Avrupa Bilim ve Teknoloji Dergisi
Özel Sayı, S. 486-493, Nisan 2020
© Telif hakkı EJOSAT'a aittir
Araştırma Makalesi

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
Special Issue, pp. 486-493, April 2020
Copyright © 2020 EJOSAT
Research Article

Characteristic Behavioral Analysis of Malware: A Case study of Cryptowall Ransomware[*]

İlker Kara[1**], Murat Aydos[2], Ahmet Selman Bozkır[3]

[1] Dept. of Medical Services and Techniques, Eldivan Medical Services Vocational School Çankırı, Karetekin University, Turkey (ORCID: 0000-0003-3700-4825)
[2] Hacettepe University, Department of Computer Engineering, Ankara, Turkey (ORCID: 0000-0002-7570-9204)
[3] Hacettepe University, Department of Computer Engineering, Ankara, Turkey (ORCID: 0000-0003-4305-7800

(Conference Date: 5-7 March 2020)

(**DOI:** 10.31590/ejosat.araconf63)

ATIF/REFERENCE: Kara, İ., Aydos, M. & Bozkır, A. S. (2020). Characteristic Behavioral Analysis of Malware: A Case study of Cryptowall Ransomware. *Avrupa Bilim ve Teknoloji Dergisi*, (Özel Sayı), 486-493.

Abstract

CryptoWalls ranks first among the Ransomware in terms of its design, objectives, and damages. Cybercriminals use CryptoWalls in a wide range of applications, from cross-country cyberterrorism to demanding ransom from an ordinary Internet user. Despite all the measures taken, an effective protection against CryptoWalls has still not been developed. This motivates cyber criminals, and new versions of updated CryptoWalls are released every day, becoming a more difficult problem to be solved. Current research studies discuss the general characteristics and consequences of CryptoWalls. How do CryptoWalls work? How the CryptoWall detection and technical analysis are done? Detailed studies on the answers to these questions will contribute to solving this problem. This study discusses detailed analysis of CryptoWall detection on a real victim's computer, targeted by the CryptoWall attack of cybercriminals. The study is of importance since it addresses how the CryptoWall attack infiltrates the target system, shows the analysis steps of its characteristic actions, and identifies the originating company of the CryptoWall malware.

Keywords: Cybercriminal, Malware Analysis, CryptoWalls.

Zararlı Yazılımların Karekterislik Analizi: Cryptowall Fidye Yazılım Analizi

Öz

CryptoWall'lar tasarımı, amaçları ve verdiği zararlar açısından Ransomware'lar içerisinde ilk sıralarda yer almaktadır. Siber suçlular ülkeler arası siber terörizmden sıradan bir internet kullanıcından fidye istemeye kadar geniş bir uygulama alanında CryptoWall'ları kullanmaktadır. Alınan tüm tedbirlere rağmen CryptoWall'ları ile etkin bir mücadele hala geliştirilememiştir. Bu durum siber suçluların iştahını kabartmakta ve her geçen gün yeni sürümler ile CryptoWall'lar güncellenerek piyasaya sürülmekte, çözülmesi daha zor bir problem haline gelmektedir. Mevcut araştırma çalışmaları CryptoWall'ların genel özellikleri ve sonuçlarını tarışmaktadır. CryptoWall'lar nasıl çalışır? CryptoWall tespiti ve teknik analizi nasıl yapılır? Bu soruların cevapları hakkında detaylı çalışmalar yapılması bu problemin çözümesine katkı sağlayacaktır. Bu çalışma, siber suçluların CryptoWall saldırısıyla hedef aldığı gerçek bir kurbanın bilgisayarında CryptoWall'un tespiti ve analizi detaylı incelemesi üzerinedir. Çalışma, CryptoWall saldırısının hedef sisteme nasıl sızdığını, karekteristik hareketlerinin analiz aşamalarının göstermesi ve CryptoWall zararlı yazılımının üretici firmasının tespit edilmesini içermesinden dolayı önemlidir.

Anahtar Kelimeler: Siber Suçlar, Zararlı Yazılım Analizi, CryptoWalls.

[*] This paper was presented at the ***International Conference on Access to Recent Advances in Engineering and Digitalization (ARACONF 2020)***.

