Computer Security: Operation Of The Ransomware And Identification Of Ransomware Attack

Operation of the Ransomware

Ransomware attacks specifically refer to that sort of attack where the cyber security of an individual or all of the employees within the organization get affected. Such attacks breach the security of the systems the employees work in, having secured all of the information present within the system blocking the access from that of the user, and demanding money in return for the decryption password. With the help of the decryption password, the user will again have the provision to access their systems with all of the information in the same form as it was (Brewer, 2016). Two of the most uprising ransomware attacks that have occurred within the period of 2017 to 2019 have been described in below as to how they have been working and affecting the working of an organization in relation to a live setting. These are,

Bad Rabbit- refers specifically to that Ransomware, which had broken out on October 24th in the year of 2017 attacking almost every single existing organization relying in the regions of Russia having victimized people from selective regions of Ukraine as the reports have suggested.

According to the observations, this particular work within any live environment within the organization spreads with the help of a drive-by attack. However, this specific attack instills malware within the system it aims to attack (Lee, Kim & Kim, 2019). The malware waits for a specific time of around 10-60 minutes after the desired infection has been done before the system reboots itself. Specifically, the reboot gets scheduled with the usage of “shutdown.exe” tools and all other tools, which perform a similar function. Once the procedure of reboot gets completed, the process of encryption of the MFT table starts within the NTFS secured partitions, having overwritten the specific MBR along with the customized loader having the addition of a specific ransom note.

This specific malware enumerates all of the existing adapters for the network, all the renowned names of the server with the help of the NetBIOS as well as the retrieval of the list relating to the current lease of DHCP depending upon the availability (Maniath, Poornachandran & Sujadevi, 2018). Each of the IP present upon the local network along with each of the server that are found is kept a check upon the TCP ports 445 as well as 139, which are open. Specifically, these kinds of machines have all of these ports attached to them, which are open and are then followed by a similar attack by one of the methods that have been described above.

Resources 1, as well as 2, relate to the malware binary, which contains two of the versions referring to the standalone tool that makes all of the tries towards the extraction of all the login details along with that of the password for each individual users. This tool referring to that of the malware is completely run by the main binary (Scaife et al., 2016). All of the extracted data gets transferred back to the primary module with the help of a pipe having a random GUID-related name.

TeslaCrypt- this particular malware was spread with the usage of social engineering to compel a specific user to have a click upon a particular link linked to that of the phishing email as well as the later on the activity of adding all of the related malicious attachments to those of the emails. It also makes use of the technique of malvertising in the form of a vector-related attack (Hampton & Baig, 2015). All of the victims have undergone the process of redirecting to that of the compromised sites related to that of WordPress having the provision of the installed Nuclear EK. This relates to at least one of the cases belonging to the exploitation of a vulnerability in an outdated version of the Flash Player that might have been installed at that very specific moment.

In addition to this specific list of all the encrypted files normally have a target marked upon other of the strains relating to all of the existing ransomware. Similarly, TeslaCrypt also tried to follow the specific method of cashing in within the existing gaming market by carrying out the procedure of encryption to over 40 types of files having a direct association with the popular games played on the computer (Poudyal, Subedi & Dasgupta, 2018). All of these games included the likes of Call of Duty, Minecraft along with that of the World of Warcraft.

Whenever such a victim gets affected with this particular ransomware, the procedure looks exactly similar to that of the CryptoLocker. The encryption stays until the specific site for the payment along with that of the instructions comes up for the owner of the computer system to pay the ransom that has been demanded by the hacker to provide the individual with the decryption key (Zimba & Chishimba, 2019).

The particular procedure for the payment has been run through a specific website, which was located within the TOR domain. Each of the instances related to this particular ransomware shares one of the belongings to that of the unique address of the bitcoin.

Identification of Ransomware Attack

Both of the ransomware attacks have been a hype, which had taken place within the periods of 2017 to that of 2019. The happenings associated with both of the ransomware attacks have been described in detail below.

Bad Rabbit

This ransomware attack had taken place in the year of 2017, on 24th of October had observed certain notifications related to that of the mass attacks caused by this ransomware, which was provided with the name of Bad Rabbit that very day when it has broken out. The primary targets for this particular ransomware had been the big organizations within the field of business as well as all of the consumers staying within the varied regions of Russia (Indu & Sharma, 2018). Also, to the updated records, this particular ransomware had also made attacks towards the varied regions of Ukraine alongside. Down below is what the exact message of the Bad Rabbit ransomware.

The dropper for the ransomware had been distributed with specific help from the drive-by attacks. Alongside the target being on a visit to the legitimate website, a particular dropper is being downloaded from the individual threat to that of the infrastructure belonging to the specific actors. However, none of the exploits had been used, making the victim follow the manual

method of dropping the malware having the pretentious behavior of an adobe flash installer (Conti, Gangwal & Ruj, 2018). On the other hand, in references to the study that had been carried out long after the ransomware had broken out that this Bad Rabbit utilized the exploit, which is commonly referred to as the EternalRomance as a vector for the infection aimed specifically aimed towards the spread within the shared network of the corporate organizations. Particularly, this same exploit has been used within the ransomware named ExPetr as well.

