A study on Growing Challenges in different Platform Cybercrime: Ransomware Attacks

Atira Nair
Student Bachelor of Computer Science
School of Computer science and Applications
SANDIP UNIVERSITY, NASHIK.

ABSTRACT :----In present days, Rapidly developing malware samples stance a deliberate threat to cyber security, exclusively when they are not getting detected by security tools and techniques.Ransomware is a malicious program where the data on victim's computer is encrypted and some ransom is demanded before the ransomed data is decrypted and access returned to the victim.The cyber criminals often demand money in virtual currency, such as "bitcoins "so that their identity is hidden from the victim.Most common way of transmission of ransomware is through websites or spam emails. The content of the injected malware in webpages or emails usually claims that, the user has won the prize, or various offers that they get for free. The user clicks on the link that they receive through mails andthen downloads the malware,this way malware enters in system.

Index Terms: ---- Malware, Crypto locker, Bitcoin, Wannacry worm.

----------********----------

INTRODUCTION

Malicious programs can be divided into various groups such as: worms, viruses, Trojans, hacker utilities and other malware, in which ransomware come under the class of malware. All of the malicious programs are designed to damage the infected machine or othernetworked machines which consist of confidential data's.Most common way of transmission of ransomware is through websites or spam emails. The content of these affected webpages or mails usually includes that ,the user has won a prize, or some offers. The user clicks on the link they receive and download the affected links. One more common way of transmission is Trojan horse or as payload of any other malware.

There are several types of ransomware, depending on how they affect the system. One type of ransomware terminates the applications from working, like security software and website browsers. The second type is that the ransomware encrypts victim's personal files such as documents and pictures, preventing the access to them, unless a ransom is paid in exchange for the decryption key , and such type of ransomware is called as "crypto locker ".Removal of Ransomware is a difficult task business and the need to have a professional company is one that will help to ensure a safe and secure return to normal operations. Some of the vicious forms of Ransomware include: CryptoLocker, Cryptowall, CTB Locker,

Ransomware:

It is a malicious software program, whose inventor is unknown, but the notion of using public key cryptography for data breach attack was introduced in 1996b by Adam L Young and Moti Yung.It encrypts all data in a computer and blocks access to them, often this malware is seen in the form of email attachments and website link conning users to open it. Ransom is demanded for decrypting the files and if the victim doesn't oblige the files will be detected. The ransom is demanded to be paid in the form of digital currencies such as "bitcoins". The use of ransomware has become a trendsetter among unethical hackers looking for quick payout.

CRYPTOGRAPHY

Cryptography has become the most widely used method for maintaining computer security. However, cryptography often fails to live up to its claims while even the strongest cryptography has it limits. Thus, the only way to guarantee the security of computer systems is to prepare for future attacks. The systems must be designed in such a way that it should withstand more intelligent attackers, increased computational power and incentives to undermine a widespread system.

Once our system is secured,our computer files have the file extension ".WNCRYT ", victim computers then shows the message with a demand of some digital currencies to decrypt the files.

Ransomware communicability spreads

Cyber criminals use different techniques for getting personal data and infect a system with malware, asking some money to decrypt the data. For not being got system with any malware it's essential **to** keep your system up to date.

The most common ways used by cyber criminals to spread ransomware:

- Spam email which include malicious links or attachments;
- Internet traffic which leads to malicious websites;
- Websites that have malicious code injected in the web pages;
- SMS text messages
- We can also use botnets for malicious programs.

Process flow of Ransomware

The work as follow:

