International Journal of Scientific Research in Computer Science and Engineering
Vol.6, Issue.2, pp.1-9 , April (2018)

Research Paper

E-ISSN: 2320-7639

An Anti-Ransomware Tool Design by Using Behavioral and Static Analysis Methods

B. Celiktas[1*], N. Unlu[2], E. Karacuha[3]

[1]Applied Informatics Department, Institute of Informatics, ITU, Istanbul, Turkey
[2]Cyber Security Engineering and Cryptography Department, Institute of Informatics, ITU, Istanbul, Turkey
[3]Applied Informatics Department, Institute of Informatics, ITU, Istanbul, Turkey

Corresponding Author: celiktas16@itu.edu.tr, Tel.: +90-541-4168162

Available online at: www.isroset.org

Received: 27/Feb/2018, Revised: 12/Mar/2018, Accepted: 31/Mar/2018, Online: 30/Apr/ 2018

Abstract— Ransomware, which constantly improves by updating itself and transferring to the network and computing environment, is the most common type of malware used by the attackers recently. Ransomware demands ransom from the user for decrypting the encrypted files. As a result of the payment of the desired amount of ransom, the files can be opened with the decryption key delivered to the user. Various antivirus software using static analysis methods fails to detect the malware because it performs analysis via hash signature samples in databases. Because hash signature samples of zero-day attacks are not recorded in anti-virus databases, detecting malware by using behavioral analysis methods is more effective. Anti-ransomware in the hybrid structure using static analysis methods, along with behavioral analysis methods, will be even more successful in detecting and preventing ransomware with minimum false-positive rate and minimal file loss. As a result of a comprehensive review of related literature and professional reports on ransomware, the attack vectors of the ransomware, the core features, the identification methods and the movements based on the Windows Operating Systems have been found. This study presents the behavior of the ransomware in detail and explains how should an anti-ransomware tool be created to detect and prevent ransomware on Windows Operating Systems.

Keywords— Ransomware; Encryption; Static Analysis; Behavioral Analysis; Attack Vectors

I. INTRODUCTION

Ransomware has been widely used to target the computers recently, and new types are being constantly added to the family. Ransomware reaches the target computer using social engineering techniques and activates after the victim downloads the e-mail attachments or clicks on insecure links. Since ransomware spreads over the network easily, the number of victims exposed to this threat is very high.

Since ransomware hides its location once it reaches to the target through jump points, detecting an attack becomes extremely difficult. The ransomware encrypts the most commonly used files in the target computer; therefore, individual users or even institutions are forced to pay a ransom for decryption. Attackers nowadays prefer Bitcoin, an anonymous payment mechanism, as a means for payment, thereby concealing their identity and location. These peculiarities encourage attackers to choose ransomware, compared to other malware, in their malicious attacks [1].

In our study, we present the basic characteristics of the anti-ransomware tool, which detects and prevents ransomware on machines with Windows Operating Systems. Our study utilized many academic publications and the reports of leading international cybersecurity companies. Based on the findings from the comprehensive review of related literature and tests performed on Kali Linux machine, Windows 7, and Windows 10, behavioral characteristics of the most basic ransomware are analyzed and then how ransomware can be detected and prevented is described. The basic contributions of this study to the literature are as follows:

- We present the ransomware that tries to be effective in Windows Operating Systems with minimum false positive results with a hybrid mechanism, which uses both static and behavioral analysis techniques together.
- We expect to be an anti-ransomware solution that detects and prevents ransomware and an example in the design of a commercial anti-ransomware tool.
- We think that this study will be a guide for the academic studies on ransomware.

The rest of the study is as follows. Section II defines and provides an overview about ransomware, Section III examines the ransomware families, Section IV explains the

anatomy of ransomware, Section V describes the anti-ransomware tool's properties, and Section VI concludes with future directions and recommendations.

II. THEORY

A. Ransomware

Ransomware is a type of malware that encrypts files on the target computer using strong cryptographic algorithms. The ransomware, after completing the encryption process, requests ransom from the victim with the information note opened on the target computer. The victim cannot open their files without paying the requested ransom, since the private key to open the encrypted files is usually stored in the attacker's Command and Control (C&C) server.

