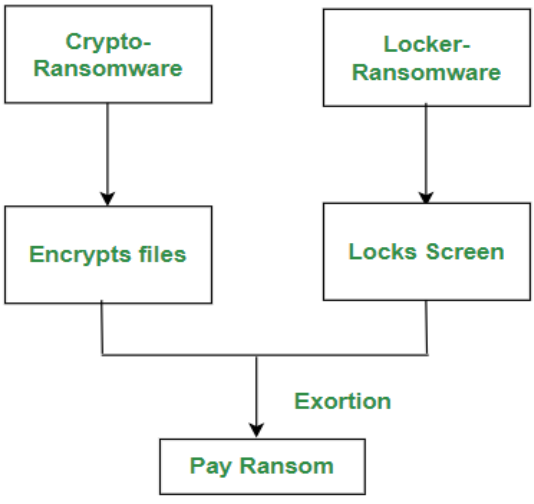
Department of Computer Engineering, Universal College of Engineering and Research, Pune

Abstract: Security was a big deal for a long time. Viruses, malware, and ransomware are other problems seen by the practitioner but as an advantage by the terrorist organizations. This paper shows the use of ransomware by terrorist organizations and the preventive methods against them. In the evolution part, the paper provides s study from the first ransomware to the current days. The study shows the light on various kinds of infection performed by ransomware including data infection and infected machines. Different attackers made choices to target various attacks; the paper provides a sight of various target types of ransomware. This paper tries to demonstrate a few ransomware attack case studies to show the problem created by various ransomware as an example. After an attack, what a victim should do after infection is also discussed at the end of the paper. How people can save their system and what are the safety measures to save the system from ransomware, are also discussed by the researcher. At the end of the paper, the researcher points out a few steps to save systems and data.

Keywords - Ransomware, Security, Attack, Cryptowall, Crypto lock, Wannacry, Terrorist Organizations.

I. INTRODUCTION:

Cybersecurity was always a challenging issue since arising from computers. It has been increased with the internet improvement of internet facilities. Many kinds of cyber-attacks are currently performed by cybercriminals. Apart from the other threat issues, the spreading of ransomware is an illegal business. It is inflow for the network since 2005 but for personal computers started from the year 2015. Crypto ransomware is the category of malware that can encrypt data of the victim machine whereas locker ransomware locks the machine, thus in the second kind user not able to use their machine. Ransomware can be understood just as the first one is like a lock that applies on the home of the victim's goods by which he can enter the but cannot use the items of their own whereas the second case is that someone locks the gate of the home of a victim by their unknown lock in this case victim is not able to enter in their own house. Paper represents threats of ransomware in terms of IoT infrastructure. Few famous cases are enlisted here as:



IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

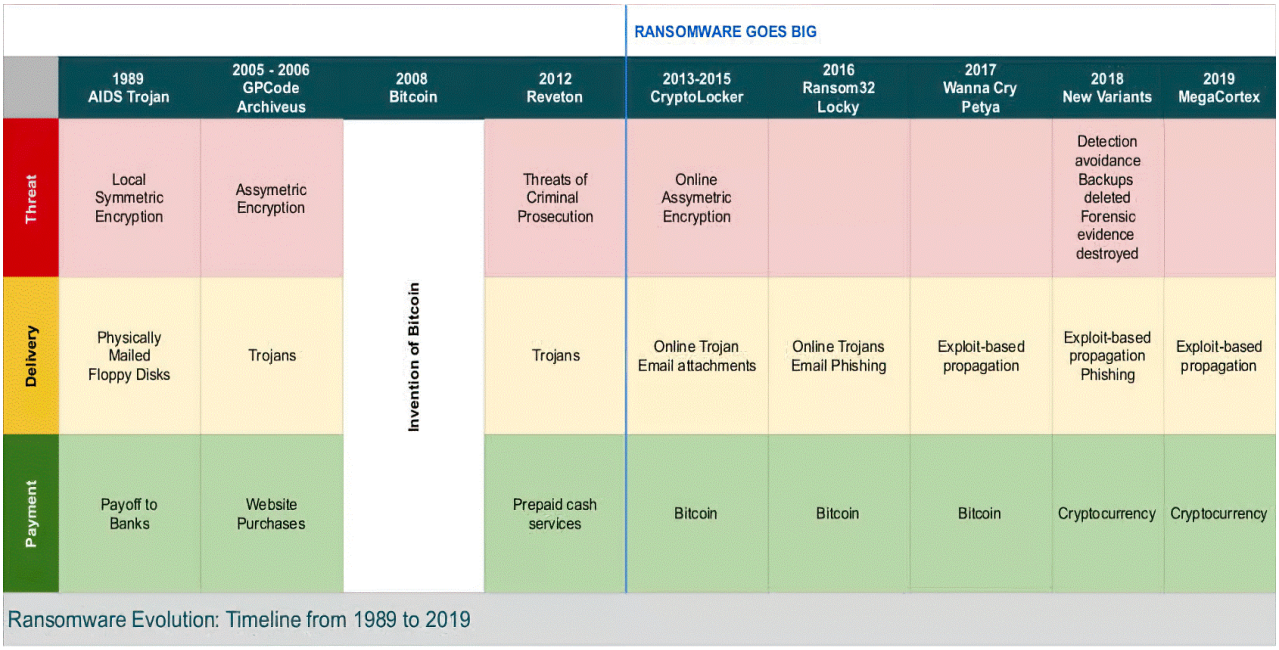
DOI: 10.17148/IJARCCE.2022.11481

Attackers have developed a way to monetize files already on a victim's computer. They accomplish this through n-encrypting select files and then charging for access to the key. This type of malware has pawned new classification, crypto-ransomware, but is more commonly known by the name of the most prevalent version, Crypto Locker, or its variants Tesla Crypt and Cryptowall.

Famous Cases:

- In August 2016, Bournemouth University successfully attacked and corrupted files by ransomware 21 times during the previous 12 months.
- In April 2016, A Network Hospital of MedStar Health in Maryland was attacked and blocked from working by the Sam Sam ransomware.
- In February 2016, Hollywood Presbyterian Medical Center was attacked by Locky ransomware and disrupted working for two weeks until they paid 40 Bitcoin (about $17,000) to recover its files.

A study of the famous cases shows that ransomware attacker makes the target a system of professional bodies. After seeing the importance of the awareness about ransomware a study on ransomware was started. The evolution of ransomware has shown in section II with its division before ransomware as a service and after ransomware as a service. This section indicates the basic characteristics of ransomware and indicates a light on new ransomware introduced in 2017. Section III shows various kinds of infections performed by ransomware after an attack. After this, section IV classifies various targets for a ransomware attack it also shows a situation of a machine after an attack.



Ransomware Evolution: Timeline from 1989 to 2019

EVOLUTION OF RANSOMWARE:

In 1989 attacks of ransomware started and got typical to crack with the expansion of type. Ransomware attacks got very common after being included as a service in form of ransomware-as-a-service. As per Ronny and Max , we have classified evolution in two parts as given in Tables 1 and 2: A. Before Ransom as a service: Ransomware with the name AIDS Trojan had come into the existence in 1989 that was also famous as a PC cyborg. This virus was created by Joseph L. Popp and distributed through a floppy disk.

Table 1: Evolution of ransomware before Ransomware-as- a-service

YEAR NAME	DESCRIPTION
May 2015, ransomware-as-a-service	• Using a TOR website, attackers could create ransomware for free. • The site handles the payment and takes a 20 percent cut of the ransom.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.11481

2015, Tor sites	• As the name implies, it targets Linux systems. It encrypts both data files and files associated with web applications.

Table 2: Evolution of ransomware after Ransom-as-a-service

September 2015, Lockerbie	• It infects Android systems and changes the PIN.
Nov,2015 Linus.Encoder.	• In was discovered by Drewe, a Russian computer security firm.
November, the fourth iteration of Cryptowall	• It includes a modified protocol to help avoid detection. • Additionally, it alters the file names when it encrypts files, making it harder to determine what files were encrypted.
January 2016. JavaScript-only	• It is a ransomware-as-a-service. • multi-platform attack, including Linus and MacOS X.
April, Petya	• Makes the whole hard disk inaccessible until the ransom is paid. • It does this by overwriting the master boot record (MBR) of the infected computer. Without the MBR, the operating system cannot reconstruct the unencrypted files.
Xbot, Feb 2016	• To target Android devices in Australia and Russia. • Tries to steal online banking details.
Jigsaw, 2016	• Embeds an image of the clown from the Saw movies into a spam email. ransom payment of $150, according to Webroot.
Not Petya, 2017	• It comes with a fake software update and harms systems of more than one hundred countries.

