The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM)
ISSN: 2602-3199

The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM), 2022

Volume 19, Pages 78-86

IConTech 2022: International Conference on Technology

Ransomware Target: Linux. Recover Linux Data Arrays after Ransomware Attack.

Rosen HRISTEV
University of Plovdiv Paisii Hilendarski

Magdalena VESELINOVA
University of Plovdiv Paisii Hilendarski

Kristiyan KOLEV
University of Plovdiv Paisii Hilendarski

Abstract: The events of the previous two years have forced many businesses from many industries to fast transition to remote work mode. Most organizations were unprepared for this new method of working, and many IT professionals first risked the security of the infrastructures they supported. As a result, ransomware developers found a way to resume development of one for the second most popular operating system – Linux, which is dominant in server infrastructures. Attacks up to now have tended to concentrate more on the end user, whereas ransomware developers now target the core of the organization, allowing for greater ransom demands to recover the data. Along with these, there have been increasing reports of new cryptoviruses for Linux in recent months. This concept is not new in 2015, the first ransomware for Linux was disclosed. The paper examines the evolution of cryptoviruses in Linux and demonstrates how to utilize a private cloud to recover data arrays after a ransomware infection in Linux.

Keywords: Ransomeware, Cyber security, Private cloud, Cryptovirus, Linux

Introduction

The situation with the Covid-19 pandemic, which occurred at the beginning of 2020, faced many business sectors with serious challenges. One of the serious challenges that most businesses have had to face is the rapid switch to remote working mode. Business, media, social interaction, education, etc. move onto platforms on the Internet. As a result, the amount and importance of information flowing through the digital landscape has increased exponentially (Sushruth et al., 2021). An increase with nearly 165 percent is the grow over the past five years, average bandwidth consumption (OpenVault, 2021). This has led to serious vulnerabilities in the cyber security of infrastructures and given a serious field for cyber criminals to appear. Proof of this is the serious increase in cyberattacks after the announcement of the pandemic, announced in numerous studies done in the field (Lallie et al., 2021).

The ransomware attacks mainly encrypts data from MS Windows, but is gradually spreading to machines with Linux-based operating systems as well. It demands a ransom from the user to decrypt the files, otherwise the hackers threaten to make the data public. This attack mostly uses infected email attachments or malicious websites. When it is compromised, companies fail to pay for the secret decryption key and therefore attackers can leak the stolen data. This trend has made it possible for cybercriminals to negotiate with victims, leading to extortionate data breaches (Tawalbeh et al., 2020).

The research describes an infection of Linux based machine with crypto-ransomware and proposes a method for data recovery after that. The study is organized as follows. First, we look at the vulnerabilities that are revealed

after the switch to remote working mode, as a result of which cyberattacks against users have increased tremendously. The next part is devoted to the main types of ransomware. The infection of the Linux-based machine and the recovery of the files are described in the last two sections.

Ignoring Cybersecurity by Organizations during Covid-19

Nowadays, the data that is stored online in an organization grows exponentially, and the financial value of the stored information repeatedly exceeds the one of the equipment which is needed for its storage (Hristev et al., 2021). The need to switch to remote working mode, due to the Covid-19 pandemic, has repeatedly accelerated the digitalization process in all sectors of the economy at a high pace. This has led many organizations to quickly change their established way of working, in remote working mode, as a significant part of them initially made compromises regarding the security of the infrastructure and the data stored in it.

The Zscaler's research: VPN Risk Report 2022 (Schulze, 2022) which was conducted among 351 IT professionals, shows that 95% of companies use VPNs for secure access to data stored in IT infrastructures, the share is increasing by 2% over the past year. A reference to Zero Day Exploits in CVE shows that since 1999, there have been 606 VPN-related vulnerabilities reported, with 34% of them whist is 206 as number have been announced since the beginning of the pandemic. For the second most common operating system – Linux, the values look similar, with 6,544 vulnerabilities announced since 1999 of which 1,400, or nearly 22% of all have been announced since the beginning of the pandemic.

