International Journal of Differential Equations and Applications
Volume **22**, No. 1 (2023), pages: 155-163
ISSN (Print): 1311-2872; ISSN (Online): 1314-6084;
url: https://www.ijdea.eu

ijdea.eu

DATA RECOVERY OF DATA STORED IN A PRIVATE CLOUD INFRASTRUCTURE WITH OWNCLOUD INFINITE SCALE

Rosen Hristev[1], Magdalena Veselinova[2], Eray Ismail[3]

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

ABSTRACT: This research examines the process of recovering data stored in a private cloud infrastructure using the capabilities of ownCloud Infinite Scale. As organizations increasingly rely on cloud solutions for data storage, security, and scalability, the need for effective data recovery mechanisms becomes paramount. This research examines the challenges associated with recovering data stored in a private cloud environment following an attack by a ransomware. After infecting the system with a cryptovirus, the data is recovered using ownCloud Infinite Scale. The research aims to present a method and tools related to data recovery in this cloud environment.

Key Words: Ransomware, Cryptovirus, Cyber Security, Private Cloud, Backup, Decrypt, Exploit, Encryption

Received: September 11, 2023 **Revised:** December 9, 2023
Published: December 12, 2023 **doi:** 10.12732/ijdea.v22i1.11
Academic Publications, Ltd. https://acadpubl.eu

1. INTRODUCTION

With the growing dependence of organizations on cloud technologies for data storage, security, and scalability, the importance of effective data recovery mechanisms becomes

crucial. Additionally, attacks on data stored and processed in IT infrastructures are significantly increasing each year. The third quarter of 2023 will be remembered as a new record for the ransomware industry, marking the most successful quarter ever recorded. All computer platforms capable of running software are susceptible to cyber attacks [1]. Windows is one of the most widely used workstation operating systems, making devices based on it the primary target of most hacker attacks. End-user knowledge is crucial, as people are the weakest link in the cybersecurity chain. The lack of user knowledge about cybersecurity risks is the cause of 50% of cyber attacks, and almost 90% of cyber attacks result from human behavior [2].

With the increasing dependence of organizations on the data they store and process daily, the aspects of availability and scalability are critically important for the smooth flow of normal business processes. There are many ways to achieve availability and scalability, but these aspects are interdependent, and solutions for their achievement must be carefully considered to optimize the outcome. OwnCloud Infinite Scale is microservices-based software, serving as a single or distributed instance. The concept of Infinite Scale is to function as a distributed service rather than a static monolithic block of services, thereby achieving availability and scalability [3]. OwnCloud Infinite Scale represents a new version of ownCloud developed specifically to offer these two aspects - scalability and improved performance. The main idea of ownCloud as a file management platform is to provide a cloud solution which allows organizations to store, share, and manage their data in a secure and controlled environment.

The research describes an approach to recover data stored in a private cloud environment after an attack by a ransomware. The focus is on data recovery using the capabilities of ownCloud Infinite Scale. To achieve this goal, a virtual machine running a Windows-based operating system in an isolated environment is infected with a ransomware. The research describes a method and tools to successfully recover the data after it has been encrypted and the original versions of the files have been deleted. Furthermore, with the results obtained in this research and based on previous research by the same authors, it is shown that the proposed method works for the more general case where we do not depend on the operating system and the ransomware that infected the system.

2. RANSOMWARE OVERVIEW.

The cryptovirus that will be used to infect the virtual machine in this study will be Thanos. Thanos was created in 2020 and has become the leading malware used by low

and mid-level cybercriminals [4]. It is part of a class of ransomware known as RaaS (Ransomware as a Service) where attackers can customize it for their desired target audience. Studies have shown that there is no guarantee that the files will ever be decrypted, even after a ransom is paid. This variant of Thanos writes a ransom note to a file named "HOW_TO_DECYPHER_FILES.hta" on the desktop and in every folders that contain files encrypted by Thanos, as shown in Figure 1.