[**] Corresponding Author: Dept. of Medical Services and Techniques, Eldivan Medical Services Vocational School Çankırı, Karetekin University, Turkey, ORCID: 0000-0003-3700-4825, karaikab@gmail.com

1. Introduction

Recently, all the world witness the increasing number of victims, who have been exposed to cyberattacks while opening fake emails or visiting unsafe websites [1-6]. This threat is widespread from commercial enterprises to individual Internet users. This type of malware is known as Ransomware. Today, new types of Ransomware are quite advanced compared to their initial versions [7,8]. A Ransomware that infiltrates the target system can cause severe damage and even make the system unusable [9-11]. Ransomware is a malware that prevents access to the files on the infected information systems by encrypting them and requesting ransom from the victims to decrypt the encryption [9,12-13].

Ransomware has been a severe cyber threat for about twenty-five years [14,15]. Ransomware was first seen in 1989 under the name of AIDS Trojan horse [16]. The first modern Ransomware "Trojan.Gpcoder" has been seen in Russia in 2005 [17]. The Trojan.Gpcoder, which was first seen in May 2015, has been easily overcome since it had a simple and easy encryption. In time, improved versions of Ransomware were found to use the user's native language, and even some versions were found to contain voicemails in the user's native language [18]. In 2008, a Trojan.Gpcoder Ransomware called GPcode.AK emerged. It has been found that GPcode.AK uses a 1024-bit RSA key and leaves a text file containing instructions in each subdirectory of encrypted files. GPcode.AK has requested a $100 payment to decrypt the encrypted files of the victims [17].

Today, cybercriminals have modified Ransomware for different purposes. In addition to a ransom request, they have succeeded in developing Ransomware for the purpose of cyberterrorism and intimidating the political and official authorities through illegal harmful attacks to the computers and databases of official units [9,18]. Cybercriminals can send one or several files of the user back to convince them that they have the files and will give the password [19]. Thus, the victim sees this as a "proof of living cybercriminals" and accepts the payment by believing that the cybercriminals will recover their encrypted files when they send the money requested. "!!! All your files were encrypted by CryptoWall !!!" is a Ransomware that makes all photos, videos, personal information and commercial files on user's computer, network drive, USB drive and Network Attach Storage (NAS) devices encrypted [20].

CryptoWall encrypts the first 1 MB portion of files, as in the case of typical Ransomware. CryptoWall uses AES (Advanced Encryption Standard) encryption standard. This encryption uses a 256-bit standard AES algorithm used to encrypt electronic data [21]. AES encryption is used as the de facto encryption standard in the international arena by the American government. Recently there has been a serious increase in Ransomware attacks. In Europe, especially the CryptoWall Ransomware attacks are seen [22]. CryptoWall, a highly dangerous Ransomware type, increases the likelihood of paying a ransom, making it easier for cybercriminals to get "money", which is what they really want [19,23].

1.1. How Do Cryptowalls Spread?

CryptoWalls are rapidly spreading all over the world by attacking all Internet users. The most commonly used infiltration medium for spreading CryptoWalls is e-mailing with phishing tactics containing harmful attachments. The message may be localized according to the victims i.e., it may be customized according to the country where the victim is located. For instance, e-mail content for the targeted victims in Turkey seems like overpriced invoices coming from Turkish telecommunication companies.

The location of the potential victim can be identified using the country domain of the victim's e-mail address or the service provider hosting the domain. If the victim, tricked via social engineering, opens the e-mail attachment, which has not been detected by the antivirus program of the system, all important files in the system are encrypted. When the encryption process is over, a warning is shown to the victim, indicating that he/she must send money to recover his/her files.

1.2. Cryptowall Prevention And Protection

Files encrypted by CryptolWall are regarded as damaged beyond repair. Recommended measures to be taken against potential CryptolWall attacks are as follows:

i. The only and best solution to make CryptoWall malware ineffective is having regular backups.

ii. CryptolWall Ransomware often comes with a file with .pdf or .exe extension. This incident is based on the fact that the Windows operating system hides known file extensions by default. Enabling the view of full file extensions on the system will make it easier to detect suspicious files.

iii. If your e-mail program is capable of filtering by file extension, filter out the emails with attachments with .exe, .scr, .pif, .js file extension and the files with two file extensions, ending with .exe (executable files).

iv. Users should be informed about not to open suspicious e-mail attachments coming from addresses that they do not know, not to click on suspicious links, and their awareness should be increased in this regard.

v. Ransomware can silently infiltrate systems that use out-of-date software.

vi. A remarkable feature of CryptoWalls is that they run the executable in the AppData or Local AppData folder. These folders can be blocked in Windows operating system or using intrusion protection systems.

vii. CryptoWalls often target the systems that use Remote Desktop Protocol (RDP) to remotely connect to systems with a Windows operating system. Cybercriminals are known to log on to the target system with RDP and disable security software. Therefore, disabling remote access would be an effective method.

