International Journal of Differential Equations and Applications
Volume **22**, No. 1 (2023), pages: 57-66
ISSN (Print): 1311-2872; ISSN (Online): 1314-6084;
url: https://www.ijdea.eu

RANSOMWARE ATTACKS ON WINDOWS SERVERS: INFECTION AND RECOVERY

Rosen Hristev[1], Magdalena Veselinova[2], Kristiyan Kolev[3]
[1,2,3]Department of Mathematics and Informatics
University of Plovdiv Paisii Hilendarskiy
236, Bulgaria Blvd., 4000 Plovdiv, BULGARIA

ABSTRACT: Cyberattacks are a part of our reality and lately more and more organizations think about what could be happened if they are attacked by a cryptovirus. At the same time the ransomware attacks are constantly evolving and cybercriminals are looking for ways to expand the scope of their attacks and increase their profit. The ransomware-as-a-service (RaaS) model has become popular because it allows cybercriminals to attack more victims with less effort. Sodinokibi is a perfect example of RaaS and it is the 4th most widespread ransomware in the world, targeting mostly American and European companies. This is the reason why Windows Server environments are affected victims by this type of attacks. This paper summarizes trends that characterize the ransomware landscape in 2022. It is described the infection of a virtual machine running Windows Server 2019 with Sodinokibi. The virtual machine has an installed .NET Framework web application that uses a Microsoft SQL Server database. The application's database and executable files are synchronized with an external cloud server. After infection an approach for successful recovering the application's executable files and database is proposed.

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

Received: May 10, 2023 **Revised:** June 11, 2023
Published: June 13, 2023 **doi:** 10.12732/ijdea.v22i1.5
Academic Publications, Ltd. https://acadpubl.eu

1. INTRODUCTION

Cybercriminals continue to threaten and extort both ordinary users and organizations worldwide. Old variants of malware return while new ones develop. In response to the progressive countermeasures against cryptovirus attacks, the severity and evasive characteristics of attack strategies have evolved [1].

Ransomware attack tactics continue to develop is one of the biggest topics in 2022. Attacks against tech companies and virtual machines wiped files instead of encrypting data. Another situation we notice in 2022 is that no industry is immune to ransomware attacks. The SpyCloud Ransomware 2022 Report [2] reports that 50% of organizations were hit by ransomware two to five times in the past year, compared to 34% the year before. In addition, only 10% had not had an attack in the past year, compared to 28% in the previous year. There have been notable attacks during the past year against governments, government agencies, the auto industry, hospitals, etc. Despite of the increasing frequency of ransomware attacks against this type of organization, the attacks do not discriminate and anyone can become a victim.

Over the years, cybercriminals have been breaking into more and more complex environments where a wide variety of systems are running. In order to cause as much damage as possible and make recovery very difficult or impossible, they try to encrypt as many systems as possible. This means that the ransomware should be able to run on different combinations of architectures and operating systems. One way to overcome this is to write the ransomware in a cross-platform programming language. There are more reasons for using a cross-platform language. For example, although ransomware may target a single platform at the moment, rewriting it in a cross-platform language makes it easier to port to other operating systems. Thanks to this software flexibility, attacks can be carried out on a larger scale. This flexibility allows ransomware attacks to quickly adapt their strategy, diversify their targets and affect more victims.

Cybersecurity professionals and researchers work to detect, prevent, and mitigate such attacks and their potential impact. Many studies have been published investigating ransomware and providing solutions to tackle this difficult task [3, 4]. In [5, 6] an approach for successful recovery of encrypted files on Linux-based machines after infection with various types of crypto viruses is proven. Our previous study proposed an approach to successfully recovering user files stored in a private cloud after an infection of a Windows-based user workstation [7]. In recent years, the focus of cybercriminals has not only been on user files. More and more RaaS are trying to reach databases or applications that are abundant in a modern IT infrastructure.

2. RANSOMWARE EVOLUTION

Ransomware emerged in the late 1980s when a medical researcher attempted to extort other researchers through malware delivered on floppy disks. Even then, it was predicted that this type of malware would become a potential threat that uses cryptography [8, 9, 10]. The subsequent evolution of ransomware has been slow. Deployment did not occur in the usual way until the mid-2000s, when cybercriminals extorted their victims into paying by denying them access to their own services and systems.