B. Locker-Ransomware and Crypto-Ransomware

There are two basic types of ransomware. The first is the Locker Ransomware. This type prevents the computer's operating system and applications from running and even opens the computer to prevent the user from performing normal operations. The second is the Crypto Ransomware. This ransomware encrypts the files in the computer's disk through the functions of the computer's operating system are running smoothly [2],[3],[4],[5].

C. Attack Vectors

The most commonly used attack vectors in ransom attacks are spam and phishing e-mails using social engineering techniques. A ransomware is generally activated by opening the e-mail containing the malicious macro and loading to the computer the executable file of the script running with the activation of macro which is in the file [6],[7],[8].

D. C&C Servers

It is very important for the attacker to ensure confidentiality and keep the location of the C&C servers undetectable [7],[9]. Thus, the new generation ransomware attacks are made via encrypted HTTPs protocol or the TOR network. The use of fully encrypted channels such as TOR and HTTPs makes the creation of the signature of the attack in advance impossible [7],[10].

E. Target File Types

File types targeted by ransomware constantly change and vary. The attacker determines target file types before the attack. For instance, a ransomware aimed at a large corporation targets the databases, financial and CAD files. In addition, more than 70 file types have become standard targets in ransomware attacks [8].

F. Payment Analysis

Up till recently, victims paid the required ransom for the decryption of encrypted files with various methods such as via mail checks, wire transfers, and payment vouchers. However, attackers recently prefer Bitcoin cryptocurrency, which is the de facto standard and more convenient and secure for attackers [8]. Bitcoin payment transactions cannot be recovered, and one out of five people who paid the requested ransom to the attackers could not get their files back [12].

G. Encryption Methods

The ransomware use encryption algorithms that vary from RC4 to RSA+AES and ECDH+AES. While the attackers used only symmetric encryption methods at the advent of the ransomware threat, they now prefer the hybrid encryption mechanism, which utilizes both symmetric and asymmetric encryption methods [8]. In the new generation ransomware attacks, only the public key is sent to the infected machine from the cryptographic key pair created on the C&C server, and the private key is never let out from the server.

The files on the infected machine are usually encrypted with AES-128, which is one of the symmetric encryption methods. The symmetric key used for encryption is re-encrypted usually with the RSA-2048 public key which is one of the asymmetric encryption methods so that encrypted files cannot be easily decrypted later [7],[10]. This process happens so fast that the encryption of the files in the target machine takes less than three minutes [13].

III. THE RANSOMWARE FAMILIES

In this part of our study, we will discuss the features of six most commonly known ransomware in the previous five years, i.e. the Cryptolocker, CryptoWall, Cerber, Locky, WannaCry, and Petya.

A. Cryptolocker

Cryptolocker launched in September 2013 with a widespread attack, literally starting the history of modern ransomware [5]. It managed to influence over 500,000 machines [8]. In just one month, the attack generated over $34,000 in revenue [14]. It often affected the systems with the spam e-mail method. After users clicked on the link, the ransomware started scanning the network devices, modifying the names of the files and folders, and encrypting them with the RSA asymmetric algorithm [4].

CryptoLocker 2.0, which is the newer and improved version and written with C# programming language appeared in December 2013. It currently uses Tor network for anonymity, 2048-bit encryption mechanism for extortion and Bitcoin for payment methods [14].

B. CryptoWall

First appeared in November 2013, CryptoWall is still one of the most widely used ransomware. In just six months; it infected more than 600,000 machines and encrypted about 5.25 billion files [4],[12]. Since the end of 2014, several versions have come into the market. It is a dangerous

ransomware with its persistence and property of process injection. By making each file name encrypted unique, makes it difficult to identify the danger [8]. It uses TOR network for the payment of ransom [5]. It demands as ransom initially $500 and after seven days $1,000. Payments are accepted in Bitcoins.

In January 2015, CryptoWall 2.0 came into the market. This version uses a unique Bitcoin address and safely deletes unencrypted original files. To hide the location of the C&C server, it uses TOR network as well [4]. In March 2015, ransomware developers released a new version named CryptoWall 3.0 [4]. In September 2015, CryptoWall 4.0 came into the market. Compared to the previous versions, there are some significant changes in this version such as encrypting file names, a more powerful Volume Shadow Copy (VSC) deletion method, a new type of ransom note, new payment mechanisms and a redesigned HTML ransom note [4]. Unlike other versions, this version of the code is still unbroken [7].