The year 2011 was very tough for the internet user because of the attack by bulk ransomware. This year more than 30,000 samples were found in two starting quarters while 60000 ransomware samples were attacked in the herd. the again year 2015 was found as a golden year for ransomware criminals. This year a new kind of crypto locker was introduced while a TOR website started ransomware as a service.
This website provided ransomware on the commission of 20%.

A. After Ransom-as-a-Service:

After providing ransomware on rent or commission, the frequency of ransomware attacks has increased, that is why the researcher classifies the evolution into two parts before and after ransomware.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.11481

Samsam.exe	**MD5 : a14ea969014b1145382ffcd508d10156 SHA1: ff6aa732320d21697024994944cf66f7c553c9cd Type :PE32 executable Size: 218.624 bytes**
Del.exe	**MD5 : e189b5ce11618bb7880e9b09b09d53a588f SHA1: 964f7144780aff59d48da184daa56b1704a86968 Type : PE32 executable Size : 155,736 bytes**
Selfdel.exe	**MD5 : e189b5ce11618bb7880e9b09b09d53a588f SHA1: 964f7144780aff59d48da184daa56b1704a86968 Type : PE32 executable Size : 155,736 bytes**

Few ransomware with initial characteristics

Other Ransomware is also tried to follow the same structure as wiasD5 And SHA1 while every criminal tried to make it tough to toughest. The rest of the paper organizes as section 2, which gives light on the evolution of ransomware yearly, whereas section three shows the stages of attack by ransomware.

B. Recent Ransomware:

WannaCry: It is just ransomware with a computer worm, On May 12, 2017, it is the first attack on the machines across the globe through a malicious link or by opening an infected mail. As p various newspapers, this ransomware, day sorted to have infected more than 200,000 computers in over 150 countries. It affected some old unpatched MS windows systems of those people, who did not perform security updating of the Operating system with the exact patch, as per the advisor of Microsoft that was released before 2 months by Microsoft on 14 March 2017 to remove a few vulnerabilities noticed by them.

III. INFECTION BY RANSOMWARE

Once infected, a user has four options:

- Pay the ransom
- Restore from backup
- Lose the files
- Brute force is the key

To brute force, the key would require factoring 617-digit numbers, which would take about 6.4 quadrillion years on a standard desktop computer.

3(a). Data on Infection

Symantec uses telemetry data to track ransomware infections by country. The rankings are shown in table 1 below. For the most part, criminals are targeting large or affluent countries. On the initial day ransomware was attacked on the Windows platform but these days it can infect Apple and Android systems, and even a few are also in the air to infect Smartwatches that come into the category of IoT devices. Now ransomware moving to IoT, as services moving from the Internet to the world. In the year 2016, SVG (scalable vector graphics) is a new method of a cyberattack. SVG files are a file that allows system code, such as JavaScript, to be embedded in the graphic. This code can be run through a browser. Few codes and techniques are also in the air to decrypt the files of the victim such as Popcorn Time allows free decryption of files of victims if infected.

3 (b). An Infected Machine

Dealing with ransomware is a costly job even if has backed up and not going to pay because correction of a system can takes days to weeks. So, after infection, a machine has limited options to operate. Ransomware does not destroy data. Rather, it locks up the data until a ransom is paid. Antivirus company AVG recommends the following steps:

Step 1: Run a full scan to find out the ransomware used.

Step 2: Copy the encrypted files to a USB drive so they can be decrypted on an uninfected computer.