The data shows that the process of digitization and the switching to remote working mode causes malware developers to focus more and more efforts on discovering vulnerabilities that they can use to compromise the integrity of data stored in IT infrastructures. 78% of the professionals who participated the Zscaler study are worried about ransomware attacks. Currently the data stored in the infrastructures does not use enough sufficiently protected methods. The most of specialists rely on the standard method of data protection - backup, which is not flexible enough. With an incorrect security policy and a successful ransomware attack, the backup also can be encrypted or the data from the last backup up to the time of infection can be lost. Many sources point to the 3-2-1 backup technique as the most successful. It includes:

- 3 archives;
- 2 different media;
- 1 different location.

Only about 31% of ransomware attacks are stopped before they encrypt part or all of the data. According to Sophos's research, The State of Ransomware in Retail 2022 (Sophos, 2022), the survey of 5,600 IT professionals from 31 countries around the world, 73% of businesses are dealing with the problem using backups, and 49% have had to pay back to the attacking organization. This means that not everyone who relies on backups was able to recover enough information and some of them had to pay a ransom for their data. Paying the ransom also does not guarantee data recovery, with only 5% of organizations claiming to have fully recovered their data.

After the appearance and popularization of RaaS (Ransomware as a Service), the number of attacks with crypto-ransomware has increased many times, and only in July this year, attacks against various organizations have increased by more than 40% compared to the previous month of the same year.

During the pandemic, many companies dramatically increased their enterprise IT budgets. There is a trend for small and medium-sized companies to invest more and more in technology, rather than security. Despite the fall of epidemic measures, a large number of companies adhere to and continue their development for a remote workplace to reduce costs. Securing computing equipment for employees working from home and connecting them to the work environment through a VPN tunnel is not enough to create a secure environment. As a result of the statistics from the various sources, we can conclude that the data stored in the organizations are vulnerable.

Undeniably a larger percentage of PCs run Windows, their users are undoubtedly a more common target for Ransomware attacks. As a result, the number of crypto-ransomware for Windows is significantly higher compared to Linux, but this is not a guarantee of security. Attempts for Ransomware attacks on the Linux operating system are not new. The first malicious crypto code for Linux appeared in late 2015 and was named Linux.Encoder. The main difference is that while Windows crypto-ransomware mainly look for user files, Linux

ones look to affect other types of files like .html, php, sql, java, class, etc. Thus, using the "double extortion" tactic, where a ransom is demanded in addition to decrypting the files, and not to publicly distribute the information that the malware developers have accessed, makes Linux users doubly vulnerable.

In one of our previous research (Hristev et al., 2022) we demonstrated the possibility of data recovery after Windows has been infected with Ransomware using a private cloud. The focus of the present study is on examining the possibilities of file recovery after infection of a Linux operating system with a crypto-ransomware.

The ability to recover data after a ransomware attack does not exclude the use of an alternative data storage option and does not negate the need to implement a backup policy. However, we must be careful and implement proper security policies due to the fact that our data can be put at risk by becoming public.

Ransomware Types

There are basically three different types of ransomware as shown in the Figure 1.

