Injection, Execution and Infection Working of Ransom ware

M. Z. Shaikh, Sulakshana B. Mane

Abstract: ***Ransom ware is type of Cyber malware which is used by attacker to block the computer system until some ransom is paid by victim .It propagates by malicious email attachments, links offering free software internet downloads etc.During given time it has to pay money which is demanded by ransom ware. This paper indicates the introduction of Ransom ware. How it works and types, attack methodology and threat carriers of Ransom ware and preventative precautions***

Keywords: Ransom ware, locker, Encryption, Crime ware, Preventation

I. INTRODUCTION

Ransom ware it has been built upon two words "Ransom and Malware". To define Ransom ware is malware infection, which is caused by a malware program that infects, locks or takes control of a system by giving full control of the victim machine to the attacker and enables the attacker to demand heavy ransom to undo it. The attacker is empowered with full authorization to use the victim machine to extract heavy and continuous ransom and secondly to steal the confidential data lying in the machine. On utmost exploitation, this can also lead to network level infection, posing heavy loss to an organization. The Ransom ware is a leading threat to confidential information of the countries which need to be protected. There are many methods to avoid them but very few methods to bypass the ransom ware and get our data without paying ransom

II. TYPES OF RANSOM WARE

1) Encrypting Ransom ware: Which uses encryption algorithm it is used in such a way that to block system files and demand Ransom the victim for decrypt the blocked contents. Example cryptowall, cryptolocker

2) Locker Ransom ware**:** Ransom ware locks the victim's computer in such a way that it is too impossible to access the desktop. They demand ransom to unlock the infected computer. Figure [2.1] shows types of Ransom ware

Fig.2.1 Types of Ransom ware

III. KEY CHARACTERISTICS

It has some key characteristics apart from the malware

1. Unbreakable encryption
2. It encrypts all kind of files
3. I will display an image or message in such a way that that lets you know "your data has been encrypted and that you have to pay a specific amount to get it back.
4. It can change the filename, so you can't predict the affected data this is one of the social engineering tricks used to confuse victims into paying the ransom.
5. It requests payment in Bit coins.
6. The ransom payment has a time limit deadline of time limit the ransom will increase ,but the data will be destroyed and lost ever
7. It spread to other PCs connected in local network.
8. It has data excretion capabilities.
9. It some times ransom note is translated into the victim's language so increase the chance for the ransom to be paid.

IV. THREAT CARRIERS OF RANSOM WARE ATTACK

In this day and age, everyone is troubled by the computer malware, threats –unwanted and malicious software code that hacks computer system causing malfunction data theft and there is loss of business their target is business individuals that threat propagated by different attack factors from that is shown in Figure [4.1]

1. Unsolicitated Emails (Phishing/Spear Phishing)
2. Unsolicited Internet downloads
3. Weak endpoint protection
4. Peer-To-Peer file transfer (USB / File shares)
5. Malware advertisement
6. SMS messages
7. Self propagation

Revised Manuscript Received on February 15, 2020.

Dr. M. Z. Shaikh, Principal, Bhagubhai Mafatlal Polytechnique, Navi Mumbai, India.

Prof. Sulakshana B. Mane, Bhrarati Vidyapeeth College of Engineering, Navi Mumbai, India.

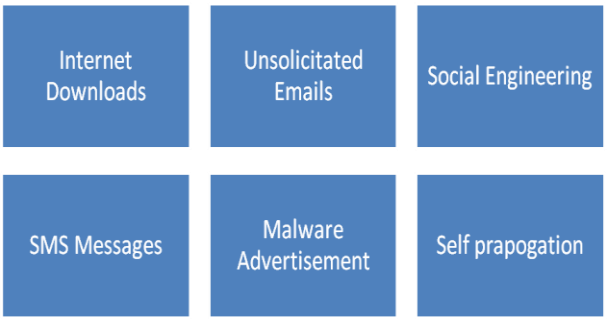

Fig 4.1 Entry points of Ransom ware

V. ATTACK METHODOLOGY

First it is very important that to understand how attack actually works. Looking to the facts of its damage, it is evident that ransom ware is not like any other attack, which can be easily detected and prevented by putting/tuning some security products, but it is much more than that. Shown in figure [5.1] As per our preliminary research, we have divided the entire process into phases which will give a clear understanding of the same. The proposed paper has explained the working and the authors have divided the working into three main parts that is the first step is attack here the injection to the system with

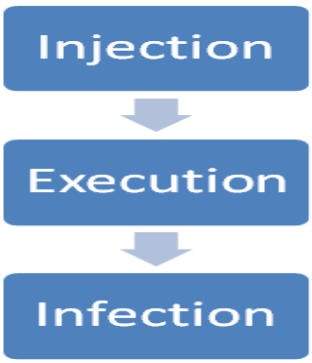

Fig. 5.1 working of attack

5.1.1 Injection

Attacker writes a targeted malicious code which is infected to the system through threat carrier there are so many threat carriers' emails, internet download, and social engineering.