C. Cerber

Cerber first appeared in the first half of 2015. Files are encrypted with the ".cerber" extension and pop-ups are shown in HTML format [5]. It leaves not only the ransom note but also an audio record. In regards, it is the first ransomware to interact with the victim [7]. Cerber's C&C servers can work even if it is offline [10].

D. Locky

Locky, first seen in February 2016, is a complicated and sophisticated ransomware that uses malicious macros in a Word document and reaches the target computer via spam e-mails [7]. The oldest versions of Locky ransomware used the phishing methods [5]. Only in the first days of its emergence, Locky infected about 100,000 computers [3]. Locky encrypts not only the files on the computer but also the VSCs using Volume Shadow Copy Service (VSS) to prevent the user's files being restored. It encrypts VSCs and every file it can find, including system files. Locky also encrypts external hard drives, database files, all network resources, and Bitcoin wallet to force the victim to pay the ransom [3].This ransomware also targets virtual machines.

Encrypted files are renamed as follows: New file name precedes with the victim's unique ID, followed by the file's ID and the ".locky" file extension. So to sum, Locky has a good engineering design, and it is very clever and ruthless.

E. WannaCry / Wanna Decryptor

WannaCry or Wanna Decryptor ransomware began to spread on May 12, 2017, by means of exploit vector named EternalBlue which was developed by the US National Security Agency (NSA) by exploiting the gap in the Microsoft's Server Message Block (SMB) protocol [15]. It has been effective in about 150 countries and 300,000 computers, which has been the largest ransomware attack in history. The ransom demanded, written in 28 different languages, is about $300 [8].

The update, published by Microsoft as a critical patch on March 14, 2017, has not been used by many organizations. So it has allowed the ransomware to spread very quickly over the internet [16]. WannaCry uses RSA-2048 as the encryption method. Like others, it uses the VSS to delete VSCs of files and the TOR network to hide the C&C Server [10].

F. Petya

Petya, which emerged in April 2016, causes a full blue screen of death crash by overwriting the Master Boot Record (MBR). Petya is also coded to delete the randomly generated unique key used to encrypt the Master File Table (MFT) [5].

When the victim opens the computer, the ransom note appears on the screen. Petya benefits from the security gap "EternalBlue", which targets SMB v1, which was also used in the WannaCry attack. Petya is the first example of such ransomware with encrypting the disc, encrypting all files and preventing the computer to be turned on [12]. In addition, Petya can work without contacting the C&C server, that is, independently from the internet [10].

IV. THE RANSOMWARE'S ANATOMY

The anatomy of the ransomware is described in detail below.

- First, click on the link to download and run the ransomware,
- Then, the ransomware is executed [3],
- Before encryption starts, information about the target machine, such as processor, hostname, RAM, etc. information in the hash state, is collected to identify the device. The ransomware creates a registry key in the following paths that it will use to store configuration information. These paths are "HKCU\Software\<uniquecomputerid>\<random id>" and "HKCU\Software \[random]".
- The ransomware checks whether there is any software that has been injected into the system before. If there is no software injected into the system;
    - The ransomware creates an instance of "explorer.exe" and injects itself into it [3]. This process is shown in Figure 1 and Figure 2.
    - The most recently created instance of "explorer.exe" establishes a TCP connection with the C&C server, and the ransomware is hidden in order not to be detected as shown in Figure 3.

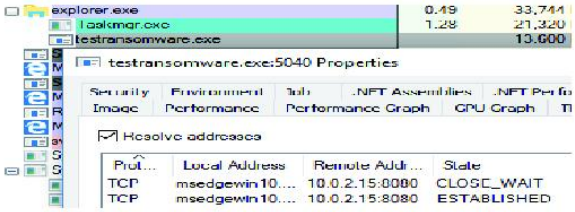

Figure 1. A connection image of "testransomware.exe" installed by C&C server

```
meterpreter > migrate 3240
[*] Migrating from 6604 to 3240...
[*] Migration completed successfully.
```