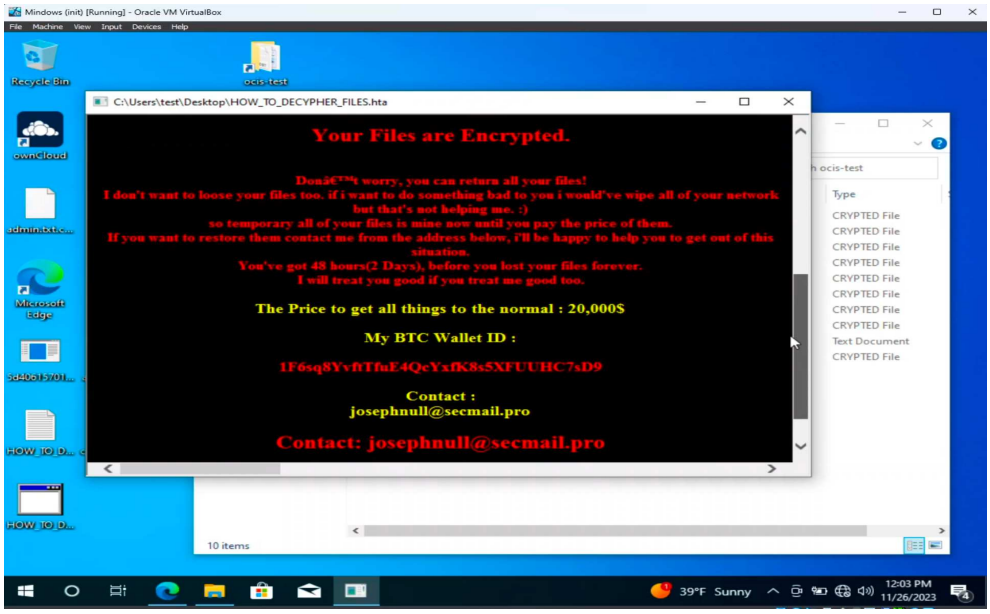

Figure 1: Thanos Encryption Message

Thanos allows users to customize or add to the default list of target file extensions to be encrypted. The list of target file types for Thanos can be as follows:

dat, txt, jpeg, gif,j pg, png, php, cs, cpp, rar, zip, html, htm, xlsx, xls,avi, mp4, ppt, doc, docx, sxi, sxw, odt, hwp, tar, bz2, mkv, eml, msg, ost, pst, edb, sql, accdb, mdb, dbf, odb, myd, php, java, cpp, pas, asm, key, pfx, pem, p12, csr, gpg, aes, vsd, odg, raw, nef, svg, psd, vmx, vmdk, vdi, lay6, sqlite3, sqlitedb, accdb, java, class, mpeg, djvu, tiff, backup, pdf, cert, docm, xlsm, dwg, bak, qbw, nd, tlg, lgb, pptx,mov, xdw, ods, wav, mp3, aiff, flac, m4a , csv, sql, ora, mdf, ldf, ndf, dtsx, rdl, dim, mrimg, qbb, rtf, 7z.

Thanos ransomware is most commonly distributed through phishing emails that include fake financial information, such as tax recovery data, invoices, etc. The ransomware is the first which use the researcher-disclosed RIPlace anti-ransomware evasion technique, in addition to other advanced features that make it a serious security threat. Most ransomwares are written in C# and do not possess a high level of complexity. On the other hand, Thanos is written in .Net and has numerous advanced features

that make it more lethal than others. Thanos is the first ransomware family to employ the RIPlace tactic. RIPlace is a Windows file system technique that can maliciously modify files, allowing attackers to bypass various ransomware mitigation methods.

3. INFECTION

One of the most widely used methods of ransomware infection is through phishing emails [5]. The most common victims of cryptovirus attacks are users with Windows-based operating systems, which are used significantly more on workstations compared to other operating systems. The lifecycle, behavior, and detection techniques of ransomware are discussed in [6] Techniques for preventing ransomware infection are explored in [7].

In an isolated environment, a virtual machine with Windows 10 installed was created. User data is stored in a private cloud environment. The used private cloud is ownCloud Infinite Scale, version 4.0.2. The virtual machine has a synchronized directory with the private cloud, through which the user will access the files they process. This configured virtual machine is infected with the Thanos ransomware.

The first stage of the attack is analysis, which involves indexing all available files and attempting to spread both locally on the already compromised machine and within the local network. The primary targets are the user's files and backups. Figure 2 illustrates the synchronization of user files with the cloud folder.

By default, Thanos uses a random 32-byte string generated at runtime as the password for AES file encryption. The string is then encrypted with the ransom operator's public key and added to the ransom note. Without the corresponding private key, recovery of the encrypted files is impossible. The basic execution path of Thanos involves three main activities:

1. Advanced Settings: Performs actions related to configuration settings. This initial phase primarily consists of executing the advanced options set during the build. These actions include tasks such as Killing Defender and Anti-VM.