1.3. What Can Be Done After A Cryptowall Attack?

If the targeted system has a Windows operating system and System Restore is enabled, encrypted files can be recovered from "Shadow" files using the "Windows Shadow Volume Copies". However, CryptoWalls can quickly consider these possibilities and produce solutions. The new generation of CryptoWall can also delete these shadow file copies and prevent files from being recovered. CryptolWalls start the process of deleting the shadow files by running as a standard Windows Operating System process on boot, and completes the process of deleting files without being noticed by users or system administrators.

Antivirus and Antimalware programs can remove the malware in a system that has been exposed to a CryptoWall attack. However, the main problem here is to provide access to encrypted files. Even if the CryptoWall is removed by Antivirus and Antimalware programs, the files remain encrypted. Therefore, in a system that has been exposed to the CryptoWall attack, recovering the files should be the priority, not removing the CryptoWall Ransomware.

In order to develop an effective solution against CryptoWalls, one should begin with a detailed description of the threat. When we look at the related studies, we see that general features and consequences of CryptoWalls are discussed in general, but there is no empirical study about the methods used in the hacking victim's computer and the encryption process.

In this study, detection of the new generation CryptoWall Ransomware, its intrusion and cryptographic behavior were examined in detail by static and dynamic analysis methods. As a result of the investigations, the company that spreads the CryptoWall Ransomware has been identified, which has caused many Internet users to suffer.

2. Materials and Methods

As is known, there is no standard method for malware analyses. However, we first performed static analysis without running the malware. Secondly, we have performed a dynamic analysis in which its actions (file-directory movements) were examined by running the malware in a controlled environment. Finally, the code analysis, we have performed and architectural analysis of the malware.

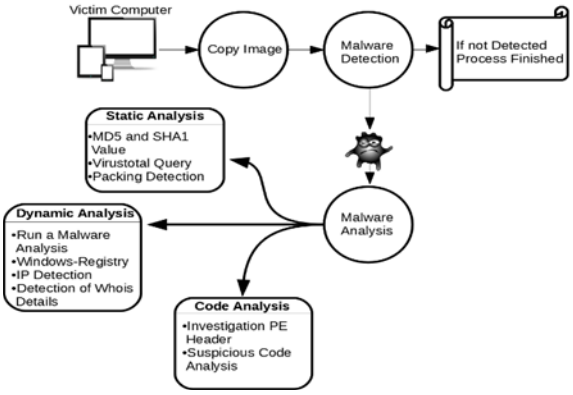


Figure 1. Malware analysis algorithm [24].

2.1.1. Experıments And Results

In order to analyze the victim computer infiltrated with CryptoWall Ransomware, which is the subject of this study, the disk of the victim computer was copied in accordance with international standards by enabling write protection on the original disk for ensuring the data integrity. The copies of the files were analyzed on a virtual machine (virtual PC) installed on a workstation. Since the CryptoWall Ransomware would quickly attack against user data upon running it, we run it in a workstation that has been set to virtual machine mode. Characteristic behavior analysis of CryptoWall ransomware was performed through the "AccessData Forensic Toolkit v6.2.1.10" software. We presented the information about the static analysis on the CryptoWall Ransomware in Table 1 and Table 2.