Figure 2. A migration of "testransomware.exe" service to "explorer.exe" service

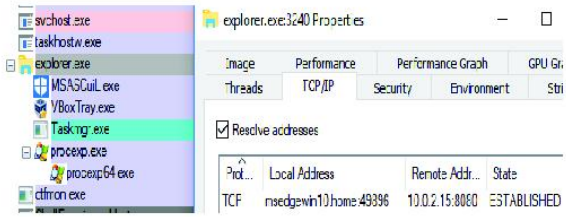

Figure 3. The image of "testransomware.exe" service not to be seen as a service

- The ransomware generally runs in the "%Localapp data%", "%ProgramData%", "%UserProfile%", and "%Temp%" paths [17].
- The ransomware also creates the "svchost.exe" instance [3]. This file is located in either "C:\ Windows\System32" or "C:\Winnt\System32" path.
- The alteration is made at the registry run key in the following path, to become persistent and executable after restarting [3]. This path is "HKCL\Software\ Microsoft\Windows\Currentversion\Run".
- The ransomware use "vssadmin.exe" service to delete or encrypt VSCs in the system [3],[7],[8],[10].
- In some ransomware attacks, "wmic.exe" service is used to delete all files in the VSCs [7].
- The ransomware may prevent altering Windows boot options, and also certain backup applications. So, the ransomware wants to disable recovery and Windows error recovery on startup by using "bcdedit.exe" service [7],[8],[18].
- The ransomware may disable the Windows System Restore feature before starting the encryption process [7].
- The ransomware can use "syskey.exe" service to encrypt user files and "cipher.exe" service to manage encrypted data.
- Encrypted files are converted into specific file extensions. The list of common ransomware encrypted file extensions are ".ccc", ".cerber", ".cerber2", ".cerber3", ".crypt", ".cryptolocker", ".cryptowall", ".ecc", ".ezz", ".locky", ".micro", ".zepto", and ".encrypted" [17].
- The ransomware may stop special services such as "wscsvc", "WinDefend", "wuauserv", "BITS", "WerSvc", etc. on the device.
- The C&C server is contacted and encryption keys with the victim's ID and password are transmitted [3],[7].
- All data traffic between the C&C server and the client generally goes to and from an encrypted protocol such as HTTPs or TOR [2].
- Files are encrypted and extortion messages about the payment of a ransom are displayed [3].

The ransomware uses a variety of attack vectors to access the target computer and develops itself constantly against the measures taken. The ransomware constantly adds new features against the defense mechanisms [5]. Today, security solutions such as firewalls and antivirus, which are traditional detection methods using threat signature samples in databases, fail to detect and prevent ransomware [8]. Therefore, using both static and behavioral methods to detect and prevent ransomware is a wiser solution [19]. Our main aim in this study is to introduce a method that detects and prevents the ransomware attacks at the beginning of the encryption. Therefore, the important point here is that threat is to be prevented with minimum false-positive and minimum file loss before the files encrypted.

The anti-ransomware tool designed for detecting and preventing the ransomware attacks consists of two phases.

1st Phase: The Phase of Static Analysis - Detection and Prevention

2nd Phase: The Phase of Behavioral Analysis - Detection and Prevention

V. AN ANTI-RANSOMWARE TOOL'S PROPERTIES

The anti-ransomware tool we propose checks registry records, the behavior of services and processes at the operating system level and continuously monitors the encryption process that the ransomware tries to start on the file system. In addition, the tool checks whether the asymmetric encryption keys used by the new generation ransomware are in contact with the C&C server that stores the ransomware, analyzes the network traffic and does signature-based control of downloaded files. In order to reach the aim of detecting and preventing with minimum file loss and minimum false-positive alarms, the tool is designed

to have a hybrid structure that combines the behavioral analysis method with the static analysis method.

The diagram of the phases of an anti-ransomware tool is shown in Figure 4.

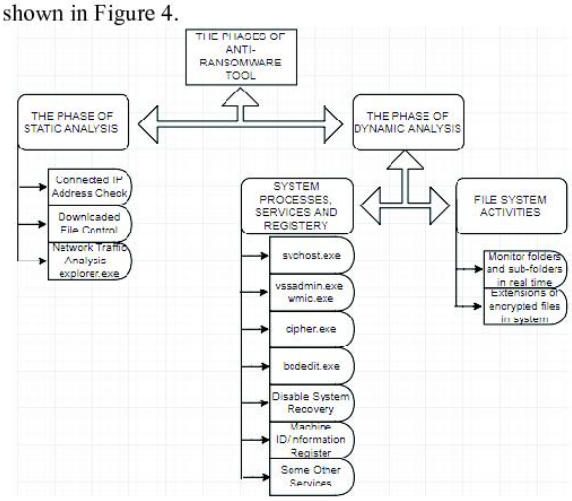

Figure 4. The diagram of the phases of the anti-ransomware tool

These phases will be explained in detail below.