Attacks in the mid-2010s relied on indiscriminate distribution among large numbers of victims. An automated approach uses phishing campaigns and vulnerability scanning to deploy ransomware on one or a small number of hosts. While this approach targets many victims, the attacks often fail. The spread of ransomware is uncontrolled and does not cause sufficient disruption to compromised networks. As a result, victims rarely comply with extortion requests. The ransom demands were relatively low by today's standards.

Next stage in the development of ransomware is when cybercriminals begin deploying post-intrusion ransomware. The defining characteristic of post-intrusion ransomware is hands-on-keyboard activity, which threat actors use to maximize the malware's destructive capabilities. This change gives much more control over ransomware deployment, enables targeted and successful encryption of files across the network, and justifies higher ransom demands.

The next big development is the RaaS model. Ransomware actors are starting to engage affiliates to deploy malware in exchange for a share of the ransom payment. This model allowed scaling attacks. Even threat participants with low technical skills have successfully stolen money and destroyed large parts of victims' networks by using RaaS in post-intrusion ransomware incidents.

Ransom demands are increasing dramatically. In 2020, the average ransom demanded from a victim was $4.8 million. In late March 2021, an US insurance provider paid $40 million to regain access to its network after a ransomware variant was deployed.

3. SODINOKIBI OVERVIEW

Sodinokibi is the name of a ransomware family that targets Windows systems. Sodinokibi encrypts important files and demands a ransom to decrypt them. The ransomware encrypts all files on local drives except those listed in their configuration file. Target files have extensions .jpg, .jpeg, .raw, .tif, .eps, .bmp, .3dm, .max, .accdb, .db, .mdb,

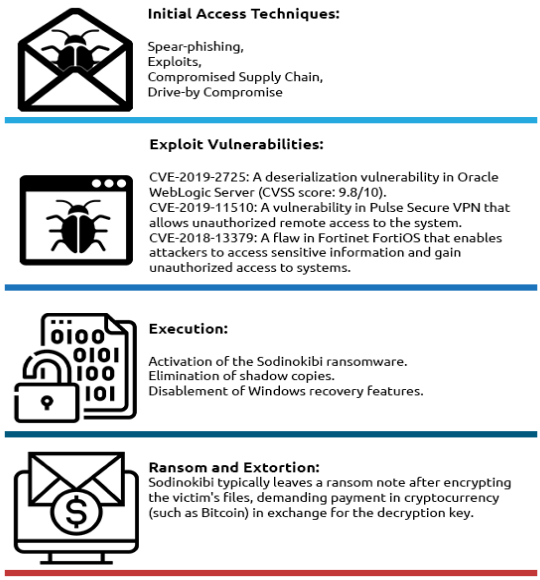


Figure 1: Sodinokibi Spread

.dwg, .dxf, .cpp, .cs, .h,php, .asp, .rb, .java, .aaf, .aep, .aepx, .plb, .prel, .aet, .ppj, .gif and .psd and more.

Without backups, a roll-back system, or other ways to recover the encrypted files, the affected systems are usable, but all important information stored on them is inaccessible. The information cannot be recovered by deep hard disk scanning software either, as the encrypted data is written to the original sources. This makes it practically impossible to recover information from disks that are mounted on the compromised machine.

Most of the time Sodinokibi ransomware spreads through brute force attacks and server exploits. This does not exclude the possibility of infection using phishing emails. Exploiting the Oracle WebLogic vulnerability Sodinokibi downloads a .zip file with the ransom code. The ransom code is written in JavaScript, moves through the infected network, and encrypts files by appending a random extension to them. Particularly dangerous is the fact that Sodinokibi will reinstall itself as long as the original ransom code is not deleted. Figure 1. shows the most common access techniques, as well as used vulnerabilities, the behavior and capabilities of the virus.

