Ransomware
Threat to Organizations

[1]Ms. Desai Anuja S.,[2]Mr. Aniruddha P. Kshirsagar, [3]Ms. Gurav Tejashree P.
[1]Assistant Professor, [2]Assistant Professor, [3]Assistant Professor,
[1,3] Department of Computer Science and Engineering
[2] Department of Computer Engineering,
[1,3] Karmaveer Bhaurao Patil College of Engineering, Satara, India
[2] Zeal College of Engineering and Research, Pune

Abstract : Today's world is a fast moving world. Distance is no more a barrier to communication or knowledge sharing. Everything is available online. Physical presence is not compulsory, online working is a new key factor. In different organizations as well as banks, all can be handled online. But while using online services threat of different types of attack is increased. As we know the internet is one type of huge network which serves all clients. High risk of different types of cyber attacks is emerging. Ransomware is one type of cyber attack which is a growing global cyber security threat and it is one which could affect any organization very easily. Ransomware is an attack in which files or user screen are locked or encrypted and to unlock them "ransom" i.e money in exchange for something is demanded from an authorized user of the system. For limiting the impact of ransomware on organization there are several mechanisms such as good access control, frequent backups of data etc.

Keywords: Ransomware, Ransom, Cyber attack, online services

1. Introduction

In the 21st century, all information is available in just one click. The internet is a global system of interconnected computer networks. All information is made available at any corner of the world in just one click. Many services are made available online. Online banking is a good example of online services. Different cyber attacks are emerging these days. Ransomware [1] is one type of cyber attack. All these cyber attacks try to forge data sent over the network. Unwanted traffic is created at a specific node to fire Denial of Service (DoS) [7] attack. Attacks like spoofing, spooning are used to steal information in between of data transfer. Due to cyber attacks information available online is at high risk.

Following are some cyber attacks:

Phishing – Phishing means sending unwanted emails to thousands of customer and tries to ask for personal details like bank details or passwords or attract the people visit a fake website. In phishing some offers are given to attract users and personal information like phone number, bank account number and passwords are asked to submit.

Water Holing – Water holing means setting up fake and non-legitimate in order to harm users which are legitimate. In water holing attack, attacker sees the websites which is frequently seen by a victim or a group of victims, and these websites are infected by malware so that when a user visits that particular website malware is easily passed to victim's machine. It is mechanism for attracting legitimate users to visit infected website.

Ransomware [1] – In ransomware attack, malware used to make an attack on a victim and important data and files of the user are decrypted with the secret key. Ransom is demanded to decrypt data and files and to get access to the user machine.
Following are stages of cyber attack [13]:

1. Survey: All detailed information about the target is collected and analyzed to identify potential vulnerabilities of users.
2. Delivery: Delivery is about getting to the point in the target system where vulnerabilities can be exploited and attack can be fired.
3. Breach: In breaching vulnerabilities in victim are exploited to gain unauthorized access to system
4. Affect: Carrying out malicious activities

In ransomware [2], user's files or user home screen is locked or encrypted by an attacker. So the legitimate user of the system is unable to use those files or the whole system. Attacker demands ransom i.e money to decrypt or unlock files or user home screen. Ransomware is the biggest threat for online systems as important files or the whole system is encrypted. In online systems such as banking, share market etc. important files should not be at such risk.

Since the beginning of year 2016, ransomware has been growing as a global cyber security threat, which could affect any possible organization that does not have appropriate and strong defense mechanisms to detect and defend attackers. Ransomware is typically used by criminal people to earn money. Money is demanded in form of BitCoins i.e. Cryptocurrency High volumes of users with vulnerable devices get affected due to this attack. In 2017, WannaCry [2] attack was fired. Here, computers having Microsoft Windows operating system were targeted by encrypting important files and data and demanded payments in the Bitcoin cryptocurrency. WannaCry takes benefit of installing backdoors onto infected computer. In 2018, more targeted ransomware attacks were launched i.e criminals (attackers) analyzed the victim network and collected some information to understand what is really important for victim organization and set a ransom demand based on importance of organization‘s data. Attacks were made very dangerous by denying access to business-critical files and whole systems and operations of victim organization were prevented by attacker. In some previous years, attacks on Windows operating system were seen commonly but now attacks are launched on Mac and Linux operating systems also. Infection of ransomware i.e minor irritation to widescale disruption can vary as per the level of preparation by the system for defense.