A. The Phase of Static Analysis - Detection and Prevention

In this phase, the computer network connections and downloaded files are analyzed for malicious content.

1) Checking Which IP Addresses Are Connected: IP addresses and Process Identification (PID) numbers that are "Established" from port 443 will be continuously monitored as seen in Figure 5, Figure 6.

```
netstat -ano 2 | findstr "ESTABLISHED" | findstr ":443" >result.dat
```

Figure 5. Searching network connections which are "Established" from "Port 443"

```
TCP    10.84.249.81:2213      172.217.17.163:443     ESTABLISHED     9852
TCP    10.84.249.81:2216      53.140.40.98:443       ESTABLISHED     9852
TCP    10.84.249.81:2233      104.20.59.238:443      ESTABLISHED     9852
TCP    10.84.249.81:2238      151.101.112.201:443    ESTABLISHED     9852
TCP    10.84.249.81:2252      216.58.212.227:443     ESTABLISHED     9852
```

Figure 6. The result of the command in Figure 5

The public IP addresses in Figure 6 are checked through the Virus Total API as shown in Figure 7 and if the result comes as malicious, the connection is ended by terminating the PID number of that IP as shown in Figure 8.

```
import requests
url = 'https://www.virustotal.com/vtapi/v2/ip-address/report'
params = {'apikey':'<apikey>','ip':'<ip>'}
response = requests.get(url, params=params)
print(response.json())
```

Figure 7. An instance of a python code that checks IP address.

```
taskkill /F /pid <PID number>
```

Figure 8. Terminating a malicious IP's connection

2) Checking Downloaded File: Whether the file downloaded to the computer is malicious is checked in almost 70 cybersecurity vendors' database as in Figure 9. This python code sends a hash value of a downloaded file to TotalVirus via the get method in order to check whether the file is malicious. The file that comes out "clean" or "not malicious" from this control can be run. Otherwise, the file will be deleted before running and the user will be warned.

```
import requests
url = 'https://www.virustotal.com/vtapi/v2/file/report'
params = {'apikey': '<apikey>', 'resource': '<resource>'}
response = requests.get(url, params=params)
print(response.json())
```

Figure 9. An example of a python code to check downloaded files.

3) Monitoring A Sample of Explorer.exe's Network Traffic: "Explorer.exe" is a component of the Windows operating system that provides many users with interfaces on the monitor such as the taskbar and the desktop besides provides a graphical user interface(GUI) to access the file systems. Before affecting the system, the ransomware launches a new suspended "explorer.exe" process and injects itself by allocating memory. The ransomware injected by the attackers communicate with the C&C servers through this process.

Before encrypting the files of the victim, the C&C servers are contacted and the encryption keys are transmitted between the victim and the attacker. In this phase, the tool tries to determine whether the connection with the C&C servers is established. If any connection is detected, i.e., the attacker has control over the victim computer through the ransomware and can start the encryption process, the connection has to be terminated. To find an answer to the question "Does the last instance of "explorer.exe" create a TCP/IP connection with a remote C&C server?", the commands in Figure 10 and Figure 11 are executed.

```
C:\Users\brscl>tasklist /fi "IMAGENAME eq explorer.exe"

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
explorer.exe                 10484 Console                    2    156,144 K
```

Figure 10. Learning "explorer.exe"s PID number

```
C:\Users\brscl>netstat -ano |findstr 10484
```

Figure 11. Learning C&C Server's IP address connected via TCP protocol.

If the instance of "explorer.exe" connecting to a remote computer is detected, this connection will be terminated as in Figure 8.

B. The Phase of Behavioral Analysis

In this phase, the tool will analyze the behavior of the Windows operating system processes, services, registry records and the file system. The steps used for controlling and monitoring to achieve defined goals are explained in detail.