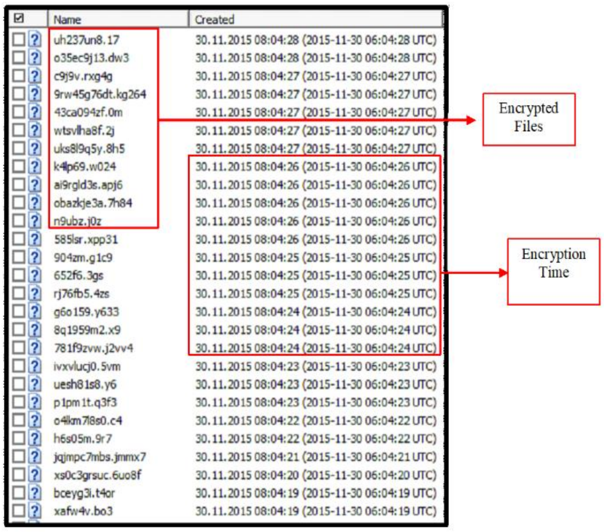
Table 1. Device Information

Process Name	**File Information.**
	Properties
Description	Physical Disk, 976.773.168 Sectors 465,8 GB
Total Size	500.107.862.016 Bytes (465,8 GB)
Total Sectors	976.773.168
Acquisition MD5	d81bbd39ff5a57888250f44ca17c1cc4
Verification MD5	*d81bbd39ff5a57888250f44ca17c1cc4*
Acquisition SHA1	*a5b0c73498543a063cd16051b47e5b526*
Verification SHA1	*a5b0c73498543a063cd16051b47e5b526*
Description	*Physical Disk, 976.773.168 Sectors 465,8GB*

Table 2. Windows OS Information

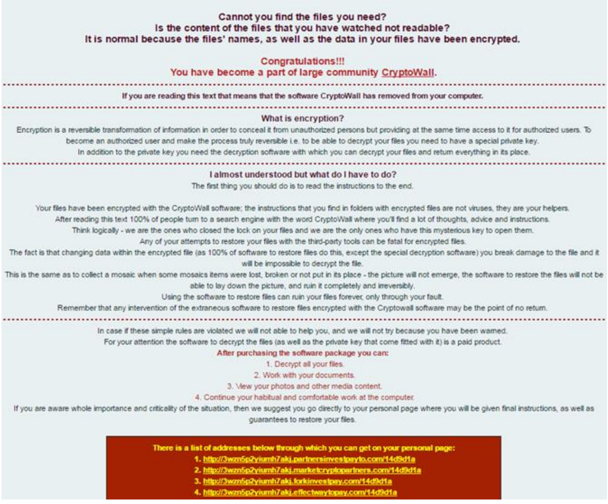
Process Name	File Information.
	Properties
Product Name	*Microsoft Windows XP*
Registered Owner	*BXX*
System Root	*C:\Windows\*
Product ID	*55896-640-3868325-XXXX*
Current Version	*5.1*
CSD Version	*Service Pack 3*
Install Date	*20.07.2012 08:04:09 UTC*
Last Shotdown Time	*30.11.2015 11:43:23 UTC*

As a result of the analysis conducted in line with the international standards on IT practices, first the files encrypted by CryptoWall Ransomware were detected, and all documents, IP logs, Operating System services and logs were analyzed. In the first examinations, CryptoWall Ransomware was found to be in the "HELP_YOUR_FILES.HTML" file located under the directory "IMAGE.001/Partition1/NONAME[NTFS]/[root]/Documents and Settings/Administrator/Desktop/".