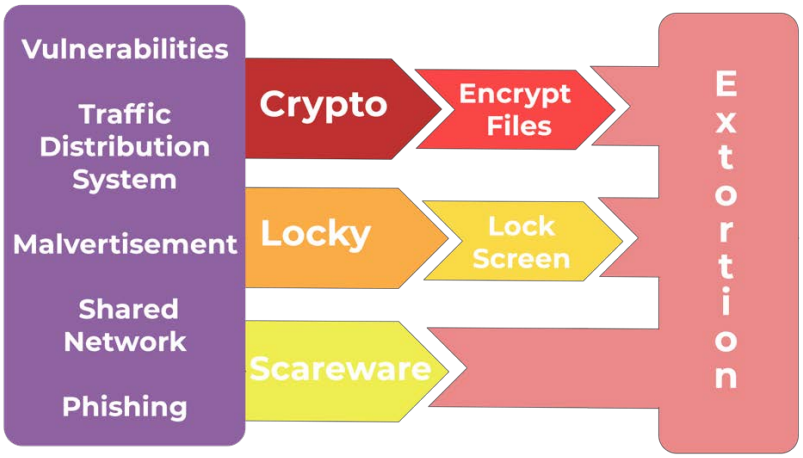

Figure 1. Ransomware types

The first type of ransomware is called crypto-ransomware. This type of ransomware is considered very dangerous because it encrypts the victim's files, making them impossible to access without a valid decryption key. We classify crypto-ransomware as malware that demands a sum of money after limiting a user's ability to access their computer or files. The most often method used by crypto-ransomware to contact its victims is through files or links that are distributed in email message campaigns, called Phishing. The email message contains links to documents that have been saved online. The documents are executable programs. The emails have attachments that download crypto-ransomware to the device. Common file formats used to deliver crypto-ransomware include the following files: Microsoft Word (.doc or .docx), Microsoft XSL (.xsl or .xslx), XML document (.xml or .xslx), Archive folder, containing a JavaScript file (.zip file containing a .js file), Multiple file extensions (eg <PRINT#2106>.pdf.js).

Other often method used by crypto-ransomware to reach victims is malvertisement. This tactic direct the victim to a website hosting an exploit kit appearing on real websites. Also crypto-ransomware can be spreaded on the affected system, attacking any devices and computers on a shared network. Another well known practice is redirecting website traffic to a website that hosts an exploit kit that exposes the computer's weaknesses and the ransomware is installed with auto-download malware. These practices can be used by all three types ransomware that we consider.

Receiving of the email with the crypto-ransomware does not cause infection. User must download or open the attached or linked file. If the opened file is JavaScript, it will try to download and install the crypto-ransomware itself from a remote website or server. If the attached file is a Microsoft Word or Excel document, malicious code such as a macro is embedded in the file. Even if the user opens this file, the macro can only run if the macros are enabled in Word or Excel or user enables macros.

The attack starts after the malicious email attachment is downloaded and a ZIP file disguised as a PDF automatically launches and downloads the ransomware. It will be saved with a random name as a file in the root file system with the user's other applications. Once activated, the ransomware first establishes a connection to the attacker's control server. After connecting to an active server, the ransomware initiates a key exchange protocol using an encrypted public key. Requests and responses between the malware and the server are made using RSA encrypted HTTP POST commands. The ransomware already contains the server's 2048-bit RSA public key when it is downloaded. It uses this public key to encrypt a request for a unique for the machine encryption key which will be used later. Along with this request, the ransomware sends information about the machine it is running on. The information that is sent includes the malware version, system language, and a numeric identifier. After the server decrypts this message with its own 2048-bit RSA secret key, the server generates a key response. The response includes the victim's IP address and a unique RSA public key. Only then does encryption begin.

The malware starts looking for specific file types in directories and mapped network drives. There is a complex encryption process for every matching file found. First, the malware generates a new 256-bit key that uses AES (Advanced Encryption Standard) file encryption. AES is an encryption system using a symmetric key. The symmetric key encrypts much faster than 2048-bit RSA. The AES key is used to encrypt the contents of the files. Instead of storing the key somewhere else, the ransomware encrypts the AES key using the unique RSA public key obtained during the key exchange. Each RSA encrypted AES key as well as the AES encrypted file contents are written back to the file. The infected user must obtain the secret RSA key that corresponds to the user's unique private key to decrypt the contents of the file. Brute force decryption of the files without a decryptor is impossible due to the 2048-bit RSA encryption. After the payment with cryptocurrency is confirmed, the Ransomware Server searches for the corresponding secret key. It is unknown exactly how this process works, but it is clear that the server stores some information about the user's unique identifier and their public key in order to find the secret key. An automatic decryptor, which already contains the secret key is sent to the infected user by the server. The RSA secret key is used to decrypt the AES key stored in the file for every single file. The decrypted AES key is then used to decrypt the contents of the file. The decryptor automates this process for the infected system. The decryption process may take hours depending on the number of files in the system.

