International Journal of Differential Equations and Applications
Volume **21**, No. 2 (2022), pages: 19-29
ISSN (Print): 1311-2872; ISSN (Online): 1314-6084;
url: https://www.ijdea.eu

CRYPTO-RANSOMWARE ATTACKS ON LINUX SERVERS: A DATA RECOVERY METHOD

Angel Golev[1], Rosen Hristev[2], Magdalena Veselinova[3], Kristiyan Kolev[4]

[1,2,3,4]Department of Mathematics and Informatics
University of Plovdiv Paisii Hilendarskiy
236, Bulgaria Blvd., 4000 Plovdiv, BULGARIA

ABSTRACT: More frequent and large-scale attacks against Linux servers and the services provided by them are the forecasts of the analysts. Proof of this is the double-digit increase in attacks against Linux server environments has been registered in the first part of 2022. This is of course no accident. Linux server environments are used for corporate and government networks, web services, and large arrays of databases owned by organizations that can afford to pay to restore operations and critical data after an attack. Regardless of the size, almost every organization implements cloud technology in some way in their business. Organizations must to determine which cloud model is most suitable for them based on the way of working and the data that is stored and processed. The research consider the advantages and disadvantages of using two of the main cloud infrastructure models - public and private clouds. The used classification of the cloud models is according to the ownership and users using the infrastructure. The used crypro-ransomware for the purpose of the research is GonnaCry. An overview of how this malicious code example works is provided, too. After the infection, two approaches have been proposed to recover the data in the server environment - through the web interface of the private cloud, as well as created a bash script that can be used in high load infrastructures.

Key Words: Ransomeware, Linux server, Cryptovirus, Cyber Security, Private Cloud, Backup, Decrypt, Exploit, Encryption

Received: August 20, 2022 **Revised:** November 2, 2022
Published: November 11, 2022 **doi:** 10.12732/ijdea.v21i2.2
Academic Publications, Ltd. https://acadpubl.eu

1. INTRODUCTION

The challenges facing IT departments to ensure the integrity of data in infrastructure are increasing. Undoubtedly, one of the biggest challenges is dealing with different types of attacks. The majority of specialists are worried about the infection of crypto-ransomware into the infrastructures entrusted to them. At first, cybercriminals using crypto-ransomware focused on encrypting the data on the compromised computer. Over time viruses evolved gradually scanning the machine for unprotected shared resources in addition to the compromised computer. The resources most often covered up to this point are shared directories. In practice, companies that do not work with shared resources to facilitate communication and data transfer between employees are units. Resources in infrastructure are most often shared through different NAS (Network-attached storage) and SAN (Storage Area Network) devices or through the Samba protocol. Once the crypto-ransomware detects such resources, the data stored in them is also encrypted. In our previous research [1], we have proven the possibility to recover this type of data thanks to a private cloud. For this purpose we infected Windows and Linux workstations, then we recovered the data that was stored simultaneously on the servers and workstations.

Standard crypto-ransomware distribution methods, such as phishing attacks, are not good enough to infect and compromise the data stored on database storage servers and application servers. The reason for this is that the people accessing them are technically literate, and these are not machines that are normally used for email etc. This is the reason that more and more crypto-ransomware in addition to scanning the computer for shared directories, also scan the network as well as all available resources in order to leave more damage on the infrastructure. Typically, the manipulation of the data in database servers or application servers occurs thanks to vulnerabilities in the operating system running the server or some of the other software equipment required to run the server. Some of the crypto-ransomeware also look for backdoors in certain poorly protected applications, and open source projects or poorly protected libraries that are used for the development of a given project.

Most infrastructures rely on data recovery from existing backups, as with file storage servers. Backups are vulnerable also, they are because they are targeted by crypto-ransomware to be encrypted., too. In addition, even if the archive is not encrypted, most likely the data from the last backup up to the time of infection will be lost. This is what makes even the best-known backup method 3-2-1 not flexible enough for part of the cases.