☑	Name	Created
□	uh237un8.17	30.11.2015 08:04:28 (2015-11-30 06:04:28 UTC)
□	o35ec9j13.dw3	30.11.2015 08:04:28 (2015-11-30 06:04:28 UTC)
□	c9j9v.rxg4g	30.11.2015 08:04:27 (2015-11-30 06:04:27 UTC)
□	9rw45g76dt.kg264	30.11.2015 08:04:27 (2015-11-30 06:04:27 UTC)
□	43ca094zf.0m	30.11.2015 08:04:27 (2015-11-30 06:04:27 UTC)
□	wtsvlha8f.2j	30.11.2015 08:04:27 (2015-11-30 06:04:27 UTC)
□	uks8l9q5y.8h5	30.11.2015 08:04:27 (2015-11-30 06:04:27 UTC)
□	k4lp69.w024	30.11.2015 08:04:26 (2015-11-30 06:04:26 UTC)
□	ai9rgld3s.apj6	30.11.2015 08:04:26 (2015-11-30 06:04:26 UTC)
□	obazkje3a.7h84	30.11.2015 08:04:26 (2015-11-30 06:04:26 UTC)
□	n9ubz.j0z	30.11.2015 08:04:26 (2015-11-30 06:04:26 UTC)
□	585lsr.xpp31	30.11.2015 08:04:26 (2015-11-30 06:04:26 UTC)
□	904zm.g1c9	30.11.2015 08:04:25 (2015-11-30 06:04:25 UTC)
□	652f6.3gs	30.11.2015 08:04:25 (2015-11-30 06:04:25 UTC)
□	rj76fb5.4zs	30.11.2015 08:04:25 (2015-11-30 06:04:25 UTC)
□	g6o159.y633	30.11.2015 08:04:24 (2015-11-30 06:04:24 UTC)
□	8q1959m2.x9	30.11.2015 08:04:24 (2015-11-30 06:04:24 UTC)
□	781f9zvw.j2vv4	30.11.2015 08:04:24 (2015-11-30 06:04:24 UTC)
□	ivxvlucj0.5vm	30.11.2015 08:04:23 (2015-11-30 06:04:23 UTC)
□	uesh81s8.y6	30.11.2015 08:04:23 (2015-11-30 06:04:23 UTC)
□	p1pm1t.q3f3	30.11.2015 08:04:23 (2015-11-30 06:04:23 UTC)
□	o4lkm7l8s0.c4	30.11.2015 08:04:22 (2015-11-30 06:04:22 UTC)
□	h6s05m.9r7	30.11.2015 08:04:22 (2015-11-30 06:04:22 UTC)
□	jqjmpc7mbs.jmmx7	30.11.2015 08:04:21 (2015-11-30 06:04:21 UTC)
□	xs0c3grsuc.6uo8f	30.11.2015 08:04:20 (2015-11-30 06:04:20 UTC)
□	bceyg3i.t4or	30.11.2015 08:04:19 (2015-11-30 06:04:19 UTC)
□	xafw4v.bo3	30.11.2015 08:04:19 (2015-11-30 06:04:19 UTC)

Figure 2. Encrypted Files.



Cannot you find the files you need?
Is the content of the files that you have watched not readable?
It is normal because the files' names, as well as the data in your files have been encrypted.

Congratulations!!!
You have become a part of large community CryptoWall.

If you are reading this text that means that the software CryptoWall has removed from your computer.

What is encryption?
Encryption is a reversible transformation of information in order to conceal it from unauthorized persons but providing at the same time access to it for authorized users. To become an authorized user and make the process truly reversible i.e. to be able to decrypt your files you need to have a special private key.
In addition to the private key you need the decryption software with which you can decrypt your files and return everything in its place.

I almost understood but what do I have to do?
The first thing you should do is to read the instructions to the end.

Your files have been encrypted with the CryptoWall software; the instructions that you find in folders with encrypted files are not viruses, they are your helpers.
After reading this text 100% of people turn to a search engine with the word CryptoWall where you'll find a lot of thoughts, advice and instructions.
Think logically - we are the ones who closed the lock on your files and we are the only ones who have this mysterious key to open them.
Any of your attempts to restore your files with the third-party tools can be fatal for encrypted files.
The fact is that changing data within the encrypted file (as 100% of software to restore files do this, except the special decryption software) you break damage to the file and it will be impossible to decrypt the file.
This is the same as to collect a mosaic when some mosaics items were lost, broken or not put in its place - the picture will not emerge, the software to restore the files will not be able to lay down the picture, and ruin it completely and irreversibly.
Using the software to restore files can ruin your files forever, only through your fault.
Remember that any intervention of the extraneous software to restore files encrypted with the Cryptowall software may be the point of no return.

In case if these simple rules are violated we will not able to help you, and we will not try because you have been warned.
For your attention the software to decrypt the files (as well as the private key that come fitted with it) is a paid product.
After purchasing the software package you can:
1. Decrypt all your files.
2. Work with your documents.
3. View your photos and other media content.
4. Continue your habitual and comfortable work at the computer.
If you are aware whole importance and criticality of the situation, then we suggest you go directly to your personal page where you will be given final instructions, as well as guarantees to restore your files.

There is a list of addresses below through which you can get on your personal page:
1. http://3wzn5p2yiumh7akj.partnersinvestpayto.com/14d9d1a
2. http://3wzn5p2yiumh7akj.marketcryptopartners.com/14d9d1a
3. http://3wzn5p2yiumh7akj.forkinvestpay.com/14d9d1a
4. http://3wzn5p2yiumh7akj.effectwaytopay.com/14d9d1a

Figure 3. Message Showing That Cryptowall Ransomware Is Present When Executing The Copy.