1) System processes, services, and registry: Operating Systems cannot provide full functionality to their users without Windows processes. Some processes require special rights or resources that a normal user cannot use. In some cases, an attacker may also escalate his/her privileges by exploiting the "normal" behavior of these processes.

a) Svchost.exe: This process is required to load the ".dll" files that are needed for the Windows and its programs running on the computer. The file of "svchost.exe" is located at the "C:\\Windows\System32" or "C:\Winnt\ System32" paths. Because "svchost.exe" is the common system process like "explorer.exe", ransomware usually is hidden under this name. To reduce resource consumption, many services share the "svchost.exe" process and migrate itself to this process. A single "svchost.exe" process can load and manage multiple services. These services are in the following Windows registry key: HKLM\ Software\Microsoft\ WindowsNT\CurrentVersion\SvcHost**.**

"Svchost.exe" infections usually install themselves by copying the executables into the system files and making necessary modifications in the registry so that infections can be run whenever the system is started [7]. To accomplish this operation, the path of "HKLM\Software\Microsoft\Windows\CurrentVersio n \Run" is used as shown in Figure 12.

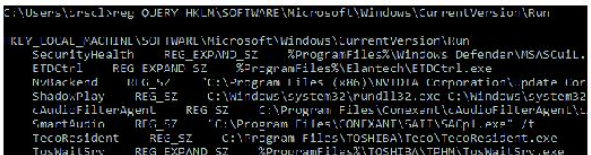

Figure 12. An instance of programs running in the path of HKLM\Software\Microsoft\Windows\CurrentVersion\Run

The tool should continuously monitor "HKLM\Software\Microsoft\Windows\CurrentVersio n\Run" path and if a new instance of "svchost.exe" occurs outside the path of "%ProgramFiles%", "%ProgramFiles(x86)%", and "%SystemRoot%\ System32", it is highly likely to be malware or ransomware. Hence, Figure 13 shows how to delete the instance of "svchost.exe" in the undesired paths.

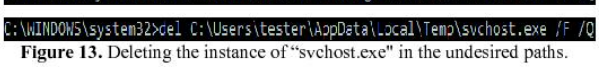

Figure 13. Deleting the instance of "svchost.exe" in the undesired paths.

b) Vssadmin.exe and wmic.exe: The new generation ransomware can permanently delete backed up files in VSCs using the VSS service. Thus, the victim cannot recover their files and has to pay the ransom to the attacker.

The Vssadmin tool is used to encrypt or delete VSCs. Some ransomware completely deletes the backed up folders and files on the system. And some terminates the process so that deleted or encrypted folders and files cannot be recovered. Figure 14 shows how some ransomware do the attacks described above [7],[8].

Figure 14. The command of deleting the VSCs on the computer.

In order prevent the attackers run these commands, the VSS service must be in the "Stopped" state. Therefore, the state of the VSS service has to be continuously monitored in our tool.

In addition, the tool needs to disable the VSS service by the command in Figure 15. So nobody can start a service if startup type is disabled.

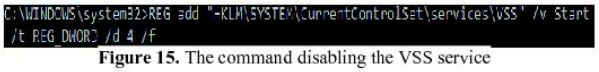

Figure 15. The command disabling the VSS service

The ransomware will need to reverse the operations to delete VSCs even the VSS service is "Stopped" and "Disabled". Hence, the output of Figure 16 will be continuously monitored where any change will indicate an abnormality and the tool will terminate the connection as in Figure 8.

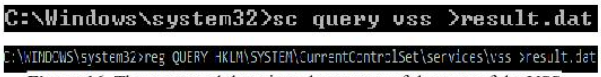

Figure 16. The command that gives the outputs of the state of the VSS service.

c) Cipher.exe and syskey.exe: The ransomware generally uses "cipher.exe" after the encryption is finished. So, the tool should disable "cipher.exe" as shown in Figure 17.

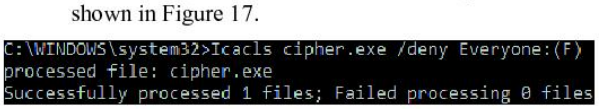

Figure 17. The command of taking all authority of "cipher.exe" file back and making unusable

According to Microsoft, the use of "syskey.exe" is no longer considered safe and is frequently used by computer hackers. Thus, we should disable it like we did for "cipher.exe".

d) Bcdedit.exe: Some ransomware block altering Windows boot options, they may also block certain backup applications. As seen in Figure 18 and Figure 19, the ransomware wants to disable recovery and Windows error recovery on startup [7],[8],[18].

```
C:\WINDOWS\system32>bcdedit /set {default} recoveryenabled NO
The operation completed successfully
```

Figure 18. The command of disabling recovery.

```
C:\WINDOWS\system32>bcdedit /set {default} bootstatuspolicy ignoreallfailures
The operation completed successfully
```

Figure 19. The command of disabling Windows error recovery on startup.