The crypto-ransomware displays a message containing the ransom demand once the encryption is complete. The amount varies depending on the particular ransomware, and payment is often only in Bitcoin or a similar digital cryptocurrency. The victim will receive the decryption key if choose to pay the ransom, although this is not guaranteed. And even if a decryption key is obtained, it is not guaranteed that it will work.

The second type of ransomware is called locker-ransomware. This type of ransomware locks the victim's system and displays a login page. The victim must pay a ransom to receive a password to unlock the system. Locker-ransomware is considered less dangerous because the attack can often be resolved by restarting the system in safe mode, followed by running anti-virus software.

Typically, a locked system allows only limited access, forcing the victim to interact only with the initiator of the attack. Keyboard sections may be locked or the mouse may be frozen, effectively only allowing the victim to respond to the ransomware's demands. Locker-ransomware usually does not penetrate the entire computer network and does not attack the files in the computer. This aspect makes it easier to find this type of ransomware and remove it without paying the ransom.

Locker-ransomware uses non-encrypting malware to lock the infected machine, whereas encryption ransomware uses encryption to lock the infected computer or device. As with crypto-ransomware, there is no guarantee that access to the computer or device will be restored after paying the ransom, even if the pop-up message says it will. On the contrary, many business owners who pay the ransom never get back access to their computer or device.

The third type, which does not carry such a danger compared to the discussed ones, is called scareware. This type of ransomware poses no real danger to its victim. Its main function is to scare the victim into paying the ransom. The cyberattack tactic of scareware ransomware is to scare people into visiting fake or infected websites or downloading malware. Scareware can take the form of pop-up ads that appear on a user's computer or spread through spam email attacks.

A scareware attack is often launched by pop-ups that appear on the user's screen, warning them that their computer or files are infected and then offering a "solution of the problem". This social engineering tactic is

intended to scare people into paying for software that supposedly provides a quick fix of the problem. However, instead of fixing a problem, scareware actually contains malware programmed to steal a user's personal data from their device. Scareware can also be spread through spam emails, through messages that trick people into buying useless items or services.

As the Linux operating system becomes more popular and more businesses than ever run on Linux now, Linux-oriented ransomware attacks are increasingly attacking Linux users and accumulating exorbitant profits. The Erebus ransomware affected about 3,400 of NAYANA's customers through advertisements containing malware. The Lilocked ransomware targeted Linux servers and gained root access to encrypt files with extensions like .php, .html, .css, etc. Victims were directed to the dark web to make a payment in Bitcoins to recover their files. Linux-targeted ransomware compared to ransomware targeting the Microsoft Windows operating system has not had a major impact on enterprises and individual users till soon. However, this situation is changing as ransomware producers are always driven by profits. It is inevitable that more companies and people in the industry will use Linux systems due to their security, stability, and open source, which will tremendously lead to the generation of a lot of ransomware targeting the Linux operating system. Due to the fact that crypto-ransomware are classified as the most dangerous of the three main types and the popularity of Linux as an operating system, the object of our research is to describe and prove an approach to recover files after GonnaCry infection in a Linux distribution of Debian is version 11.

Infecting Linux Based Machine with Crypto-Ransomware and Restoring User Files

Infection with crypto-ransomware is accomplished through a simple initial vector attack. We already discussed that the most widespread method for this is through phishing emails, you bet on the ignorance of the user, and mostly these attacks are aimed to users with Windows-based systems which are used significantly more for workstations. Analysis shows that for the Linux operating system, infections occur most often through old system vulnerabilities, key gaps in the provided services that make it easier to access and compromise the target system.

The simple example with GonnaCry Rasomware shows all the necessary characteristics for the effective execution and mass distribution of a piece of malicious code:

- Low memory consumption to avoid encryption overhead. This way, the user will find out that he has become a victim of an attack as late as possible.
- Ability to restore files only with the private key from the control server.
- Distribution and self-recovery plan when the encryption process of the target files stops.