According to the analysis performed on the copy, the creation date of the files encrypted with CryptoWall Ransomware were found to be 30/11/2015 - 08:04 UTC. The files that have been executed on this date were examined, and the CryptoWall Ransomware software was found to be located under the "IMAGE.001/Partition 1/NONAME [NTFS]/[root]/Documents and Settings/Administrator/Local Settings/Temp/" directory with the deleted filename of "88656522.exe".

Table 3. The Technical Information Of The Encrypted File In The Victim Computer Is Presented Below.

Process Name	File Information.
	Properties
File name	HELP_YOUR_FILES.HTML
Creating Time	30.11.2015 08:51:42 (2015-11-30 08:04)
Access Time	30.11.2015 14:42:22 (2015-11-30 08:04)
Replacement Time	30.11.2015 08:51:42 (2015-11-30 08:04)
File Size (Byte)	25.548 bytes (24,95 KB)
MD5 Hash Value	6af767f18f886bcdbf0785006f1e5074
File Path	IMAGE.001/Partition1/NONAME [NTFS]/[root]/Documentsand Settings/Administrator/Desktop/
File name	HELP_YOUR_FILES.HTML

Technical information of "88656522.exe" is as follows. The MD5 hash value of the malware was queried via the website "www.virustotal.com" and it was found out which antivirus companies identify the malware detected (Table 4).

Table 4. Static Analysis Results Of “88656522.Exe” Malware Via www.virustotal.com website.

Analysis	53 engines detected this file
	SHA-256 2797f44cdfa28c73d7a9b838f46ce3 File Name: 88656522.exe Last Analysis: 2017-12-7 13:01:45 UTC
AVG	❗ Zbok.AKKK
AVware	❗ Trojan.Win32ç.Generic!BT
Ad-Aware	❗ Trojan. GenericKD.2900815
Yandex	❗ Trojan. Filecoder!2dZC6TdKMg
AhnLab-V3	❗ Malware/Win32.Generic
Acrabit	❗ Trojan. Generic. D2C43F
Avast	❗ Win32:Malware-gen
Avira (no cloud)	❗ TR/FileCoder.629760.1
Baidu-International	❗ Trojan.Win32.Filecoder.FJ
BitDefender	❗ Trojan.GenericKD.2900815
CAT-QuickHeal	❗ Ransom.Crowti.M5
Cyren	❗ W32/Filecoder.XMQH-8836
DrWeb	❗ Trojan.DownLoader17.64698
ESET-NOD32	❗ Win32/Filecoder.FJ
Emsisoft	❗ Trojan.GenericKD.2900815 (B)
F-Prot	❗ W32/Filecoder.AE
F-Secure	❗ Trojan. GenericKD.2900815
Fortinet	❗ PossibleThreat.P0
Ikarus	❗ Trojan.Win32.Deshacop.big

The file-directory and registry logs of the malware named 88656522.exe were analyzed on the copy, and the findings were listed below (Table 5).

After identifying the file-directory and registry logs of the malicious software, which its detailed information is presented in Table 4, the network accesses of the related malware were analyzed by means of the software called "Wireshark" to find the attacker's IP addresses and domain names, as shown in Table 6.

Table 5. File-Directory And Registry Logs Of "85656522.Exe" Malware.