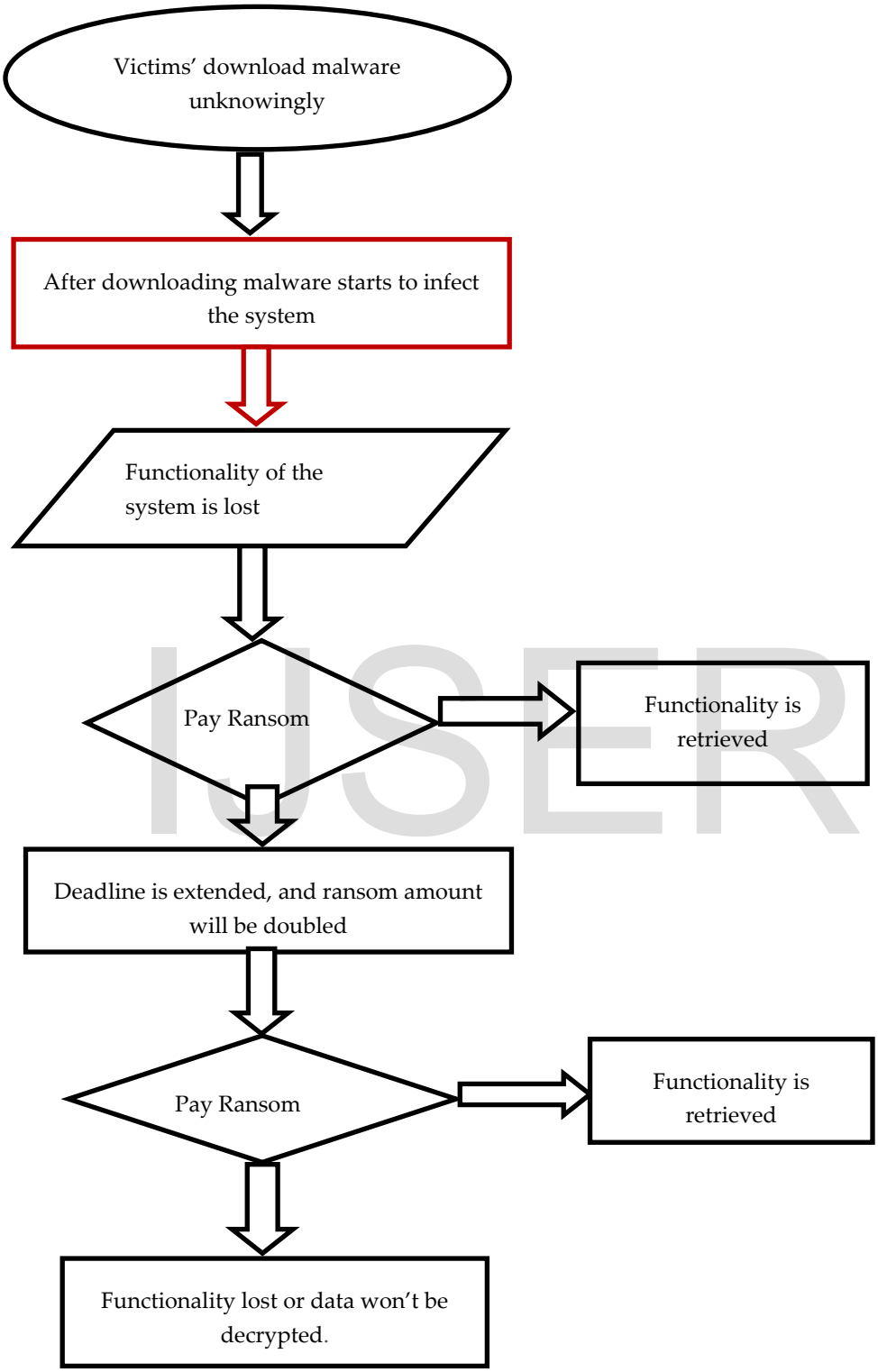
1. User unknowingly download the malware:
   The users download the malware through email attachments or links they receive in the mail or through the website which offers a temptation to the user by providing various offers .
2. Malware infects the system :
   After downloading the link which consists of malware our system will be get infected by encrypting our necessary files .We can understand that our system being get affected from malware by pop-up message that your system has been affected with malware.
3. Functionality lost and users read ransom note:
   After our system being gets affected by malware we can't use the necessary files in our system.
4. Pay Ransom :
   After malware is activated in our system the cyber criminals asks for the ransom in the form of bitcoins.Malicious programs can be divided into various groups such as: worms, viruses, Trojans, hacker utilities and other malware, in which ransomware comes under the class of malware.

All of the malicious programs are designed to damage the infected machine or othernetworked machines which consist of confidential data's.Most common way of transmission of ransomware is through websites or spam emails. The content of the ransomware injected webpages or emails usually claimsthat, they have got some prize, or some offers. The user clicks on the link that they receive through mails andthen downloads the malware, this way malware enters in system.

There are different types of ransomware, which depends on how severely they affect the functionalities of the computer. *One type* of ransomware terminates the applications from working, like security software and website browsers. The *second type* encrypts the userspersonal files as documents and pictures whose system have been affected with ransomware and preventing the access to these, unless a ransom is paid in exchange for the decryption key, and such type of ransomware is called as "crypto locker ".There is need for ransomware professional services to review, validate and confirm the safety and security of a system, never occurs.