The first stage of the attack is the analysis, which includes indexing all accessible files and trying to spread them, both locally on the already compromised machine and also on the local network. The major priority has the user files and the backups. Figure 2 illustrates the synchronization of user files with the cloud folder, in order to prove the proposed method for data recovery. Replication of the virus occurs at two levels, the first is local to the compromised machine, while at the same time the network is scanned for vulnerabilities through which the virus can penetrate other workstations in the organization.

After the analysis and compromise part of the maximum number of workstations is completed, encryption follows using a symmetric file encryption algorithm. For this purpose, GonnaCry uses an AES cipher, due to its high speed and efficiency. For each of the resources targeted by the attack, a public key, a private key and the location of the file to be encrypted are recorded. This list with information about the encrypted files is used to decrypt them when the ransom is paid. Once the file encryption process reaches a certain stage, depending on the virus that has penetrated the system, the original copies of the files are deleted. NextCloud support double delete functionality where deleted files are moved to “Deleted files” (Figure 3). To be deleted from the server, they must be deleted from there as well, and can be restored from the same place.

The file may be overwritten with zeros and then deleted depending on the crypto-ransomware. This action aims to avoid the possibility of data recovery with deep scan software for deleted files. Even if the file is not overwritten with zero, these types of software are not effective because of the large amount of data that is overwritten on the hard disk. In this situation, after restoring the file from "Deleted files", a previous version will need to be restored for each file.

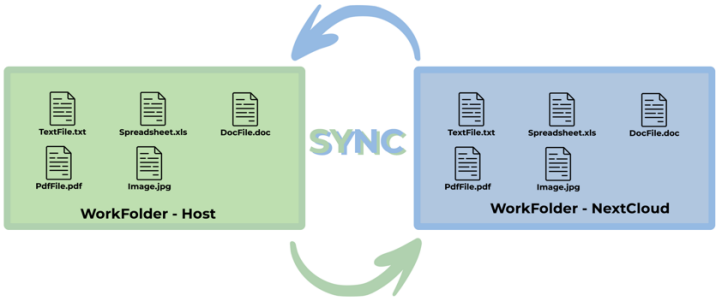

Figure 2. Synchronizing local folder with cloud folder

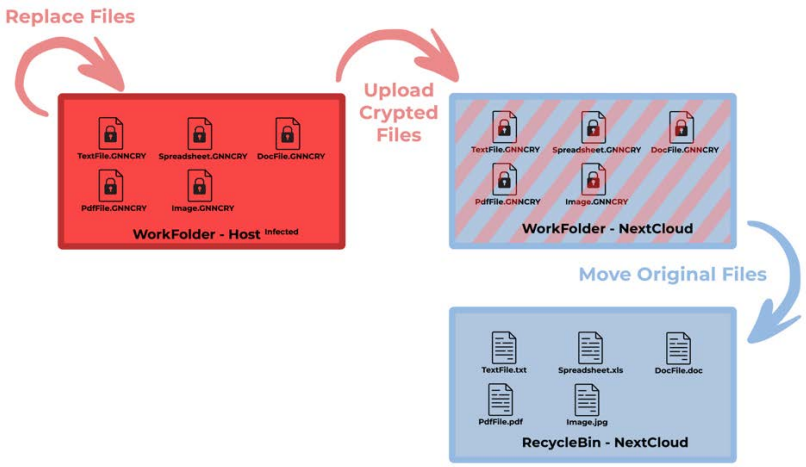

Figure 3. Upload process of the corrupted data to the cloud.