Analysis	**Process**
	Thread Events
Creates process:	*C:\WINDOWS\Temp\88656522.exe [“C:\windows\temp\88656522exe”]*
Creates process:	*C:\WINDOWS\exploer.exe [“C:\windows.exe”]*
Creates process:	*C:\WINDOWS\system32\svchost.exe[-k netsvcs]*
Creates process:	*C:\WINDOWS\system32\vssadmin.exe [vssadmin.exe Delete Shadows /All*
Write process:	*PID:1404 C:\WINDOWS\explorer.exe*
Write process:	*PID:1404 C:\WINDOWS\system32\svchost.exe*
Terminal process:	*C:\WINDOWS\Temp\88656522.exe*
Terminal process:	*C:\WINDOWS\system32\vssadmin.exe*
Creates remote thread:	*C:\WINDOWS\exploer.exe*
Creates remote thread:	*C:\WINDOWS\system32\svchost.exe*
Creates process:	*C:\WINDOWS\Temp\88656522.exe [“C:\windows\temp\88656522exe”]*
Creates process:	*C:\WINDOWS\exploer.exe [“C:\windows.exe”]*
Creates process:	*C:\WINDOWS\system32\svchost.exe[-k netsvcs]*
Creates process:	*C:\WINDOWS\system32\vssadmin.exe [vssadmin.exe Delete Shadows /All*
Write process:	*PID:1404 C:\WINDOWS\explorer.exe*
Write process:	*PID:1404 C:\WINDOWS\system32\svchost.exe*
Terminal process:	*C:\WINDOWS\Temp\88656522.exe*
Terminal process:	*C:\WINDOWS\system32\vssadmin.exe*
Creates remote thread:	*C:\WINDOWS\exploer.exe*
Creates remote thread:	*C:\WINDOWS\system32\svchost.exe*

Since the sample examined was selected from a real cyberattack, the information was blurred (hidden) for privacy purposes. After recording and analyzing the network accesses of the respective malicious software shown in Table 7, it was determined that the malware tries to contact the domain names "astrxxxxx.ca, becktonescoxxxxx.eu, bloggerrexxxxx.info and chaletlesarmaxxxxx.com", without IP addresses associated with the domain names.

In order to find out companies that registered the identified domain names, WHOIS queries were performed via the website "http://internet.tib.gov.tr/" and the findings obtained are given below. According to data obtained from WHOIS queries of the identified domain names, the domain names "astrxxxxx.ca and ecktonescoxxxxx.eu" were found to be registered at "www.godxxx.com" website and "bloggerrexxxxx.info" was found to be registered at the "www.publicdomainregistry.com" website, and the "chaletlesarmaxxxxx.com" was found to be registered at the "www.exxx.com" website. The suspects can be found through international legal assistance with the representatives of the websites identified.

Table 6. IP Logs Of "85656522.Exe" Malware.

Soure	**Process**	**Process**
	Destination	**Info**
10.7X.X.100	*8.8.8.8*	*Standard query 0xcc09 A xnoedge. ca*
10.7X.X.100	*8.8.8.8*	*Standard query 0xcc09 A xnoedge. ca*
10.7X.X.100	*10.74.9.255*	*Name query NB XNNTROEDGE.*
10.7X.X.100	*10.74.9.255*	*Name query NB XNNROEDGE.*
10.7X.X.100	*8.8.8.8*	*Standard query 0xeb4c A bxxktyyescorts4u.eu*

The contact information of the websites identified were searched, but the respective websites were found to hide the contact information, and only the website of www.publicdomainregistry.com was found to have a contact form for communication.

3. Conclusion

The volume, variety and speed of cyberattacks are increasing. Attacks of cybercriminals began to affect people and institutions much more deeply in the world increasingly digitalized with new technologies and devices. In these attacks, cybercriminals seem to focus on money theft mostly. Ransomware developed for this purpose forces the victims to pay a ransom by using online payment methods to allow access to their files or to retrieve their data after encrypting their files. The Ransomware coded for this purpose has been constantly updated, and became a problem impossible to solve. It is important for Internet users to know the functions of the Ransomware and the great threat they create and the best practices to be protected against them. Despite the fact that commercial enterprises are invested in billions of dollars in cybersecurity to be protected against these dangers, the success of the measures is still in debate. How can individual Internet users protect themselves if commercial firms are hardly protected from this threat? Therefore, it is necessary to determine how, where, when and why a threat occurs.

This study addresses the detection and analysis of CryptoWall attack, which is one of the new generation Ransomware, in detail. It was suggested that studies conducted on this subject should address the technical analysis dimension as well. After evaluating the file-directory and registry logs of the detected CryptoWall Ransomware, CryptoWall's network accesses were analyzed to find out the IP address and Domain information of the attacker, and the DNS records of the attacker were identified. Company records and contact information have been identified through a WHOIS query.

We anticipate that our research will have a positive impact not only on the cybersecurity industry but also on future research and on many individual Internet users. Finally, we believe that technical analysis studies are required for different types of Ransomware that have advanced encryption algorithms.

References

[1] B. Anderson, D. Quist, J. Neil, C. Storlie, and T. Lane. 2011. Graph-based malware detection using dynamic analysis. Journal in Computer Virology, 7(4):247–258.