Removal of ransomware is a difficult task business and the need to have a professional company is one that will help to ensure a safe and secure return to normal operations. Some of the vicious forms of Ransomware include:
CryptoLocker,Cryptowall, CTB Locker,

Process of Ransomware:



Bitcoins

Bitcoins,It is a cryptocurrency and used in payment system.It is the first decentralized digital currency.Bitcoins are created as a reward for the process "mining", which can be exchanged for other currencies, products, and services.The upgraded version of the bitcoin is called as Bitcoin cash(BCH), which is a peer to peer electronic money / a virtual money which features low fees as well as fast transaction time.

Ransomware Features

- It have a very strong encryption , that won't allow yourself to decrypt the files on your own
- It will be encrypting all kinds of files which includes files like documents ,pictures ,video, audio and other necessary files that we have.
- The victim cannot easily identify, which data was affected , since malware scrambles the file names.
- A different extension to the file will be added ,when the file is infected with ransomware.
- If our data has been encrypted , then it will display an image or a message.
- If file has been encrypted then it request payment in the form of bitcoins as the cryptocurrency is not easy to tracked by cyber security or law agencies .
- Usually the ransom amount will give some time limit.
- The ransomware can spread to other systems which will be connected to a local network which would create a further damage.

Types of Ransomware:

There are different types of ransomware, such as follows:

CryptoLocker: It came to action in 2013.The word CryptoLocker, much like Xerox, has become similar with the ransomware.

Crypto Wall: It became popular after the downfall of the Crypto Locker. Analyzing preliminary network traffic obtained by Maltester it was obvious thatthe whole communication is somehow encrypted. However, Crypto Wall uses domain names instead of direct IP addresses. That means it needs a DNS service to resolve his peers. In order to get more control over the communication process the Maltester's firewall was specially configured and fake DNS service provided. It records, blocks or redirects (if needed) the DNS requests.

- **Locky:** The malware is transmitted through email message in the form of voice .When we open, the audio is scrambled and the victim is forced to activate macros in order to read the attachment/files. When macros0 are enabled, it begins to encrypt a huge amount of file types.

- **Petya**: This type of ransomware encrypts entire system and ,overwrites the master boot record, which makes sthe operating system unbootable.

- **Spider**: It spread through spam emails across Europe. These kind of malware are hidden in Microsoft Word documents which will be installing the malware on the victim's system when it is downloaded. When these macros are activated, the malware begins to sencrypt the victim's data.

- **WannaCry**: This Ransomware hit among 150 countries. The Wannacryis known in the name as WCry ,as well as WanaCryptor and greatly affects Windows machines through a Microsoft exploit known as "EternalBlue".

Effect of Ransomware:

According to eScan antivirus report in the year 2017 India was the country which wasworstly affected by cyber-attack. In which, Madhya Pradesh was the worst affected region in the country with around 32.63% of total ransomware attacks ,followed by Maharashtra at 18.84% and then the Delhi which at third position with 8.76% share.

Companies like Nissan, railway companies of Germany, Russian Railways, Interior ministry, megaforTelephonic in Spain, which is a telecommunication company. At least 16 NHS organizations in UK were badly affected. Lots of colleges and students computer were worstly hit by the attack in China.

Vodafone - the well-known ISP were worstly affected.

WannaCry malware encrypts all the data and necessary files stored on the computer system of user, and it leaves only two files :The file which is used for instructing the user ,to tell what the victim should do next to decrypt the program.

Recover from Ransomware:

There are different methods for recovering from the malware:

1. **Disconnect the computer from the network:** If a system is affected with ransomware, then take it offline ,and pull the ethernet cord or shut off the Wi-Fi and then shut down the system.

   Ransomware can spread through a network, as sooner we disconnect any infected computers the better your chances are of containing the breach.

2. **Disable shared drives**: There are different varieties of ransomware, such as Locky, which will encrypt network and shared drives that are connected to the infected computer.If there is some ransomware infection, then take all of shared drives offline temporarily until network is cleaned out.
3. **Update and run your security software: Since** we have isolated the infected computer and alert users, and if there is any update to install for the security software, then install it and always run a scan on your device.
4. **Restore from backup (if possible) :** If a ransomware attack occurs then it will encrypt all files that the system have, there are three basic options:

   1. Pay the ransom
   2. Restore from a backup
   3. Cut your losses and nuke the computer

Advantages and Disadvantages of Ransom:

Pros

The ransom amount can be affordable as sometimes it will be of minimal value.