The final stage is when all files are encrypted and the file list contains the decryption data for each compromised file. This list is encrypted using the RSA algorithm for higher security and eliminating the possibility of decrypting the file itself. A file with the public key, as well as information about the requested ransom is shown to the user. Thanks to the public key, if the ransom is paid, a private key is obtained, which is kept by the attacking organization. The public key information and ransom payment instructions are usually in one of the following or similar files: READ_IT.txt, READ_ME.txt, info.txt, info.html, More.html, recover.txt, README.HTML, wallpaper. jpg, start.txt, Instructions.html, DECRYPTION.txt, ReadMe.txt, w.jpg, READ_ME.TXT, motd.txt, desk.jpg and others. Paying the ransom does not guarantee the receiving of a private key, nor does it guarantee the recovery of all data. The following figure (Figure 4) shows infected user files on the attacked machine.

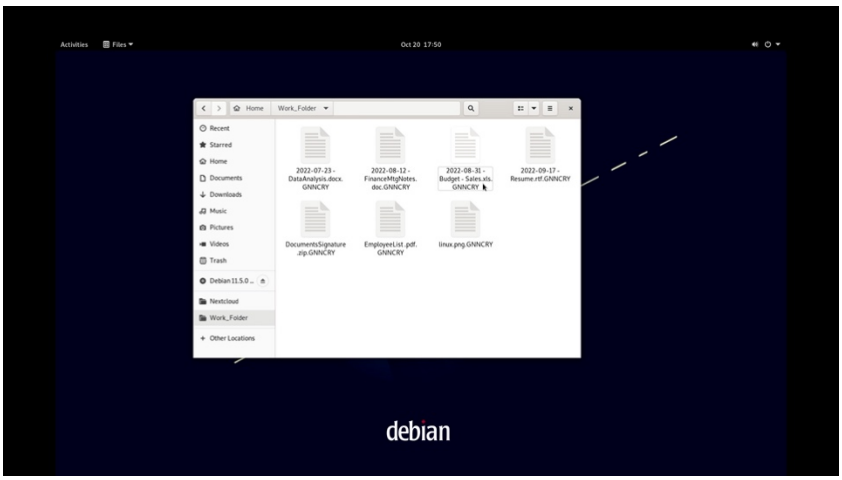

Figure 4. Corrupted files

Before proceeding to recovery, it is recommended to clean the infected device and then recover the deleted files, using NextCloud WEB from “Deleted Files” and restore previous versions for each file if it is necessary (Figure 6). The process is illustrated in Figure 5.