[2] T. Hastie, R. Tibshirani, and J. H. Friedman. The Elements of Statistical Learning: Data Mining, Inference, and Prediction. Springer, 2009.

[3] M. Hopkins and A. Dehghantanha, “Exploit kits: The production line of the cybercrime economy?” in 2015 Second International Conference on Information Security and Cyber Forensics (InfoSec). IEEE, nov 2015.

[4] Scaife, N., Carter, H., Traynor, P., & Butler, K. R. (2016, June). Cryptolock (and drop it): stopping Ransomware attacks on user data. In Distributed Computing Systems (ICDCS), 2016 IEEE 36th International Conference on (pp. 303-312). IEEE.

[5] Rastogi, V., Chen, Y., & Jiang, X. 2014. Catch Me If You Can: Evaluating Android Anti-Malware Against Transformation Attacks. IEEE Trans. Information Forensics and Security, 9(1), 99-108.

[6] Faruki, P., Bharmal, A., Laxmi, V., Ganmoor, V., Gaur, M. S., Conti, M., & Rajarajan, M. 2015. Android security: a survey of issues, malware penetration, and defenses. IEEE communications surveys & tutorials, 17(2), 998-1022.

[7] K.-K. R. Choo, “The cyber threat landscape: Challenges and future research directions,” Computers & Security, vol. 30, no. 8, pp. 719–731, nov 2011.

[8] J. Walls and K.-K. Choo, 2017. “A study of the effectiveness abs reliability of android free anti-mobile malware apps,” in Mobile Security and Privacy. Elsevier, pp. 167–203.

[9] A. Gazet. Comparative analysis of various Ransomware virii. 2010. Journal in Computer Virology, 6(1):77–90.

[10] A. L. Young. 2006. Cryptoviral extortion using microsoft’s crypto API. International Journal of Information Security, 5(2):67–76.

[11] Scaife, N., Carter, H., Traynor, P., & Butler, K. R. 2016, June. Cryptolock (and drop it): stopping ransomware attacks on user data. In Distributed Computing Systems (ICDCS), 2016 IEEE 36th International Conference on (pp. 303-312).

[12] J. Oberheide, E. Cooke, and F. Jahanian. CloudAV: N-Version antivirus in the network cloud. In USENIX Security Symposium, 2008.

[13] P. Traynor, M. Chien, S. Weaver, B. Hicks, and P. McDaniel. 2008. Noninvasive methods for host certification. ACM Transactions on Information and System Security, 11(3).

[14] J. Z. Kolter and M. A. Maloof. 2006.Learning to detect and classify malicious executables in the wild. The Journal of Machine Learning Research, 7:2721–2744.

[15] V. Chandola, A. Banerjee, and V. Kumar. Anomaly detection: A survey. 2009.ACM Comput. Surv., 41(3).

[16] H. L. Kevin Savage, Peter Coogan, The evolution of Ransomware. Symantec, 2015.

[17] K. Rieck, P. Trinius, C. Willems, and T. Holz. Automatic analysis of malware behavior using machine learning. Dec. 2011. J. Comput. Secur., 19(4):639–668.

[18] Richardson, R., & North, M. 2017. Ransomware: Evolution, mitigation and prevention. International Management Review, 13(1), 10-21.

[19] Luo, X., & Liao, Q. 2007. Awareness education as the key to Ransomware prevention. Information Systems Security, 16(4), 195-202.

[20] Symantec, “Internet security threat report,” Symantec, Tech. Rep., apr 2016.

[21] K. Cabaj and W. Mazurczyk, 2016. “Using software-defined networking for Ransomware mitigation: The case of CryptoWall,” IEEE Network, vol. 30, no. 6, pp. 14–20.

[22] A. Patcha and J.-M. Park. 2007. An overview of anomaly detection techniques: Existing solutions and latest technological trends. Computer Networks, 51(12).

[23] F. Sinitsyn. Teslacrypt 2.0 disguised as cryptowall. https://securelist.com/blog/research/71371/ teslacrypt-2-0-disguised-as-cryptowall/, 2015.

[24] Kara, İ., & Aydos, M. (2019). The ghost in the system: technical analysis of remote access trojan. International Journal on Information Technologies & Security, 11(1).