2. Prevention of Virus Termination and Recovery: Halts services and processes that impede its ability to operate, deleting backup files and shadow copies of files. After the client performs the configuration actions, it will execute a series of tasks to ensure its successful startup and to delete backup copies and shadow copies of files.

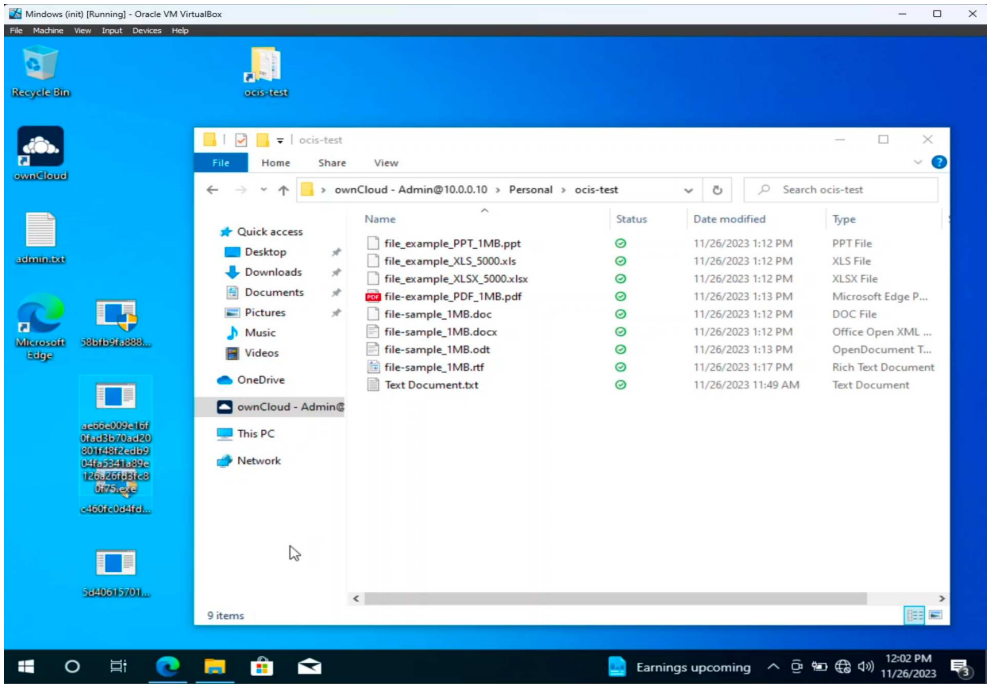

Figure 2: Synced User Folder

3. Encryption and Upload: Encrypts files and uploads them if configured to do so during creation, displaying the ransom note. Finally, the Thanos client will traverse connected storage drives and attempt to locate and encrypt files with file extensions configured in the builder. If the option to upload files to an FTP server is activated, then files with extensions matching the list configured during construction will be uploaded before encryption. The extensions of the encrypted files are altered, with the default value being ".crypted," as shown in Figure 3.

4. DATA RECOVERY

Most ransomware, including Thanos for Windows-based computers, encrypt entire files by deleting the original copies of the files. In this case, data can be recovered thanks to the double-deletion approach. Each deleted file is moved to the "Deleted files", and to erase the file from the server, it must also be deleted from the Recycle Bin, only then will it cease to exist. OwnCloud Infinite Scale has built-in mechanisms that will help us recover data in this way. Every infected and practically deleted file will be moved to the server's Deleted Files and stored there until it is permanently deleted by the module or