In our research, we have proven that shared files used by a company can be protected and recovered after being infected with crypto-ransomware thanks to a private cloud. In this research, we will restore an application server and a database server after being infected with crypto-ransomware. We will infect Linux Debain with GonnaCry crypto-ransomware. On the server, we will have a WordPress instance installed with the website's database. The differences between private and public clouds will be considered with their advantages and disadvantages. Also, an alternative way to recover files on NextCloud will be described.

2. ADVANTAGES OF USING A PRIVATE CLOUD OVER A PUBLIC CLOUD

The cloud model infrastructures can be classified in different ways, depending on the service they offer and the owners and tenants of the clouds, respectively. In this section, we'll look at the two main classifications of cloud models, according to ownership and the users who use them. These are precisely the public and private clouds.

Public cloud infrastructure is available to the general public or a large industry group and is owned by an organization selling cloud services [2]. In public clouds, the resources are offered as a service, usually over an Internet connection. The service can be free or pay-per-use. Users can scale their usage on demand and no hardware purchase is required to use the service.

Public clouds are available to the general public and organizations with various measures and are owned by a third-party organization that offers the cloud service. The most common tenants of this model cloud infrastructure are end users, small and medium-sized companies, as well as companies developing open source and mobile applications. The public cloud is hosted over the Internet and is designed to be used by any user with an Internet connection to provide a range of capabilities and services. Google, Amazon, and Microsoft are examples of providers of public cloud infrastructures that offer their services to the general public [3].

One of the main disadvantages of using public clouds is that users do not know where their data is stored, what the backup policy is, and whether unauthorized users can access it. Reliability is an important concern for public cloud infrastructures. A public cloud interruption can leave many large websites, online stores, etc. inactive or completely unavailable. Public cloud service providers usually do not reflect privacy and security needs of a particular organization. An understanding of the context in which the organization operates in terms of the risk and consequences of unauthorized

access and other real-world threats is necessary for cloud service compliance.

The biggest obstacle to public cloud infrastructures is security. Service decision-making and service arrangements require balancing cost and performance benefits against risk and liability disadvantages [4]. In the presence of sensitive data stored and processed by the organization, the probability of outsourcing all information technology services to a public cloud is very low.

The cloud computing paradigm provides opportunities for innovation in the provision of security services that have the prospect of improving the overall security of organizations. A major benefit of using a private cloud is security. Private cloud infrastructure is owned or leased by an organization and used only by that organization. It can be managed by the organization or a third party. The cloud infrastructure is accessible only by members of the organization or only by users with given access to it. The purpose of the service is significantly different compared to public cloud infrastructures. Intended for use within the organization. Typically, a private cloud is hosted in an organization's data center.

A private cloud provides more security than a public cloud. The private cloud has the potential to give an organization greater control over the infrastructure and computing resources at its disposal [5]. There are researches that suggest using private clouds results in lower operating costs compared to using public cloud infrastructures. In fact, all cloud models offer similar benefits as there is not much difference in technology. The most valuable resource an organization has is probably its data. The most significant advantage that a private cloud has over a public cloud is data security and privacy. The private cloud's ability to virtualize services significantly increases the utilization of available hardware, resulting in cost reductions. We can mark that the main disadvantage of the private cloud is its high price. Compared to a public cloud the cost of purchasing equipment, software and employees often results in higher costs for an organization that has its own private cloud.

3. GONNACRY OVERVIEW

Much to the dismay of Linux sysadmins and users, the past few years have been saturated with emerging malware campaigns targeting Linux servers. These attacks demonstrate new and dangerous tactics for spreading and compromising servers. Although it represents a small sample of emerging malware targeting Linux systems, GonnaCry is an example of the rapid evolution of malware targeting Linux. GonnaCry is a Linux crypto-ransomware variant that is under active research development. In [6] for eval-

uating the network-assisted approach used for ransomware detection, docker was used to establishing the experimental environment and GonnaCry to simulate a ransomware attack.