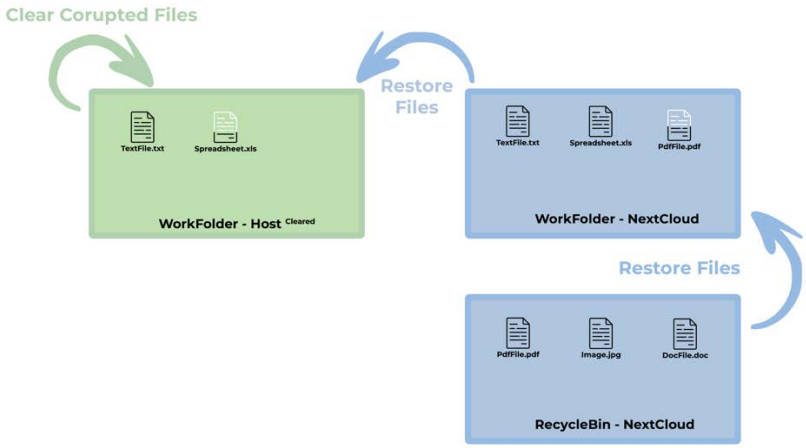

Figure 5. Process of deleted data recovery from the cloud

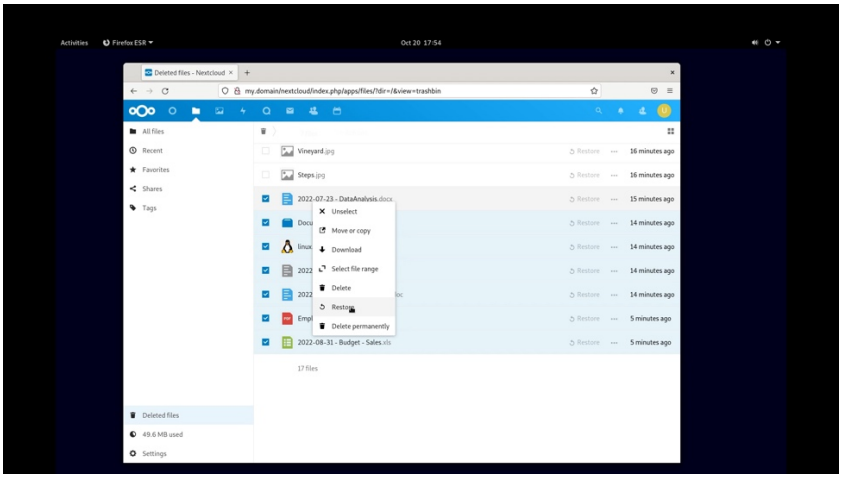

Figure 6. NextCloud deleted files

Describing a Method for Data Recovery

The method we used to recover the files after infecting a Debian Linux operating system machine with GonnaCry crypto-ransomware is the same as shown in previous research (Hristev et al., 2022) in which we prove the possibility of recovering encrypted files with CERBER in Windows operating system crypto-ransomware system using NextCloud. As a result of the two studies, we can conclude that the described method works for Windows and Linux workstations after being infected with crypto-ransomware and we can recover user data as follows:

1. Identifying the compromised departments in the infrastructure – First, it is necessary to discover how many workstations in the infrastructure have been compromised and infected with crypto-ransomware. Usually, it is one or a group of computers from a specific department, depending on the attack. There is a possibility that infected computers can be in more than one department.

2. Isolation of Compromised Devices - Once infected computers have been identified they must be isolated. Skipping this step would introduce a loop in the method because after recovering the files through the private cloud, the compromised devices would re-encrypt the recovered files.

3. Identifying and analyzing the breach - It is recommended to analyze how the crypto-ransomware penetrated the IT infrastructure and if it is possible establish policies and rules to limit the possibility of re-infection in the future.

4. Cleaning a Compromised Devices - Compromised devices should be cleaned of the crypto-ransomware. Companies that develop anti-virus software are pouring more and more funds into updates to clean computer systems of such threats. Once the virus is identified, we can check the internet for products that can

detect the infection and clear it. If we can't find a tool to fix the problem, there is always the option of reinstalling the infected machines.

5. Recovering of the files - Depending on the type of crypto-ransomware we are infected with, the NextCloud network offers two built-in options through which we can recover the files.

Most crypto-ransomwares, including GonnaCry for Linux based operating system and CERBER for Windows based operating system encrypt entire files by deleting the original copies of the files. In this situation, the data can be recovered thanks to the double deletion approach. Every deleted file is moved to the "Deleted files" in order to delete a file from the server, it must also be deleted from the recycle bin itself, and only then will it cease to exist.

If the attacking crypto-ransomware overwritten the file with zeros , we can restore it through Versioning Control of the private cloud. In this situation we need to restore each file to its previous version. Depending on the encryption algorithm that is used by the infected virus, an important feature is that the encrypted file is larger than the original one. In the general case, the encrypted file is about 30% larger than the uncompromised data. I.e. to ensure the safe storage of 100 GB of data, NextCloud must have more than 230 GB of free space. Thus, the first 100GB will be used to store the files before the encryption and the other 130GB will be for the encrypted files. We can install a Ransomware protection add-on on the NextCloud server. The add-on will not protect us from being infected with crypto-ransomware, but it will prevent uploading on the server encrypted files. The plugin tracks file extensions that users upload to the server. When we are using the add-on we must always keep it updated to the latest versions. Some of the crypto-ransomware extensions are not described by default and in this situation, the NextCloud server administrator needs to maintain the extensions manually. As new crypto-ransomware are constantly emerging which rename infected files with different extensions this is a difficult task (Hristev et al., 2022) and (Hristev et al., 2021).

When NextCloud works with shared files, it does not matter who is the owner of the original file. The deleted file must be searched for in the recycle bin of the user who deleted it or in the users that the compromised computers work with on the network.