Therefore, the commands in Figure 20 and Figure 21 will run continuously and the attempt of the ransomware to prevent the system from correcting the error in the phase of disabling recovery and boot will be eliminated.

```
C:\WINDOWS\system32>bcdedit /set {default} recoveryenabled YES
The operation completed successfully
```

Figure 20. The command of enabling recovery.

```
C:\WINDOWS\system32>bcdedit /set {default} bootstatuspolicy displayallfailures
The operation completed successfully
```

Figure 21. The command of enabling Windows error recovery on startup.

e) Disabling Windows' System Restore Feature: In some ransomware attacks, the attacker disables the system restore feature before starting the encryption process. To do so, the attacker runs the command in Figure 22.

```
C:\WINDOWS\system32>Reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\
CurrentVersion\SystemRestore" /V DisableSR /t REG_DWORD /d 1 /f
```

Figure 22. The command of disabling system restore.

As a precaution, the output of Figure 23 should be monitored constantly and checked to see if the ransomware makes changes in the registry as in Figure 22. If any change is detected, the command in Figure 24 should be executed.

```
C:\WINDOWS\system32>Reg QUERY "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\
CurrentVersion\SystemRestore" >result.dat
```

Figure 23. The command of permanently monitoring a registry path.

```
C:\WINDOWS\system32>Reg add "HKLM\SOFTWARE\Microsoft\Windows NT\
CurrentVersion\SystemRestore" /V DisableSR /t REG_DWORD /d 0 /f
```

Figure 24. The command of enabling system restore.

f) Machine ID and Information Registry: Before encryption starts, information about the machine, such as processor, hostname, RAM, etc. information in the hash state, is collected to identify the device at C&C server.

When CryptoWall encrypts a file, it will store the file and its path as a value in the registry. The location of the subkey is in "HKCU\Software\<unique computer id>\<random id>" format. It will then create a value for each file that it encrypts under this key. The other example is Locky. It creates a registry key to store configuration information. This registry key is located at "HKCU\Software\[random]", "HKCU\Software\Locky", "HKCU\Software\Locky\id", "HKCU\Software\Locky\pubkey", "HKCU\Software\Locky\paytext", and "HKCU\ Software\Locky\completed".

So, the "HKCU\Software" path in the registry should be continuously monitored, as shown in Figure 25 and it should warn when registries such as CryptoWall or Locky instances are created.

```
C:\WINDOWS\system32>reg QUERY HKCU\SOFTWARE >result.dat
```

Figure 25. An HKCU\Software query for registry control

2) File System Activities:

a) Monitoring the folders and sub-folders in real time: The ransomware generally creates a copy of itself in the victim's specific folder path under a filename generally chosen randomly and obtained from the "%Windir%\system32" folder [18]. "%Localapp data%", "%Program Data%", "%UserProfile%", "%Temp%" sections are described as encryption locations generally used by ransomware [20]. So, an anti-ransomware tool should continuously monitor the file paths defined above.

b) Extensions of encrypted files in the system: Today, all categories of the ransomware have encrypted about 200 types of file. In this phase, the most popular and most widely used extensions among these file types will be checked. List of the common encrypted file extensions are ".ccc", ".cerber", ".cerber2", ".cerber3", ".crypt", ".cryptolocker", ".cryptowall", ".ecc", ".ezz", ".locky", ".micro", ".zepto", and ".encrypted" [17]. If the file extensions stated above are detected in the monitored file paths, they will indicate that there is a ransomware in the system.

Within the monitored folders, the presence of the extensions listed above is checked as shown in Figure 26.

```
fname = event.get_process().peek_string(lpFileName, fUnicode=True)
if fname.find(".ecc") >= 0 or fname.find(".ezz") >= 0:
    if dev:
        print "[*] Cryptolocker has detected! ->", fname
```

Figure 26. An example of generating a message when a file with extensions ".ecc" or ".ezz" written in Python script language is detected

VI. CONCLUSIONS AND RECOMMENDATIONS FOR FUTURE RESEARCH

The comprehensive review of related literature and professional reports suggest that using the static analysis methods by their own fails to detect and prevent ransomware. So, we try to design a tool with a hybrid mechanism, which uses both static and behavioral analysis techniques together.