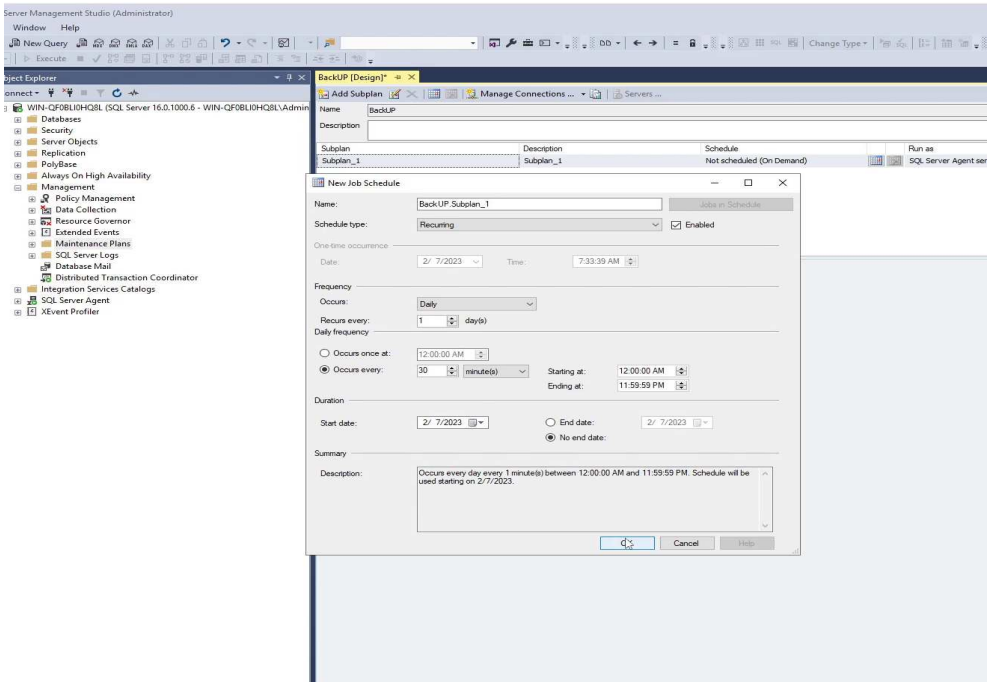


Figure 2: SQL Server Management Studio Backup Set Up

4. INFECTION

After break in the system, Sodinokibi makes a list of all files with the above-described extensions that can be affected by the ransomware and starts encrypting them. Only after the virus has finished its work does the user realize that he has become a victim of a crypto virus. For the purpose of this research, an application running on .Net Core and using Microsoft SQL Server 2022 was run in a controlled environment running on Microsoft Windows Server 2019. A daily backup of the database is set up through Microsoft SQL Server Management Studio as shown in Figure 2.

The database archives are stored on the C:\ drive of the operating system, in a folder that is named DB-Archive, and the working directory of the web-based application is C:\inetpub\hr. For the purposes of this research, database backups and application executable files are synchronized with a cloud server that has NextCloud version 21 installed. Windows Server 2019 has NextCloud Client installed on it and is configured to synchronize database backups located in C:\DB-Archive and the web application located in C:\inetpub\hr, this way when we have a change in the application executable files, they will be synced to the NextCloud server, as shown in Figure 3.

Once in the system, Sodinokibi will encrypt all files with the described extensions