5.1.2 Execution

After injection of a bot file it creates its location on operating system he will wait for a trigger this can be human or system generated action .once the trigger is done this install itself on the file system of the OS and starts locating data source in the file system

5.1.3 Infection The bot is capable to take the full control of the machine's data stores in the file system this control is given to the attacker to pass on the encryption command which encrypt the confidential data. The private key to decrypt the same is retained by the attacker and is shared only when the asked ransom is paid we have to understand the composition of this attack. The fundamental challenge is that, when this bot is installed on the target machine, it erases all the traces of its existence and hence it is very difficult to track the manifestation, so in order detect this attack .that Ransom ware working as shown in the figure [5.2]

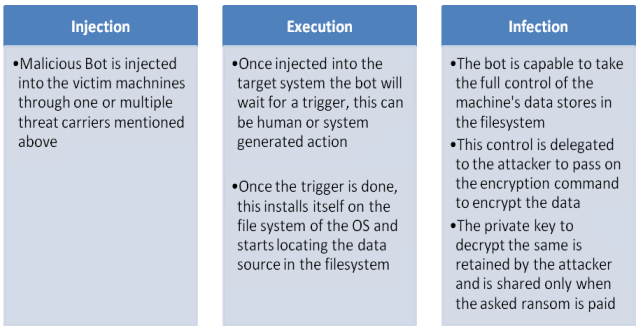

Fig.5.2 Ransom ware working

Any ransom ware classified into three parts attacker writing malicious code infected which infected through threat vectors take whole control of victims machine in his hand and display a message on the screen who locks and encrypts the machine when u pay a ransom they restore the machine

Industry Challenges

The integrity change of an object is irreversible in nature, which means without a valid key the change cannot be reverted

No assurance, where the files will be restored back, even after the ransom is paid

Not a single attack to track, Ransom ware / Destruct ware is a combination of multiple attacks, which makes the containment difficult

Hard to detect as the carriers and vectors used in these kinds of attacks are often trusted

Change in the attack surface, with each newer version of the same, making it hard to establish an uniform controlled environment

Use of weak / unsecure protocols / services which normally points to the usage of legacy windows systems and thereby usage of weak services like RDP, SMB etc.

Unpatented impact in terms of synchronized infection. It is also found that the infection is often random, which adds to the pain in detection.

VI. HOW TO PROTECT YOUR COMPUTER FROM RANSOM WARE

Several antivirus companies have come up with always to remove the virus but that does not decrypt the files unfortunately, you don't have many options unless you backups of your data but you can protect your computer with some common sense

VII. PRIMITIVE PREVENTATIONS

Antivirus should always update.

Spam messages should not opened or replied

Regularly take a external storage of confidential data.

Don't visit the unsafe and unreliable websites

Don't clock on harmful links.

Required some precautions when u access the Wi-Fi network Keep the windows firewall turned on and properly configured all times Apply patches and use operating system antivirus, browers, Adobe flash player Java.

VIII. RANSOM WARES AFFECT OTHER DEVICE THAN COMPUTER

There are ransom ware that affects Network attached storage computer server, networks, Mobile phones. It also uses on phones There are so many free apps that provide premium services adult contents illegal service user install they try it on their phones .It locks the phone and demand a ransom to unlock it .Also try on database stored on the sever of a financial websites. It may affect any device connected to the internet especially the smart connected devices that have limited interface option like IOT.

IX. NEED OF DETECTION AND PREVENTATION

IT goes undetected by traditional mode threat management technologies like antivirus we give a mechanism which will help information system to safeguard their sensitive data it is a biggest threat, public encryption in the cyberspace