Step 3: Use a tool to decrypt the files in the USB drive. AVG provides free tools for decrypting six Ransomware strains: Apocalypse, Bad Block, Crypt888, Legion, SZF Locker, and Tesla Crypt. When files are recovered in any way ransomware must be removed.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.11481

IV. TARGETS FOR RANSOMWARE

4(a).User wise:

The Average User: All age groups are considered a target to get ransom, but people who are not technical personnel pressurize easily. Attackers sometimes increase pressure by including a timer with the increment ransom amount. A solution of ransomware like Tesla crypt is coming in form of Tesla Decoder but for people who do not use through with the decoding of the encrypted file then ransomware can do its job even if it is easily decodable. Individual users are targeted because they pay ransom due to the fear of corrupted files and not having a backup for valuable data. On the other hand, organizational members due to business secrecy sometimes pay due to not having cybersecurity personnel. As per Symantec, 25% of home users have not had a backup, 55 % backup some files and only 25 % have regular backed up in a week. The rest only made backups sometimes.

Businesses: Businesses are on priority for ransomware because their systems are the house of the valuable database with sensitive data, important documents, and other information; in the meantime, they have the general system updated and tried to secure. Crypto ransomware focuses to target the corporate network or individual systems to be spread in the whole network.

Emergency Services: Ransomware targets these organizations also due to Multi-State Information Sharing and its importance by which it can pay the cost of delay in terms of lives. Most vulnerable emergency services are law enforcement, fire departments, and hospital chains. On the other hand, the healthcare sector is not a traditional target for a few years these have also been targeted including the example of Hollywood Presbyterian Hospital Medical Center which was infected with the Locky. ransomware.

Financial Institutions: The banking and finance sector is the frequent target of ransomware schemes including botnet-like problems. Dyre, Dridex, and Ramnit are botnets included especially for the banking sectors. Educational Institutions and religious organizations are also the favorite targets of ransomware criminals due to these having all the costly data with the least secure mechanism.

4(b). System wise: All kind of system is valuable to the user and might be a target for ransomware due to the profitability target system including:

Personal computers (PC): PCs are the current primary target of ransomware due to their easy compromise. These systems are generally updated OS and software. Ransomware variants are designed to target various OS, but windows systems are a soft target. Mobile devices: Ransomware is currently active in the air for smartphones also. Servers: An organization's servers and databases store all their critical information. Within a serve are an organization's documents, databases, intellectual property, personnel files, client lists listed other intangible resources. The compromise of one essential ever can hobble an organization. Despite their value, organizations regularly fail to secure, update, and patch the systems. This makes servers susceptible to lateral movement and attack. When a server is compromised, the organization goes into a panic. Even if the attack is a ransomware attack, there is a concern for reputational harm due to the perception of lost customer data. Even if the organization has a business continuity plan or disaster recovery plan, the amount of time necessary to revert to a redundancy system may be unacceptable.

PAYMENT METHODS:

Bitcoins are the first choice for criminals but in general we can say digital payment mechanism is the choice of criminals. Bitcoins: Bitcoins are a cryptocurrency that can be assumed as electronic coins. It allows people to transfer digital payments from one end to another. It is an easy system of payment due to not involving any financial institution in the process for any kind of activity as a mediator. To find out payment ransomware instructs victims as:

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.11481

Figure: Crypto locker's message

Figure: Ransom message to pay

V. SAFETY METHOD

Mobile phone is also found attacked by ransomware as other machines, while data recovery from ransomware affected systems can be done by a forensic tool as per described by PH Rughani, who evaluated the practical over the android phones and found a better success rate on SD card than a phone. To deal with ransomware experts have given a few

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.11481

suggestions to use before and after infection as Step 1: Back-Up Step 2: Avoid all spam links if unknown. Use Adblockers can protect against malvertising. Turning off Java and JavaScript. Step 3: Patch and Block All the OS, browsers, and security systems should always be kept matched and up to date including third-party plug-ins, like Java and Flash. Step 4: Drop-and-Roll If a machine found the sign of infection, then to minimize the infection infected machine should immediately turn off, the network also should be turned off if this machine is on the network [1]. Based on case studies, to deal with ransomware, a few suggestions areas:

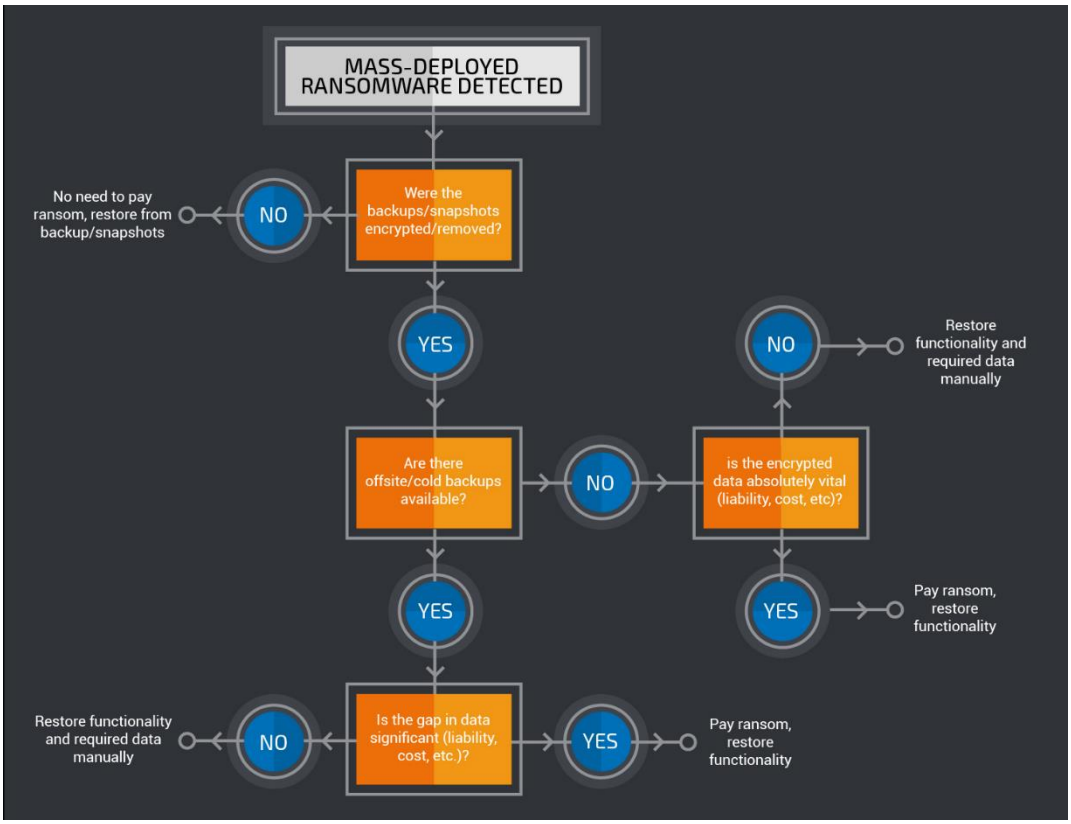


Figure 5: Flowchart to deal with ransomware

1. To save a system from ransomware attacks first step is to update the operating system, sometimes it requires patches thus installation of patches is the next step.
2. Do not use Operating System that is not supported.
3. Tasks of step 1 are meaningless if the system does not have any updated antivirus, so it is a suggestion that the system must have an excellent quality antivirus.
4. Cleaning spam folders must be the next step after the removal of all malware/spyware.
5. JavaScript files and website open option is risky so deactivate it at the end of all precautions.

VI. CONCLUSION FUTURE WORK

This work presents the working of ransomware by terrorist organizations with its working and suggestion to save computers from attack. It shows safety guidelines for ransomware that will be helpful to researchers as well as society to save data in near future. The review discusses a picture of the evolution of ransomware with its effects on the system, way of working, and tricks to save our data during the attack.

REFERENCES

[1]. R. Richardson and M. Nort, Ransomware: Evolution, Mitigation, and Prevention", International Management Review, Vol. 13, No. 1 2017.
[2]. An Osterman Research, "Best Practices for Dealing with Phishing and Ransomware SPON", White Paper Published September 2016.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.11481

[3]. C.Beek and A. Furtak, "Targeted ransomware No Longer a Future Threat: Analysis of a targeted and manual ransomware campaign", Advanced Threat Research, Intel Security, feb2016.
[4]. J. Wyke and A. Ajjan, "The Current State of Ransomware," A Sophos Labs technical paper December 2015.
[5]. WannaCry Response, Metasys, Johnson Control, June 2017.
[6]. WannaCry Ransomware Analysis, White paper, May 2017, Stream scan.