2. What is Ransomware

2.1 Ransomware

Ransomware[3][4] is an emerging malware which locks the user out of its important files or their whole device and demands ransom i.e an anonymous online payment to get access to important files and the whole system. Payment is demanded in form of cryptocurrency (Bitcoin) [5] to hide transaction details.

Figure 1. Ransomware attack

Ransomware is used for firing multiple high-profile cybercrime cases incidents like in May 2017 the Wannacry incident which attacked NHS very badly. Some ransomware act like a worm, once they enter the network, they will spread automatically to other computers without any communication by attacker or the user who get infected. This was the scenario of attack in Wannacry attack.

There are two types of ransomware attacks:

1. File Encryption on a computer or no.of computers in a network which are important
   - In this type of attack, files in the computer are encrypted by an attacker.
   - User can't decrypt those files unless decryption key is provided by an attacker
   - Attacker demands ransom (i.e money) to decrypt those files.
   - The threat of deleting the file is given by attacker if money is not given to them

2. Locks a user's screen.
   - In this type of attack, the user home screen is locked by an attacker
   - Overall access to the system is restricted by an attacker
   - User can't perform any action unless and until the screen is unlocked - Attacker demands a ransom to unlock user screen

In both types of attacks victim needs to pay ransom to attacker to unlock or to decrypt files which are locked by attacker. In many cases of attacks, the ransom amount demanded from victim is quite tolerable so that victim can pay ransom easily and data can be recovered easily. Even after paying ransom there is no surety that our secure key or secret password which is used to unlock the machine will be surely given by attacker Still, data or files are at risk. The threat of permanent loss of data is given by attacker if the exact ransom is not paid in stipulated time. More often, ransomware can attack the same victim for more than once in succession. Ransomware attacks can infect any type of sector or organization.

2.2 Methods of injection of ransomware

Computers are infected by the following manners:

1. Users are tricked for running a legitimate looking program which is actually not legitimate

-Some requests are sent to users in form of discounts or free gifts. When the user clicks on that link, the injection of ransomware happens.

2. Using authenticate looking email attachments

-Ransomware links are sent by making requests in very authenticate manner through authenticate looking emails.

3. Visiting malicious websites

- When a user visits malicious websites ransomware can enter into the system.

4. Ransomware can also spread through data transfers between computers

-When other storage devices are connected to an infected machine via USB cables etc. ransomware is easily passed to a connected storage device.

3. Limiting the Impact of Ransomware

Prevention is always better than cure so it is essential to keep the computer safe. It is recommended for users of systems that operating system of machines and softwares should be kept updated. Multilayer protection security that is reliable against attacks is highly required. Back up of the data should be done. Files should be backed up offline on regular basis. Ransomware can be sent via Emails, Advertisement. Ransomware is spread using different honeypots. It restricts the system use by user in number of ways. [11] Following are some control measures to limit the impact of Ransomware:

A. Keeping your devices and computers updated

- By keeping software and operating systems updated, the risk of attacks is reduced.

B. Protecting PCs and mobiles using antivirus or anti-malware

- PCs and mobiles must be properly secured using antivirus or anti-malware

C. Good Access Control

- User privileges to particular data can control unwanted access to important files or data.

D. Limited access to the web using an admin account

- Admin with more access privileges should limit web access to avoid ransomware injection.

E. Timely backup of data

- Backups of important files or data should be taken very frequently. Access to backup data should be limited to avoid intrusion.

F. Controlling code execution

- Attacker trick user to execute macros which are infected by ransomware

4. How to Tackle Ransomware If A Machine Is Infected?

If a machine in an organization has been infected by malware, then following steps helps to limit the impact of the infection [14].

1. Disconnection of the computers, laptops or tablets from network which are infected from network.
2. Turn off WiFi and unplug network carrying cables.
3. Safely format or replace the disk drives and installation of latest operating system.
4. Device need to be reconnected to a clear network.
5. Update latest antivirus software.
6. Network reconnection.
7. Network traffic monitoring.

If an organization is infected with ransomware, the National Crime Agency (NCA) informs industry and the client do not pay for it.