X. RESULT ANALYSIS

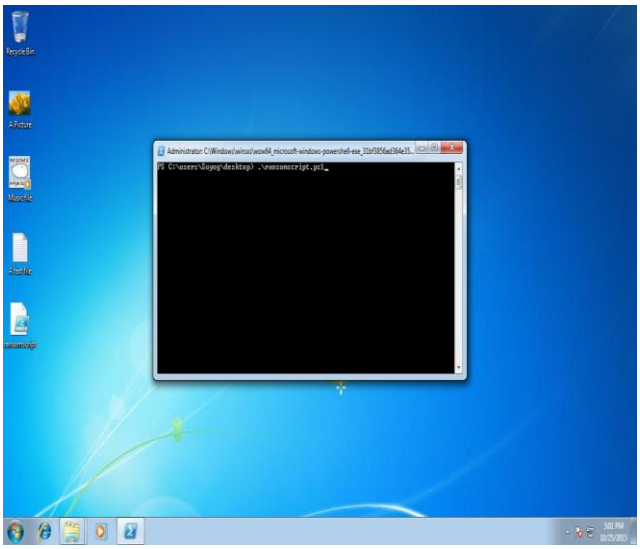

Fig 10.1 Infection anatomy

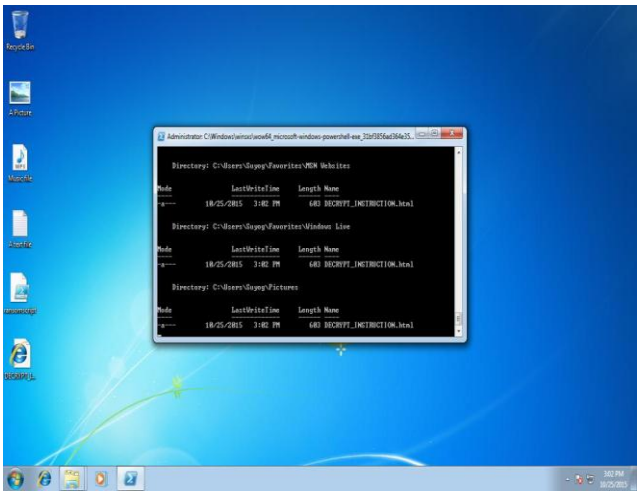

Fig 10, 2 Execution anatomy

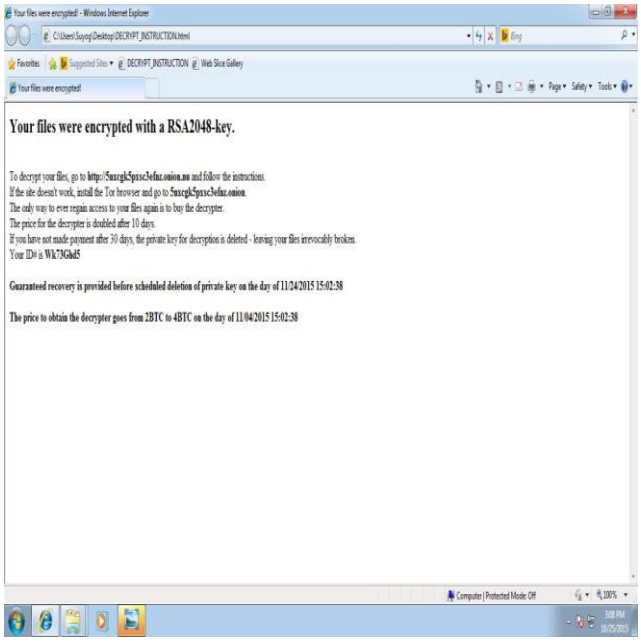

Fig 10.3 Infection anatomy

XI. CONCLUSION

The proposed paper focuses on the ransom ware as a virus that can hijack a victim's system and disrupt the normal working of the system. The proposed paper has been focusing on the basic of ransom ware, there families that is from creation, working, detection and prevention also. The proposed paper has also shown the different entry point for ransom ware and how it travels through the network it also states the basic prevention methods, detection criteria and explained briefly about the impact of ransom ware on society.

11. Acknowledgement

This paper is possible because of the able guidance of our Respected Principal sir Dr.M.Z.Shaikh so we extend heartfelt acknowledge to our professor and would also like to thanks others who helped us to fulfill this paper. Would also extend our heartfelt acknowledge to our parents for encouraging us.

REFERENCES

1. Savita Mohurle, Manisha Patil, International journal of advanced research in computer science, A study of Wannacry Threat: Ransom ware Attack 2017. volume 8, No. 5, May-June 2017
2. S. mahmudha Fasheen, P. Kanimozhi, B. Akora Murthy, Detection and avoidance of Ransom ware. Volume 5, issue 1, IJDER
3. Alexandre Gazet, Comparative analysis of various Ransom ware virii. 4th july 2008, EICAR
4. Julio Hernandez-Castro, Edward Cartwright, Anna Spepanova, Economic Analysis of Ransom ware.
5. Tianda yang, Yu Yang, Kai Qian, , Automated detection and analysis of android ransom ware, High performance computing and communication conference. 30th November 2015,