GonnaCry starts with finding the files it will encrypt. After identifying these files, they are added to a list that contains the full path to each file that will eventually be encrypted. Once it has the full path to each file, the crypto-ransomware begins its encryption routine. GonnaCry encrypts files with AES-256-CBC. After encryption, the old file must be destroyed so that it cannot be recovered. These files cannot be recovered using recovery software tools. The next stage is to create a desktop file that will help the decryptor to access the path and key used to encrypt each file. This file must be encrypted with the user's public key, and the user's private key must be encrypted with the server's public key, which is hardcoded to the ransomware. The private key is encrypted with RSA-1024 by the server. The user can easily decrypt its files if this file is not encrypted. The ransomware then releases the memory allocated by the computer's files.

4. SERVERS DATA RECOVERY AFTER CRYPTO-RANSOMWARE ATTACKS

When a server is infected, it is not advisable to start immediately with its recovery and return to production mode. First, we need to isolate the compromised system and analyze both the infected system and the surrounding servers and users had access to it. Self-propagation is a key feature of successful attacks. Malicious code self-replicates to all available local resources and multiple times in case it is detected and removed to bring back itself.

The self-replication of the malicious code makes attacks successful by spreading the malicious code across local devices, analyzing and accessing resources with the aim of causing extensive damage to the infrastructure. Therefore, our infected server may not be primary source the virus into the work environment. If we immediately start to recovery, it is possible to get infected again and thus go into a cycle of encryption and recovery, wasting valuable time and resources. In addition to isolating the server, we need to undertake extensive monitoring of the resources that have been accessed to and from the infected machine. It is mandatory to analyze the malicious code and identify the vulnerability through which it was able to infect in order to remove it from our infrastructure and avoid future infections.

Our experience with crypto-ransomware that affects machines with Linux-based

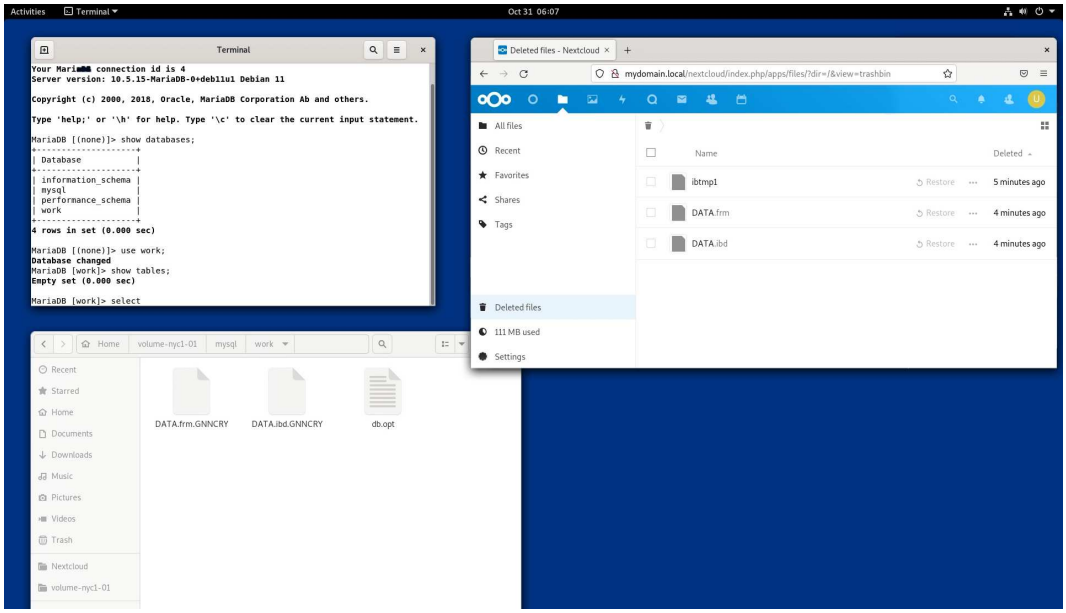

Figure 1: Infected Server Environment

operating systems shows that Lilu/Lilocked implements its attacks using old vulnerabilities in Exim (mail transfer agent), which through CVE-2019-13917 [7] & CVE-2019-15846 [8] allows attackers to execute arbitrary code as root via a trailing backslash. One of the most affected distributions is openSUSE LEAP 15.0 and 15.1 delivered in their Exim package. These flaws are enough to encrypt only some extensions like HTML, CSS, PHP, INI, and all image formats, but enough to do the desired damage.

