ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 9, Issue 3, pp: (53-55), Month: July - September 2021, Available at: www.researchpublish.com

The Revolution of Ransomware

Abdulaziz Abdulrahman Alrushaid

Affiliation none

Saudi Aramco, Dhahran, Saudi Arabia

Abstract: **Computer malware are very common and they are classified based on their behavior. One common form is the ransomware where it will encrypt the user data/files resulting in access denial to them. Nowadays, this type become a very attractive and efficient to attackers for many reasons that will be elaborated in this research and further will learn how to mitigate such attack and secure the user data.**

Keywords: **cyber security – attack – ransomware – malware – cryptocurrency – files.**

I. INTRODUCTION

Computer technology has become increasingly important in the contemporary society due to the recognized performance to enhance efficiency in service provision. Indeed, computer technology is important in processing storage, collection, retrieval and manipulation of data that is important in decision-making. However, such data would only have the desired outcomes when it is accurate, available, relevant and sufficiently comprehensive to allow for decision-making. Unfortunately, there are number of ways in which the availability and accuracy of the data may be compromised, key among which is the infiltration of the data using ransomware. At its most basic, the concept of ransomware underlines a form of malware that is designed to encrypt important files within a particular device or network, thereby rendering the systems and files that are dependent on them unusable, after which the malicious actors would make demands for a ransom in exchange for decrypting the compromised data. In most cases, the malicious software would threaten to block or publish access to a computer system or data often through encrypting it until they have been paid a particular fee by the victim. The advanced computer technology has enhanced the anonymity of the ransomware's source through requiring the victim to pay using payment methods that would be almost impossible to trace, an element that assists cybercriminals to remain anonymous. Nowadays, ransomware has become more popular as a result of the increased proliferation of cryptocurrencies such as Bitcoin. Cryptocurrencies are digital currencies that utilize encryption techniques in the verification and securing of transactions, as well as controlling the generation of new units. Cryptocurrencies are a key player in the ransomware attacks since payments can be transferred to criminals in an untraceable manner, which allows the criminals to remain anonymous. The main reason for the utilization of ransomware among hackers is its effectiveness in compelling the victims to pay the desired ransom. Indeed, it has been acknowledged that encryption tends to lock out the target from the key system functions, thereby preventing them from accessing crucial systems and files or even the utilization of the computer altogether. Once the victims have been locked out of their systems, they are highly likely to pay the criminals in order to retrieve access to their systems. It is acknowledged that criminal hackers undertake this form of attack in an attempt to extort money from individual organizations, groups and people. The effectiveness of the ransomware is predictable due to the fact that it instills panic and fear in the victims, thereby causing them to seek ways of paying the ransom. Efforts to eliminate the same often trigger additional malware infections. Furthermore, the criminals display intimidating messages that push the victims to make payment in order to regain control of the computer systems and networks.

II. HOW ATTACKERS USE RANSOMWARE

Normally, ransomware would be spread via phishing emails that incorporate malicious attachments or via drive-by downloading. It is noteworthy that drive-by downloading comes up in cases where the user has unintentionally visited infected websites, after which the malware would be automatically downloaded and installed often without the permission

or knowledge of the users. For instance, crypto ransomware, which underlines a malware variant that ultimately encrypts the files, would be spread via similar techniques and may be spread via social media too. In addition, there are newer techniques that ransomware infection takes place. A case in point is the utilization of vulnerable web servers, which are often exploited as an entry points to access the network of an entity. Once the user has clicked the link sent to their email or accessed a website that is infected, the malware would automatically infiltrate the computer system especially in cases where there are no structures or safeguards that prevent the occurrence of such infection. Any computer that is connected to the network system could be infected and potentially have its system and files locked out of access until such a time when the users pay the attackers the stipulated fee. It is noteworthy that the payment of the ransom does not offer any guarantee that the attackers will restore access to the computer system. If they do so, however, they often provide a decryption key that the victims would use, thereby allowing them to access their systems or contents.