1. It takes time to restore the access to data / files.
2. It has a minimized adverse publicity.
3. We are not paying cyber criminals and trying to support the cyber crime.

Cons

There is no guarantee of restoration of data / access to data.

1. It offers an incentive that such attacks may continue.
2. Another disadvantage is that if you are not paying the ransom it will be a very time-consuming process to recover all the files that is there in the system from data backups.
3. Causes the disruption to business and users , whose system is affected with ransomware.

Most ransomware attacks need to be paid, in order to decrypt the files, which can be paid in the form of bitcoin, which is a cryptocurrency or virtualcurrency based on the block chain mode.

Protection from Ransomware

1. Do not pay the ransom; there is no guarantee that even after paying ransom we will be able to access our files again.

2. If we want to restore any impacted files, then backup it from a known good backup; restore it, so you can access it.

3. Never provide your personal information while answering an email or any unsolicited phone call, or even the text messages, because the phishers will try to trick to install malware.

4. Always use reputable antivirus software and a firewall, because by maintaining a strong firewall we can keep our files up to date and it provides more security.

5. Make sure that always systems and software are up-to-date with relevant patches.

6. While travelling, especially if you're using public wireless Internet, always make sure that use a trustworthy Virtual Private Network (VPN).

7. Always scan and filter on mail servers. Inbound e-mails should be scanned properly, as it may be containing threats and block any kind of attachment which would affect the system or can cause a threat.

Countries that affected with Ransomware:

Top 10 Affected countries:

1. India was affected with ransomware of 9.6% .
2. Russian Federation was affected with ransomware of 6.41% .
3. Kazakhstan was affected with ransomware of5.75%
4. Italy was affected with ransomware of5.25%
5. Germany was affected with ransomware of 4.26%
6. Vietnam was affected with ransomware of 3.96%
7. Algeria was affected with ransomware of 3.9%
8. Brazil was affected with ransomware of 3.72%
9. Ukraine was affected with ransomware of 3.72%
10. United Stateswas affected with ransomware of 1.41%

CONCLUSION

The purpose of this paper is to analyze and to make aware of what is ransomware is. Andits effects and how it can be prevented if a system is affected with ransomware malware. We come to the conclusion that WannaCry Ransomware Attack wars were the most terrificattack, which affected most of the countries and public sectors too. The most important source of ransomware virus is via phishing emails and the website links which contains the malicious program. So, even though the system is affected with ransomware by keeping backup up to date regularly, to an extent we can prevent this malware.

References

[1] Cabaj K., Gawkowski P., Honey Pot systems in practice, Przegląd Elektrotechniczny, 91 (2015), nr 2, 63-67.

[2] Cabaj K., Grochowski K., Gawkowski P., Practical Problems of Internet Threats Analyses, in: Theory and Engineering of Complex Systems and Dependability, Advances in Intelligent Systems and Computing, 365 (2015), 87-96.

[3] Cabaj K., Denis M., Buda M., Management and Analytical Software for Data Gathered from HoneyPot System, in: Information Systems in Management, 2 (2013), nr 3, 182-193.

[4] Cabaj K., Visualization as Support for Web Honeypot Data Analysis, w: Information Systems in Management, WULS Press Warsaw, 4 (2015), nr 1, 14-25.

[5] Ulrich Bayer, Andreas Moser, Christopher Kruegel, and Engin Kirda. "Dynamic analysis of malicious code," Journal in Computer Virology, vol. 2, pp. 67-77, 2006.

[6] Lim, C.; Ramli, K. "Mal-ONE: A unified framework for fast and efficient malware detection", Technology, Informatics, Management, Engineering, and Environment (TIME-E), 2nd International Conference on, (2014), 1 – 6.

[8] Mihai Christodorescu, and Somesh Jha, "Static Analysis of Executables to Dete
ct Malicious Patterns," Univ. of Wisconsin, Madison, US. (2006).

[9] Xu, M., Wu, L., Qi S., Xu, J., Zhang, H., Ren, Y., Zheng, N.: A similarity metric method of obfuscated malware using function-call graph. Journal in Computer Virology
, 9 (2013), Issue 1, 35-47.

[10] Chen X., Andersen J., Mao Z.M., Bailey M., Nazario, J., Towards an understanding of anti-virtualization and anti-debugging behavior in modern malware," IEEE International Conference on Dependable Systems and Networks, (2008), 177-186.