Linux.Rex.1 has a similar implementation logic. Again by scanning for vulnerabilities, but on the provided web services, such as Wordpress, Magento, CMSs, JetSpeed, etc. The malicious code manages to deploy to the server and start searching the available file system for passwords and keys so that it can elevate its privileges using sudo, su, or SSH connections. Then it self-replicates and builds an entire botnet network. It is found by analyzing an infected machine, that it receives directives from a P2P network over HTTPS protocol on port 5099 and then transmits them to local nodes via RPC.

Detailed research of the crypto attack and how it spread throughout our infrastructure will provide us with key information we need to understand how malicious code is executed and replicated. This information would help to prevent new infections, and upcoming attacks and completely eliminate the crypto-ransomware from our environment. We can move to the full recovery stage after we locate and fix the vulnerabilities in our infrastructure.

Through the Nextcloud web interface, we can track the files versions that have occurred over time, as well as their encryption. During the attack, the crypto-ransomware reads our files and creates an encrypted copy of them using high-speed AES encryption, which makes the files up to 30% larger in volume. Thus, recovery by software for deleted files is almost impossible, because the hard disk has other information written on the corresponding blocks. Thanks to synchronization, we can restore the original content of our files through version control or, depending on the attack method, restore them directly from Nextcloud's "Deleted files". Figure 1 shows locally encrypted data and original deleted files kept in the cloud. After the successful restoration of our data, normal server operation can be resumed and we can return it to production mode.

5. RECOVERY OF LARGE VOLUMES OF DATA

We can have many different setups depending on the data that will be stored in the private cloud and the number of users that will work with it. As described in our previous research [9] for organizations with up to 150 users we can store the database, web server, and storage on one physical or virtual machine. In situations where the private cloud is expected to be used by more users, the configuration can be scaled to multiple servers. Under intense load and improperly planned infrastructure in advance for NextCloud, it is possible to start slowing down some of the non-critical functionalities of the application. In addition, it is possible to observe a delay in the operation of the web-based part of the application.

Our previous research on crypto-ransomware recovery has looked at the possibility of recovering the files via the web interface. On servers with a higher load, the web interface of the server may run significantly slower, this in turn would lead to difficulties in recovering the encrypted files and deleting the encrypted files from the crypto-ransomware and would take a lot of time. NextCloud and OwnCloud store their files in directories, with the following structure available for each user:

- cache
- files - stores the user's files
- files_encryption - stores the user's encrypted files, with the encrypted file storage module enabled
- files_trashbin - files deleted by the user
- files_versions - the versions of the files that the user created

- uploads

The three directories that are more important in this case are: files, files_trashbin, and files_versions, and their structure is available for each user. Normally, unless otherwise selected by default, this structure is stored in <nextcloud folder>/data/user/...

In addition to a web-based interface, both clouds also have an Own Cloud Console (occ) thanks to which part of functions are also accessible from the shell, which can greatly facilitate the administration of this type of cloud. Despite numerous requests from users to develop occ functionality to recover files from Deleted Files, none has yet been developed.

On a file system basis, after a user deletes a file or directory files in the files_trashbin/files directory, the versions of the corresponding files are moved from files_versions to files_trashbin/versions. To ensure the uniqueness of easier identification, an 11-character postfix is added to their names, which for a file/directory is the same as that of its versions.

We first need to move the contents of the files_trashbin/files and files_trashbin/versions directories to temporary directories to recover files from Deleted Files. Files and versions will be renamed and the last 12 characters (dot + postfix) removed from their names. Since just moving them from the two directories will not delete the corresponding records in the cloud database, which would lead to the accumulation of redundant information and subsequently errors, we can rescan the files that are in the trash thanks to occ with the command php occ trashbin :cleanup <username> for the corresponding user.