III. PROTECTION FROM RANSOMWARE

Malware infections may be immensely devastating to organizations and individuals, with recovery being a difficult process. Scholars and computer experts have recommended that administrators and users to practice varying measures that would come in handy in the protection of their computer networks from ransomware infection. Key among them is the employment of data backup and recovery plan for any critical information that it has in its possession. This involves performing and testing system backups on a regular basis that would restrict the effects of ransomware on system or data and expedite the process of recovery. It may be acknowledged that network-connected backups could also become affected by ransomware, therefore critical backups must be isolated from the network to maximize the protection against ransomware attacks.

In addition, the organization must ensure that its operating systems and software are updated with the latest and most secure patches. Indeed, a large proportion of attacks primarily target operating systems and applications that are immensely vulnerable. It is noteworthy that a large proportion of malware are always updating themselves and reinventing their characteristics to evade the anti-malware systems from detecting them in order to infect more targets. Cybercriminals are always trying to come up with new ways of infiltrating systems and stealing data often for financial gain. In this case, software and operating systems must be constantly updated to ensure that they have the capabilities to detect and prevent the infection of such ransomware. Ensuring that the systems and software are patched using the latest updates would significantly reduce the number of entry points that can be exploited by the attackers, thus reducing the attack surface for ransomware attacks. Of course, such updates would not solely be restricted to critical software and operating systems of the computer network but also the anti-malware software. The installation of anti-malware (Static and Dynamic) software would be fundamental in monitoring the computer systems, detection of the malware prior to its infiltration of the computer network systems, as well as elimination of the same. In this case, it is imperative that the organizations and individuals put in place anti-malware software that would not only detect but also eliminate the malware prior to its entry into the computer systems. This would also necessitate that the computer system and all the software that have been downloaded from the internet are completely scanned prior to their installation or execution in the system to prevent or avert the possibility of any malware infection in the long-term and the short-term.

Part from the technological measures that would prevent the occurrence of infections with ransomware, organizations must also change their policies particularly with regard to access to computer systems and the permissions for the execution of particular activities. For instance, it is essential that organizations restrict the permissions of users to run and install unwanted software applications. This would involve the application of the principle of least privilege to every other service or system. In this case, the restriction of privileges means that no software (or malware) would run or be installed without the permission of the computer administrators, consequently restricting its capability to spread across the network. Of course, such restrictions would also be placed on individual levels where individuals can have their computers being password protected to prevent other users from accessing and manipulating them. This would be complemented by the incorporation of network and host scanning where any device that is placed on the network would be automatically scanned and any malicious software either blocked or completely deleted from the devices prior to their installation in the computer system. Such measures would also be extended to access to malicious sites where the anti-malware software would block such sites immediately and provide a warning to the user regarding the dangers involved in accessing the site.

IV. CONCLUSION

Of course, ransomware attacks are becoming increasingly innovative, in which new and more effective strategies will have to be implemented to prevent them. Currently, however, there is no one appropriate and effective method of combating ransomware rather organizations have to use a combination of strategies to ensure that the incidences and potential for attacks have been reduced or completely eliminated. In any case, having a backup of the critical files away from the current computer system and combining the same with limited access and incorporation of anti-malware could appreciably reduce the potential for occurrence of attacks.

REFERENCES

[1] Chowdhry, D. G., In Verma, R., & In Mathur, M. (2020). The evolution of business in the cyber age: Digital transformation, threats, and security. New York, NY: Routledge

[2] Gonzalez, J. J., &Kemp, R. L. (2020). Cybersecurity: Current writings on threats and protection.Jefferson, North Carolina : McFarland & Company, Inc.Palm Bay, Florida, USA : Apple Academic Press

[3] Kim, S., &Shrestha, R. (2020). Automotive cyber security: Introduction, challenges, and standardization.

[4] Rains, T. (2020). Cybersecurity threats, malware trends, and strategies: mitigate exploits, malware, phishing, and other social engineering attacks. S.l.: Packt Publishing.

[5] Steffens, T. (2020). Attribution of advanced persistent threats: How to identify the actors behind cyber-espionage.Berlin, Germany : Springer Vieweg