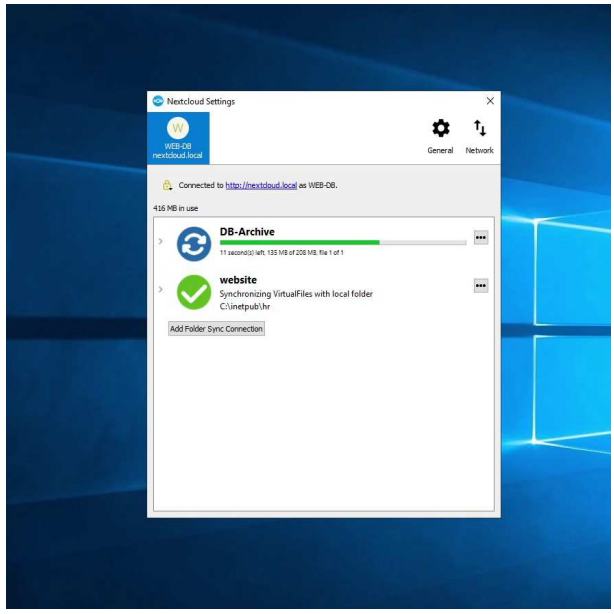


Figure 3: NextCloud Synchronization Set Up

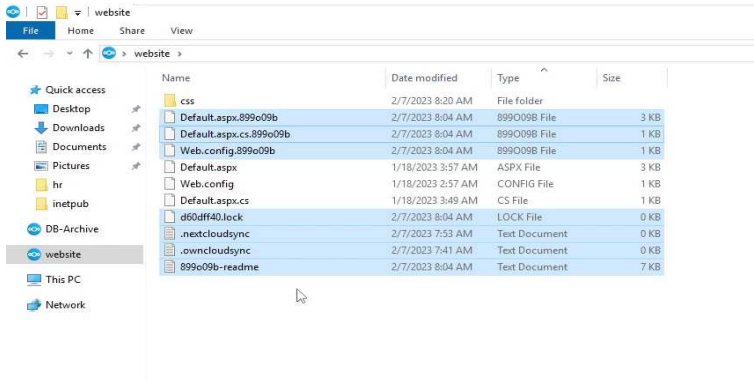


Figure 4: Encrypted Files

(Figure 4) and making the application practically inaccessible (Figure 5).

Most known ransomware self-destructs once the encryption of the target files is done. This reduces the chance of their code being reverse engineered, as well as making it easier and faster to create a tool to decrypt the files back.

In order to restore the normal operation of the server, a method was described in previous research of the team [6]. After the server was cleaned and scanned for viruses the files were restored from deleted files in the private cloud Deleted Files (Figure 6):

After the restoration of the files to the already cleaned server, the database backup was restored too (Figure 7).