6. Deleting the files created by the crypto-ransomware - The last step that needs to be done before going back to normal operation mode is to delete the files that were encrypted by the crypto-ransomware. Encrypted files must be deleted from the directories and also must be deleted from Deleted files to cease to exist on the server.

Conclusion

The challenges facing consumers and industry in the 21st century as a result of the declaration of a pandemic bring with it even more difficulties than we can imagine. The situation gave cybercriminals the green light. More than 7 years after the first ransomware for Linux was disclosed, now machines with Linux-based operating systems became more and more attractive to cyber criminals. More massive attacks occurred targeting Linux appear recently. Every day, many users become victims to crypto-ransomware attacks more than ever. The study gives a method for data recovery on Linux-based operating system machine with Debian version 11 distribution after user files infection with crypto-ransomware. The user's data is stored on the private cloud and synchronized with a controlled workstation that is infected with GonnaCry. It is proved that the proposed approach can be used successfully for recovering data after crypto-ransomware attack.

Scientific Ethics Declaration

The authors declare that they are responsible for the scientific, ethical, and legal aspects of the paper published in EPSTEM.

Acknowledgements

* This article was presented as an oral presentation at the International Conference on Technology (www.icontechno.net) held in Antalya/Turkey on November 16-19, 2022.

* Rosen Hristev is supported by Fund MU21-FMI-007, University of Plovdiv "Paisii Hilendarski". Magdalena Veselinova is supported by Fund MU21-FMI-009, University of Plovdiv "Paisii Hilendarski".

References

Hristev, R., & Veselinova, M. (2021). ICT for cyber security in business. *IOP Conf. Ser.: Mater. Sci. Eng. 1099 012035*.

Hristev, R., & Veselinova, M. (2022). Using private cloud for information arrays recovery from ransomware attacks. *AIP Conference Proceedings 2505, 060006 (2022)*.

Lallie, H. S., Shepherd, L. A., Nurse, J.R.C., Erola, A., Epiphaniou, G., Maple C., Bellekens, X. (2021).Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security.Volume 105,102248.*

OpenVault. Broadband insights report (OVBI), 4Q21. Retrieved from https://openvault.com/wp-content/uploads/2022/03/OVBI_4Q21_Report_FINAL-1.pdf. Accessed 25 Oct 2022.

Schulze, H. (2022). VPN risk report. Retrieved from https://vpnoverview.com/wp-content/uploads/2022-zscaler-vpn-risk-report.pdf

Sophos (2022). The State of Ransomware in Retail 2022. Retrieved from https://assets.sophos.com/X24WTUEQ/at/ms85vsqz3sx9tnmnkh3bp5r/sophos-state-of-ransomware-retail-2022-wp.pdf

Sushruth, V., Rahul Reddy, K. & Chandavarkar B. R. (2021). Social engineering attacks during the COVID-19 pandemic. *SN COMPUT. SCI. 2, 78.*

Tawalbeh, L., Muheidat, F., Tawalbeh, M., Quwaider, M. & Saldamli,, G. (2020). Predicting and preventing cyber attacks during COVID-19 time using data analysis and proposed secure IoT layered model. *2020 Fourth Inter"national Conference on Multimedia Computing, Networking and Applications (MCNA)*, 113-118.

Author Information

Rosen Hristev
University of Plovdiv Paisii Hilendarski
236, Bulgaria Blvd., Plovdiv 4027, Bulgaria
Contact E-mail: *hristev@uni-plovdiv.bg*

Magdalena Veselinova
University of Plovdiv Paisii Hilendarski
236, Bulgaria Blvd., Plovdiv 4027, Bulgaria

Kristiyan Kolev
University of Plovdiv Paisii Hilendarski
236, Bulgaria Blvd., Plovdiv 4027, Bulgaria

To cite this article:

Hristev, R., Veselinova, M. & Kolev, K. (2022). Ransomware target: Linux. Recover Linux data arrays after ransomware attack. *The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM), 19*, 78-86.