After the trash is scanned and the information is updated, we can return the data from the temporary directories to files and files_versions respectively. The rights and ownership of the relevant files should be fixed, then with the command php occ files:scan –all, to rescan corresponding directories and add the files again to the database.

The entire script that can be used to recover data without using a web interface is as follows:

```
#!/bin/bash
mv /var/www/html/data/$1/files_trashbin/files/* /root/files/
mv /var/www/html/data/$1/files_trashbin/versions/* /root/versions/

ls /root/files > /root/filenames
ls /root/versions > /root/fileversions

cd /root/files
```

```
file="/root/filenames"
while IFS= read -r line
do
    mv -i "$line" "${line%?????????????}";
done <"$file"

cd /root/versions
file="/root/fileversions"
while IFS= read -r line
do
    mv -i "$line" "${line%?????????????}";
done <"$file"

cd /var/www/html
sudo -u www-data php occ trashbin:cleanup $1

mv /root/files/* /var/www/html/data/$1/files/
mv /root/versions/* /var/www/html/data/$1/files_versions/

chown -R www-data:www-data /var/www/html/data/$1/files/
chown -R www-data:www-data /var/www/html/data/$1/files_versions/
sudo -u www-data php occ files:scan --all
```

The script can be stored as an executable file in the /root directory named ncrestorefiles.sh. It is recommended to run it through a user with root access to the system. The script must be run with one argument, which is the name of the user whose files are to be restored from Deleted Files. It can be started with command ./ncrestorefiles.sh demo.

The script will restore all deleted files of the respective user. We recommend that a backup be made before using the script. It will not restore files correctly if the server data encryption module is enabled.

6. CONCLUSION

The past year has seen a significant increase in attacks by cybercriminals. Not only end users are targeted, but also server environments that provide services. Linux is among the most used operating systems by individual users and by organizations running

servers. Linux powers the Internet with most of all web servers running on it. This is the main reason why cybercriminals use crypto-ransomware attacks against Linux users. As crypto-ransomware is one of the most dangerous digital threats this is the reason the target of the presented study. The research observe advantages of using private cloud over public clouds. In the study, an application server and a database server are restored after being infected with crypto-ransomware. The used sample of crypto-ransomware is GonnaCry. Infected server runs Linux Debain with WordPress instance installed with the website's database. The data is stored on the private cloud and synchronized. A method for recovering the infected files using the private cloud web interface, as well as a method for recovering through a bash script, have been proven.

ACKNOWLEDGEMENTS

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

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

[2] Mell, P. and Grance, T. , The NIST Definition of Cloud Computing, *NIST Special Publication 800-145*, (2011).

[3] Mather, T. , Kumaraswamy, S. and Latif, S. *Cloud security and Privacy: An Enterprise Perspective on Risks and Compliance*, Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472, (2009).

[4] Goyal, S., Public vs Private vs Hybrid vs Community - Cloud Computing: A Critical Review, *I.J. Computer Network and Information Security*, 3, 20-29, doi: 10.5815/ijcnis.2014.03.03, (2014).

[5] Jansen, W. and Grance, T. Guidelines on security and privacy in public cloud computing, *NIST special publication*, 800-144, (2011).

[6] Xiaa, T., Suna, Y. , Zhua, S. , Rasheedb, Z. , Shafique, K., *Toward A Network-Assisted Approach for Effective Ransomware Detection*, arXiv:2008.12428v2 [cs.CR] 19, (2020).

[7] CVE-2019-13917, *Common Vulnerabilities and Exposures* Retrieved from https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-13917

[8] CVE-2019-15846, *Common Vulnerabilities and Exposures* https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-15846

[9] Hristev, R., Veselinova, M. ICT for Cyber Security in Business, *IOP Conf. Ser.: Mater. Sci. Eng. , 1099 012035,(2021).*