The Bad Rabbit attack related to that of the ransomware places encryption within all of the files along with that of the disks attached to the particular computer. This specific ransomware, when had attacked in the year of 2017, had enumerated all of the processes that had been running within the system at that particular point of time, comparing all of the hashed names related to each of the processes along with the embedment of all the existing hash values. The hashing algorithm related to Bad Rabbit ransomware had also been linked as well as with that of the ransomware named ExPetr.

As the Bad Rabbit had hit the business organizations working within the varied regions of Russia, the primary damage that the malware did was to place encryption upon all of the files as well as the storage devices within the system of each employee. In addition to this, a wide message was displayed across the screen of the system asking for remuneration in order to get hold of a decryption password that shall be utilized for the lifting up of the encryption (Roberts, 2018). However, the message across the screen of the system also ensured the users, in turn the owner of the business organizations that the information contained within the privacy is safe and will be returned in the same form.

As a result of the ransomware attack caused by the Bad Rabbit, all of the owners belonging to the specific business organizations, which had been attacked by the ransomware had to take the necessary steps for privacy as well as the protection of the sensitive data that they had. This was followed by the business organizations to gather the required amount of money to be presented to the group of hackers in order to get hold of the decryption password to get their business back on track and get back all the information contained within the individual systems of the company.

TeslaCrypt

This is commonly referred to as one of the major ransomware attacks that had broken out at the end of the year 2016 has affected almost all of the organizations working within the field of business in most of the European countries together (Everett, 2016). This name was given specifically for the reason relating to the fact that what kind of files does this malware encrypted within the user’s computer.

This particular ransomware attack had the primary motive of encrypting all of the data related to the games that were being installed as well as played by the individual users within their system. The specific kinds of files that this ransomware attacked had particularly painted a target upon were the likes of saved games, along with the maps, all of the content downloadable and other similarly existing files.

As an impact of this ransomware upon the individual gamer’s computer, all of the saved data along with the inclusion of the downloadable content was placed upon with a password, hence

the user had no provision to even copy the data to some other device and continue with the work (Le Guernic & Legay, 2017).

The hackers programmed the ransomware with the utilization of such exploits that consists of the potential to directly breach the security of the user system and travel to the core of every single file, be it small and lock it with a password, which shall be provided only when the ransom is paid (Gonzalez & Hayajneh, 2017). Getting to the core of the computer was considered to be the primary process of a security breach, which was a serious concern for the individuals.

As an outcome of the ransomware attack caused by the TeslaCrypt, all of the users who were specifically gamers, which had been attacked by the ransomware had to take the necessary steps for privacy as well as the protection of the sensitive data that they had related to the games, which they played (Mauraya et al., 2017). This was followed by the individual users to gather the required amount of money to be presented to the group of hackers in order to get hold of the decryption password to get their gaming back on track and get back all the information contained within the individual systems of the gamers.

References

1. Brewer, R. (2016). Ransomware attacks: detection, prevention and cure. Network Security, 2016(9), 5-9.
2. Conti, M., Gangwal, A., & Ruj, S. (2018). On the economic significance of ransomware campaigns: A Bitcoin transactions perspective. Computers & Security.
3. Everett, C. (2016). Ransomware: To pay or not to pay?. Computer Fraud & Security, 2016(4), 8-12.
4. Gonzalez, D., & Hayajneh, T. (2017, October). Detection and prevention of crypto-ransomware. In 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON) (pp. 472-478). IEEE.
5. Hampton, N., & Baig, Z. A. (2015). Ransomware: Emergence of the cyber-extortion menace.
6. Indu, R., & Sharma, A. (2018). Ransomware: A New Era of Digital Terrorism. Computer Reviews Journal, 1(2), 168-226.
7. Le Guernic, C., & Legay, A. (2017, March). Ransomware and the legacy crypto API. In Risks and Security of Internet and Systems: 11th International Conference, CRiSIS 2016, Roscoff, France, September 5-7, 2016, Revised Selected Papers (Vol. 10158, p. 11). Springer.
8. Lee, S., Kim, H. K., & Kim, K. (2019). Ransomware protection using the moving target defense perspective. Computers & Electrical Engineering, 78, 288-299.
9. Maniath, S., Poornachandran, P., & Sujadevi, V. G. (2018, September). Survey on Prevention, Mitigation and Containment of Ransomware Attacks. In International Symposium on Security in Computing and Communication(pp. 39-52). Springer, Singapore.
10. Mauraya, A. K., Kumar, N., Agrawal, A., & Khan, R. A. (2017). Ransomware: Evolution, target and safety measures. International Journal of Computer Sciences and Engineering, 6(1), 80-85.
11. Poudyal, S., Subedi, K. P., & Dasgupta, D. (2018, November). A Framework for Analyzing Ransomware using Machine Learning. In 2018 IEEE Symposium Series on Computational Intelligence (SSCI) (pp. 1692-1699). IEEE.

12. Roberts, N. (2018). Ransomware: an evolving threat(Doctoral dissertation, Utica College).
13. Scaife, N., Carter, H., Traynor, P., & Butler, K. R. (2016, June). Cryptolock (and drop it): stopping ransomware attacks on user data. In 2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS)(pp. 303-312). IEEE.
14. Zimba, A., & Chishimba, M. (2019). Understanding the Evolution of Ransomware: Paradigm Shifts in Attack Structures. International Journal of Computer Network and Information Security, 11(1), 26.