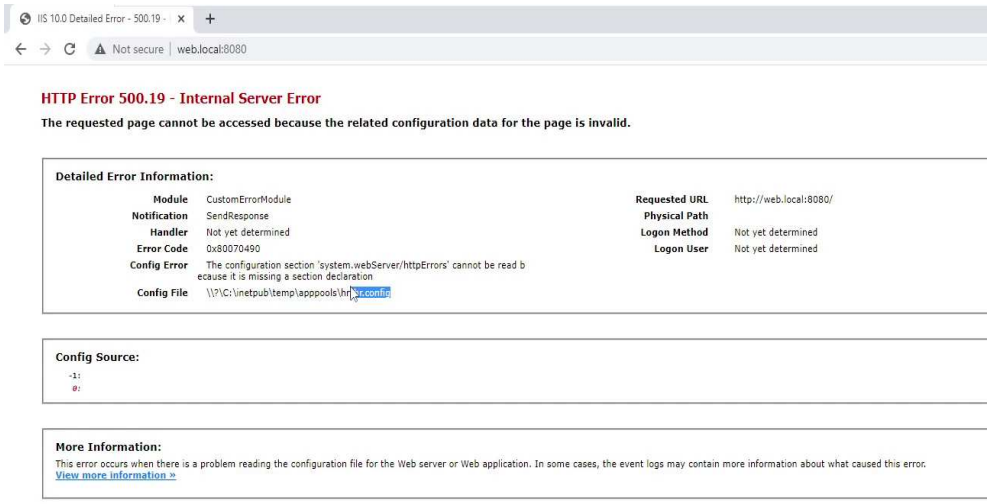


Figure 5: Server Error after Encryption

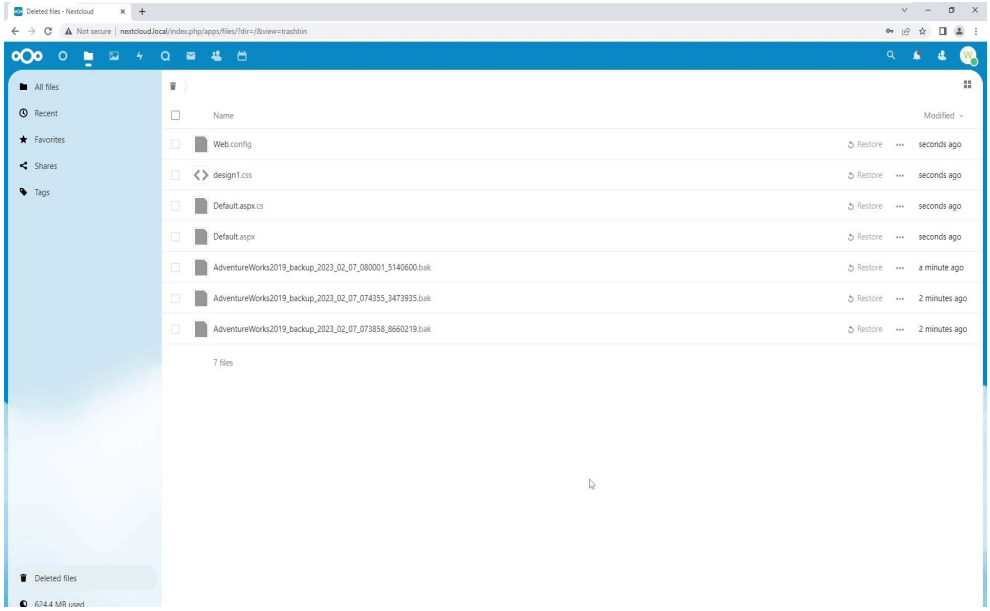


Figure 6: Restored Files

The web server is then returned to production mode on the computer network so that it can continue to serve clients (Figure 8).

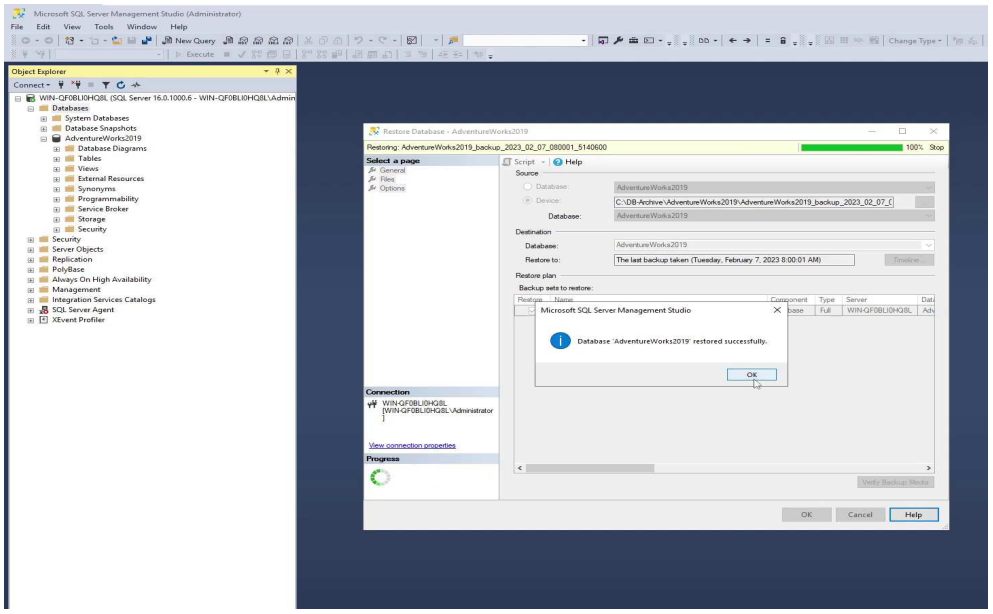
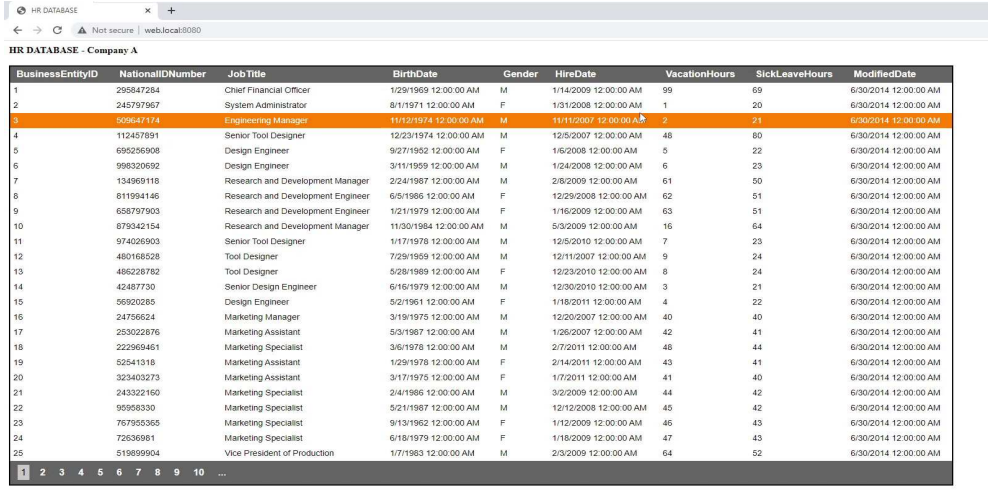