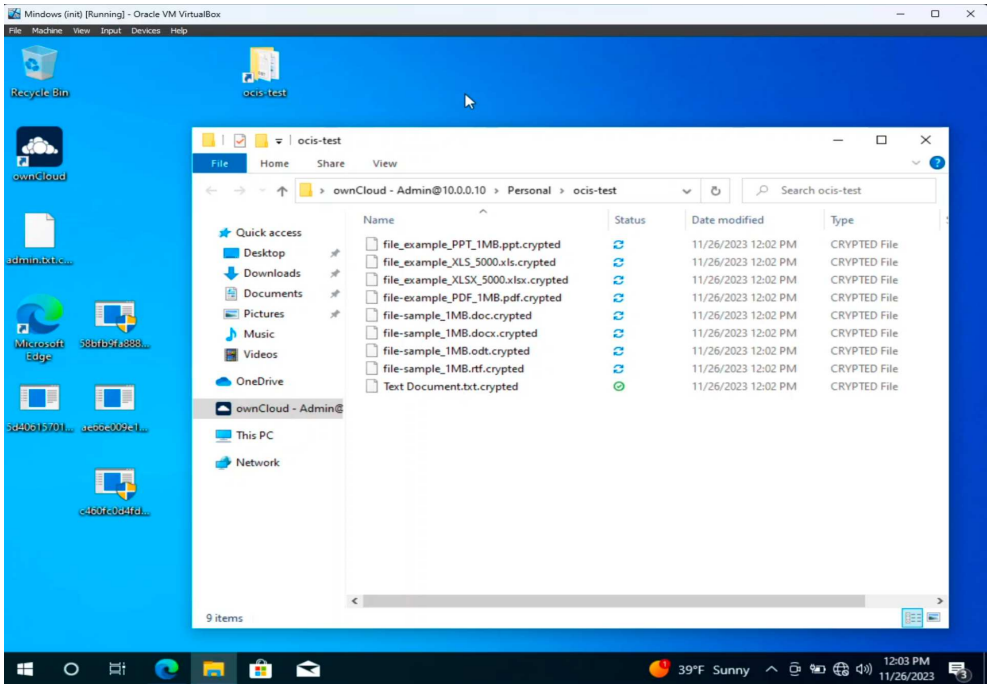

Figure 3: Encrypted files

the server's file system, as shown in Figure 4. When sharing files among multiple users, the ownership of the files does not matter for the system. The unencrypted data will be stored in the user's "Deleted Files" from whom the synchronization of the compromised machine is being performed [5].

Depending on the encryption algorithm used by the ransomware, the size of the data may increase by up to 50%. Since the encrypted data will also be uploaded to the server, to ensure the recovery of files after infection with malware, it is necessary to ensure free space on the ownCloud Infinite Scale server in advance. To calculate the required free disk space, we can multiply the size of the files with a coefficient of 1.5. The free disk space should be more if we have activated features for storing data on the server in encrypted form for greater security. In infrastructures that store large volumes of data, this can be a resource-intensive process. To ensure that the integrity of the data is not compromised, it is recommended that the server has allocated resources on the hard disk.

As a result of the conducted experiment, it can be concluded that data recovery stored in a private cloud environment ownCloud Infinite Scale is possible for workstations with a Windows-based operating system. The recovery of user data involves the following steps:

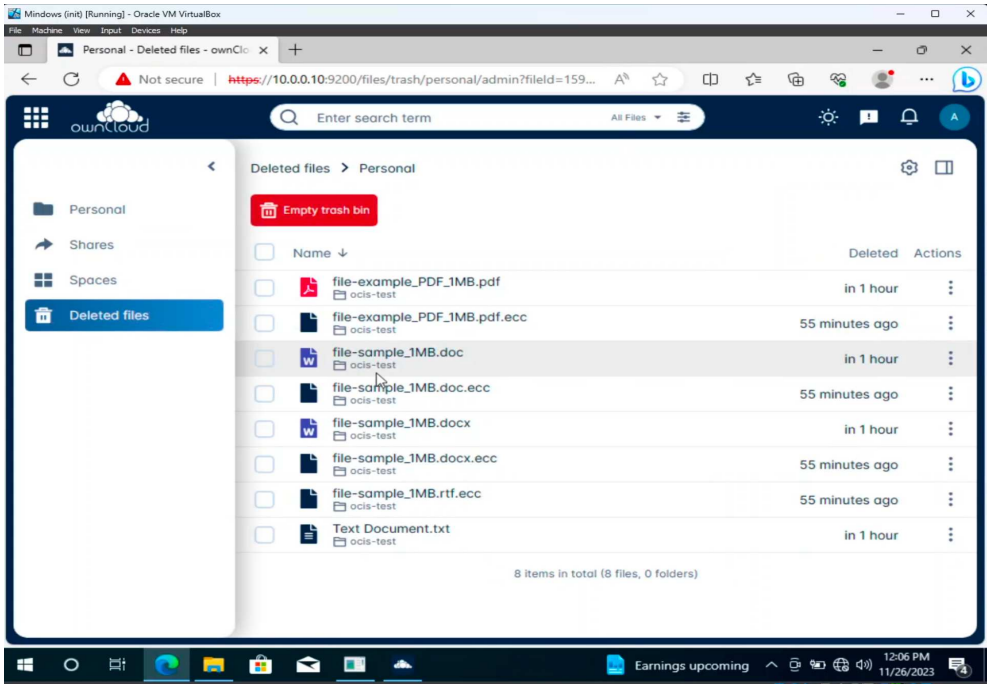

Figure 4: ownCloud Infinite Scale User Deleted Files

1. Identification of compromised elements in the infrastructure.
2. Isolation of compromised devices.
3. Identification and analysis of the ransomware and the method by which it infiltrated the IT infrastructure.
4. Cleaning compromised devices from the ransomware.
5. Recovery of files through the double-deletion approach.
6. Deletion of files created by the ransomware, both from directories and from the server's Deleted Files.

5. SUMMARY OF RESULTS.

In previous researches of the same authors, experiments were conducted on infecting both user workstations and server environments with ransomware. In [8], a user workstation with a Windows-based operating system was infected with the CERBER

ransomware. User files were stored in a private cloud infrastructure, and for the specific research, NextCloud version 21.0.1 was used, employing the same approach as in the current article. User files were successfully recovered using the Deleted Files module. In [5] a user workstation based on Debian Linux was infected with the GonnaCry ransomware, utilizing the same type of private cloud for storing user files. Recovery in this situation was also successful using the same approach.Two other studies [9] and [10] demonstrate the successful recovery of encrypted files after a ransomware attack in server environments. Based on the conducted research and the previous ones, we can conclude that using the proposed method allows us to successfully recover deleted original versions of files that have been replaced by their encrypted copies, regardless of the operating system and the ransomware used.

6. CONCLUSION.

Ransomware attacks are a form of malicious software that encrypts data on user systems and demands payment for decryption. This type of attack is among the most dangerous for modern IT infrastructures and is a subject of serious security concern in the digital world. This study examines key aspects of the data recovery process in the context of a private cloud infrastructure, utilizing the capabilities of ownCloud Infinite Scale. In the study, user data is stored in a private cloud environment and synchronized with a controlled workstation running a Windows-based operating system, which is subsequently infected with the Thanos ransomware. It has been demonstrated that the proposed approach can be employed for the successful recovery of data following a ransomware attack. Based on this and previous research by the same authors, it can be concluded that the method is effective in a more general case where there is no dependency on the specific ransomware used and the infected system.

7. ACKNOWLEDGMENT

This research is funded by the Bulgarian National Science Fund under Project KP-06-NP62/1.

REFERENCES

[1] Hamdani, S.W.A., Abbas, H., Janjua, A.R., Shahid, W.B., Amjad, M.F., Malik, J., Murtaza, M.H., Atiquzzaman, M., and Khan, A.W., 2021. Cybersecurity

standards in the context of the operating system: Practical aspects, analysis, and comparisons. *ACM Computing Surveys (CSUR)*, **54(3)**, 1-36.

[2] Saravanan, A. and Bama, S.S., 2019. A review on cyber security and the fifth generation cyberattacks. *Oriental journal of computer science and technology,* **12(2)**, 50-56.

[3] https://doc.owncloud.com/ocis/next/availability_scaling/availability_scaling.html, last visit November 2023.

[4] Ogiriki, I., Beck, C. and Heydari, V., 2022. *Technical Analysis of Thanos Ransomware.*

[5] Hristev, R., Veselinova, M., Kolev, K., Ransomware Target: Linux. Recover Linux Data Arrays after Ransomware Attack., *The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM)*, 2022, **19**, 78-86.

[6] Kok, S., Abdullah, A., Jhanjhi, N. and Supramaniam, M., 2019. Ransomware, threat and detection techniques: A review. *Int. J. Comput. Sci. Netw. Secur* **19(2)**, 136.

[7] Tailor, J.P. and Patel, A.D., 2017. A comprehensive survey: ransomware attacks prevention, monitoring and damage control. *Int. J. Res. Sci. Innov*, **4(15)**, 116-121.

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

[9] Golev, A., Hristev, R., Veselinova, M., Kolev, K., Crypto-ransomware attacks on Linux serveces: A data recovery method, *Intern. J. Diff. Eq. Appl.* **21**, (2022), 19-29.

[10] Hristev, R., Veselinova, M. and Kolev, K., RANSOMWARE ATTACKS ON WINDOWS SERVERS: INFECTION AND RECOVERY. *International Journal of Differential Equations and Applications*, **Volume 22, No. 1**, (2023), 57-66.