Even if a ransom is paid the following possibilities are there:

1. No guarantee is provided by attacker that he/she will again receive data access after paying ransom to an attacker.
2. Even if you pay ransom to attacker, your pc might be at huge risk and infected if you don‵t clean up your machine.
3. Attacker usually assumes that you would be always open to pay for the attacks in the future also. You become more vulnerable to attack in the future as you are ready to pay ransom
4. Indirectly funding to criminal groups is given by victim. Indirectly funds are provided to criminals and this is an encouragement for more crimes in the future.

References

[1] Danny Yuxing Huang, Maxwell Matthaios Aliapoulios, Vector Guo Li ― Tracking Ransomware End-toEnd‖ 2018 IEEE Symposium on Security and Privacy (SP)

[2] Shou-Ching Hsiao ; Da-Yu Kao ― The Static Analysis of Wannacry Ransomware‖ 2018 20th International Conference on Advanced Communication Technology (ICACT)

[3] Daniel Gonzalez , Thaier Hayajneh ― Detection and prevention of Crypto ransomware‖ 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)

[4] MattiasWeckstén, Jan Frick, Andreas Sjöström, Eric Järpe, ―A novel method for recovery from Crypto Ransomware infections‖, Computer and Communications (ICCC), 2016 2nd IEEE International Conference.

[5] X. Luo and Q. Liao, "Ransomware: a new cyber hijacking threat to enterprises," in Handbook of Research on Information Security and Assurance, IGI Global, 2009.

[6] P. Ducklin, ―Reveton/FBI ransomware—exposed, explained and eliminated,‖ NakedSecurity, August 2012, https://nakedsecurity.sophos.com/.K. Elissa,

[7] N. Andronio, S. Zanero, and F. Maggi. HelDroid: Dissecting and detecting mobile ransomware. In Proceedings of the International Symposium on Research in Attacks, Intrusion, and Detection (RAID), 2015.

[8] E. Arnold. Tennessee sheriff pays ransom to cybercriminals, in bitcoin. http: //www.bizjournals.com/memphis/blog/2014/11/ Tennessee-sheriff-pays-ransom-to-cybercriminalsin.html, 2014.

[9] D.Carrigan. Police departments hit by ransomware virus.http:// www.wcsh6.com/story/news/local/2015/ 04/10 /police-departments-hit-by-ransomware-virus/ 25593777/, 2015.

[10] S. Axelsson. The base-rate fallacy and its implications for the difficulty of intrusion detection. In Proceedings of the ACM Conference on Computer and Communications Security (CCS), 1999.

[11] C. J. Dietrich, C. Rossow, and N. Pohlmann. Exploiting visual appearance to cluster and detect rogue software. In Proceedings of the ACM Symposium on Applied Computing. ACM, 2013

[12] S. Forrest, S. A. Hofmeyr, A. Somayaji, and T. A. Longstaff. A sense of self for Unix processes. In Proceedings of the IEEE Symposium on Security and Privacy (S&P), 1996.

[13] S. Jana and V. Shmatikov. Abusing file processing in malware detectors for fun and profit. In IEEE Symposium on Security and Privacy (S&P), 2012.

[14] H. Weisbaum. CryptoLocker crooks launch ‗customer service' site. http://www. cnbc.com/id/101195861, 2013.

[15] D. J. Tian, A. Bates, and K. Butler. Defending against malicious USB firmware with GoodUSB. In Proceedings of the Annual Computer Security Applications Conference (ACSAC). ACM, 2015.

[16] Pathak, P B.‖Malware a Growing Cybercrime Threat: Understanding and Combating Malvertising Attacks‖,2016,

[17] Nolen Scaife, Henry Carter, Patrick Traynor, Kevin R.B. Butler." CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data",2016, IEEE 36th International Conference on Distributed Computing Systems

[18] Sanggeun Song, Bongjoon Kim, and Sangjun Lee. ―The Effective Ransomware Prevention Technique

Using Process Monitoring on Android Platform‖, Hindawi Publishing Corporation Mobile Information Systems Volume 2016, Article ID 2946735, 9 pages.

[19] N. Andronio, S. Zanero, and F. Maggi, ―HelDroid: dissecting and detecting mobile ransomware,‖ 2015, in Research in Attacks, Intrusions, and Defenses, vol. 9404 of Lecture Notes in Computer Science, pp. 382–404, Springer. International Journal of Advanced Research in Computer Science

.