Figure 7: Database Restoration



BusinessEntityID	NationalIDNumber	JobTitle	BirthDate	Gender	HireDate	VacationHours	SickLeaveHours	ModifiedDate
1	295847284	Chief Financial Officer	1/29/1969 12:00:00 AM	M	1/14/2009 12:00:00 AM	99	69	6/30/2014 12:00:00 AM
2	245797967	System Administrator	8/1/1971 12:00:00 AM	F	1/31/2008 12:00:00 AM	1	20	6/30/2014 12:00:00 AM
3	509647174	Engineering Manager	11/12/1974 12:00:00 AM	M	11/11/2007 12:00:00 AM	2	21	6/30/2014 12:00:00 AM
4	112457891	Senior Tool Designer	12/23/1974 12:00:00 AM	M	12/5/2007 12:00:00 AM	48	80	6/30/2014 12:00:00 AM
5	695256908	Design Engineer	9/27/1952 12:00:00 AM	F	1/6/2008 12:00:00 AM	5	22	6/30/2014 12:00:00 AM
6	998320692	Design Engineer	3/11/1959 12:00:00 AM	M	1/24/2008 12:00:00 AM	6	23	6/30/2014 12:00:00 AM
7	134969118	Research and Development Manager	2/24/1987 12:00:00 AM	M	2/8/2009 12:00:00 AM	61	50	6/30/2014 12:00:00 AM
8	811994146	Research and Development Engineer	6/5/1986 12:00:00 AM	F	12/29/2008 12:00:00 AM	62	51	6/30/2014 12:00:00 AM
9	658797903	Research and Development Engineer	1/21/1979 12:00:00 AM	F	1/16/2009 12:00:00 AM	63	51	6/30/2014 12:00:00 AM
10	879342154	Research and Development Manager	11/30/1984 12:00:00 AM	M	5/3/2009 12:00:00 AM	16	64	6/30/2014 12:00:00 AM
11	974026903	Senior Tool Designer	1/17/1978 12:00:00 AM	M	12/5/2010 12:00:00 AM	7	23	6/30/2014 12:00:00 AM
12	480168528	Tool Designer	7/29/1959 12:00:00 AM	M	12/11/2007 12:00:00 AM	9	24	6/30/2014 12:00:00 AM
13	486228782	Tool Designer	5/28/1989 12:00:00 AM	F	12/23/2010 12:00:00 AM	8	24	6/30/2014 12:00:00 AM
14	42487730	Senior Design Engineer	6/16/1979 12:00:00 AM	M	12/30/2010 12:00:00 AM	3	21	6/30/2014 12:00:00 AM
15	56920285	Design Engineer	5/2/1961 12:00:00 AM	F	1/18/2011 12:00:00 AM	4	22	6/30/2014 12:00:00 AM
16	24756624	Marketing Manager	3/19/1975 12:00:00 AM	M	12/20/2007 12:00:00 AM	40	40	6/30/2014 12:00:00 AM
17	253022876	Marketing Assistant	5/3/1987 12:00:00 AM	M	1/26/2007 12:00:00 AM	42	41	6/30/2014 12:00:00 AM
18	222969461	Marketing Specialist	3/6/1978 12:00:00 AM	M	2/7/2011 12:00:00 AM	48	44	6/30/2014 12:00:00 AM
19	52541318	Marketing Assistant	1/29/1978 12:00:00 AM	F	2/14/2011 12:00:00 AM	43	41	6/30/2014 12:00:00 AM
20	323403273	Marketing Assistant	3/17/1975 12:00:00 AM	F	1/7/2011 12:00:00 AM	41	40	6/30/2014 12:00:00 AM
21	243322160	Marketing Specialist	2/4/1986 12:00:00 AM	M	3/2/2009 12:00:00 AM	44	42	6/30/2014 12:00:00 AM
22	95958330	Marketing Specialist	5/21/1987 12:00:00 AM	M	12/12/2008 12:00:00 AM	45	42	6/30/2014 12:00:00 AM
23	767955365	Marketing Specialist	9/13/1962 12:00:00 AM	F	1/12/2009 12:00:00 AM	46	43	6/30/2014 12:00:00 AM
24	72636981	Marketing Specialist	6/18/1979 12:00:00 AM	F	1/18/2009 12:00:00 AM	47	43	6/30/2014 12:00:00 AM
25	519899904	Vice President of Production	1/7/1983 12:00:00 AM	M	2/3/2009 12:00:00 AM	64	52	6/30/2014 12:00:00 AM

1 2 3 4 5 6 7 8 9 10 ...

Figure 8: Restored Web Server in Production Mode

5. CONCLUSION

Note that 2022 was one of the most remarkable years for ransomware attacks. Damage that has been caused by crypto viruses continues to grow and the security experts

predict that the number of attacks will continue to increase in time. In the future, we could expect the increase of the amounts of ransoms which are paid by infected organizations, given that in the past year we have reported an increase of almost a 100%. Infecting user workstations is no longer a top priority for cybercriminals. The main targets are enterprise networks because malware is highly resistant and multi-platform. Modes of spread also continue to evolve making it possible to infect a larger number of victims. One of the most common methods of infection is through the use of phishing emails. Domains with unproper configured DNS settings are often used for this purpose and this allows the sender of the malicious message to pretend to be part of the network they are trying to break into. This tactic succeeds in imposing itself on many users and it has a high success rate. The paper considers the current ransomware situation and the main stages in the evolution of ransomware and attack techniques. For the current study we have been used virtual machines which provide complete isolation and control over the environment. The recipient virtual machine is running Windows Server 2019 and includes a sample web application that uses Microsoft SQL Server 2022 and an IIS web service to present the data on the web from the sample imported database - AdventureWorks2019. The virtual machine is infected with ransomware from the Ransom.Sodinokibi family. After infection an approach for successful recovering the application's executable files and database is proposed.

6. ACKNOWLEDGMENT

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

REFERENCES

[1] Al-rimy, B.A.S.; Maarof, M.A.; Shaid, S.Z.M. Crypto-ransomware early detection model using novel incremental bagging with enhanced semi-random subspace selection. *Future Gener. Comput. Syst.* 2019, **101**, 476-491.

[2] 2022 in Review: The Year of Ransomware, https://spycloud.com/blog/2022-in-review-the-year-of-ransomware/. Visited on 11.05.2023

[3] U. Urooj, M. A. B. Maarof and B. A. S. Al-rimy, A proposed Adaptive Pre-Encryption Crypto-Ransomware Early Detection Model, *2021 3rd International Cyber Resilience Conference (CRC)*, Langkawi Island, Malaysia, 2021, 1-6, doi: 10.1109/CRC50527.2021.9392548.

[4] M. N. Olaimat, M. Aizaini Maarof and B. A. S. Al-rimy, Ransomware Anti-Analysis and Evasion Techniques: A Survey and Research Directions, *2021 3rd International Cyber Resilience Conference (CRC)*, Langkawi Island, Malaysia, 2021, 1-6, doi: 10.1109/CRC50527.2021.9392529.

[5] 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.

[6] 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.

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

[8] Al-rimy, B.A.S., Maarof, M.A., Shaid, S.Z.M. (2018). A 0-Day Aware Crypto-Ransomware Early Behavioral Detection Framework. In: Saeed, F., Gazem, N., Patnaik, S., Saed Balaid, A., Mohammed, F. (eds) *Recent Trends in Information and Communication Technology.* IRICT 2017. Lecture Notes on Data Engineering and Communications Technologies, vol. 5. Springer, Cham. https://doi.org/10.1007/978-3-319-59427-978

[9] Al-rimy, B.A.S., Maarof, M.A., Prasetyo, Y.A., Shaid, S.Z.M., Ariffin, A.F.M. Zero-day aware decision fusion-based model for crypto-ransomware early detection. *Int. J. Integr. Eng.*, **10** 6 (2018), 82-88.

[10] F. A. Aboaoja, A. Zainal, F. A. Ghaleb and B. A. Saleh Al-rimy, Toward an Ensemble Behavioral-based Early Evasive Malware Detection Framework, *2021 International Conference on Data Science and Its Applications (ICoDSA)*, Bandung, Indonesia, 2021,181-186, doi: 10.1109/ICoDSA53588.2021.9617489.