We aim to create an anti-ransomware tool which detects the behaviors of the ransomware and prevents these behaviors before the encryption starts. A hybrid structure by using both behavioral and static analysis methods is preferred and suggested to perform this aim.

In the phase of static analysis, network traffic analysis of the last created "explorer.exe" sample, signature-based controls of connected IP addresses, and downloaded files are performed.

In the phase of behavioral analysis, monitoring the operating system processes, services, registry records, as well as behaviors on the file system is performed.

When an anti-ransomware tool detects an abnormality in the phases of static or behavioral analysis, it provides an early warning to the user and prevents the ransomware from running. In addition, our tool provides protection against not only the known ransomware but also zero-day ransomware that has never existed before. Our main aim when detecting and preventing ransomware is to maintain minimum false positive alarms and minimum file loss on the system.

This study suggests a better perspective to the users, software developers, and security administrators about the key features of the anti-ransomware tool that can be used as a solution. This tool does not require high fees for commercial software and provides the users with flexibility in taking measures against ransomware. We believe that several people involved in the software development business will be able to design anti-ransomware tools by examining the content of our study.

We also think that our study will be a guide for future academic studies on ransomware and other malware.

ACKNOWLEDGMENT

The authors would like to thank Virus Total for providing private API key support. The authors also thank Mehmet Celiktas, a Ph.D. student at the Boğaziçi University, who spent a good deal editing the article. The work is partially supported by the Istanbul Technical University Informatics Institute. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the Istanbul Technical University Informatics Institute.

REFERENCES

[1] N. Sacife, H. Carter, P. Traynor and K. R.B Butler, "CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data", IEEE 36th International Conference on Distributed Computing Systems, 2016.

[2] A. Bhardwaj, V. Avasthi, H. Sastry and G. V. B. Subrahmanyam, "Ransomware Digital Extortion: A Rising New Age Threat", Indian Journal of Science and Technology, Vol 9(14), 2016.

[3] M. Wecksten, J. Frick, A. Sjostrom and E. Jarpe, "A Novel Method for Recovery from Crypto Ransomware Infections", 2nd IEEE International Conference on Computer and Communications, 2016.

[4] M. H. U. Salvi, & M. R. V. Kerkar, "Ransomware: A cyber-extortion", Asian Journal of Convergence in Technology, 2(3), 2016.

[5] A. Zahra and A. S.Munam, "IoT Based Ransomware Growth Rate Evaluation and Detection Using Command and Control Blacklisting", Proceedings of the 23rd International Conference on Automation & Computing, University of Huddersfield, Huddersfield, UK, 7-8, 2017.

[6] CheckPoint, "Ransomware: Attack Trends, Prevention, And Response", White Paper, 2017.

[7] A. Liska and T. Gallo, "Ransomware: Defending Against Digital Extortion", O'Reilly Media, Inc., 2016.

[8] V. Kotov, M. S. Rajpal, "In-Depth Analysis of the Most Popular Malware Families", Bromium, Understanding Crypto-Ransomware Report, 2014.

[9] N. Hampton and Z. A. Baig, "Ransomware: Emergence of the cyber-extortion menace," Aust. Inf. Secure. Manag. Conf., vol. 2015, pp. 47–56, 2015.

[10] A. Adamov, A. Carlsson, "The state of ransomware. Trends and mitigation techniques", vol. 00, no., pp. 1-8, Doi:10.1109/ EWDTS. 2017.8110056, 2017.

[11] N. Hampton and Z. A. Baig, "Ransomware: Emergence of the cyber-extortion menace," Aust. Inf. Secure. Manag. Conf., vol. 2015, pp. 47–56, 2015.

[12] Kaspersky Lab, "Kaspersky Security Bulletin, Story of The Year: The Ransomware Revolution", Report, 2016.

[13] B. Heater, "How ransomware conquered the world", PC Magazine Digital Edition, 2016.

[14] Symantec, "CryptoDefense, the CryptoLocker Imitator, Makes Over $34,000 in One Month", Symantec Security Response, 2014.

[15] A. Liska, T. Gallo, "Ransomware: Defending Against Digital Extortion", O'Reilly Media, Inc. First Ed., 2016.

[16] T. Anjana, "Discussion On Ransomware, WannaCry Ransomware, and Cloud Storage Services Against Ransom Malware Attacks", IJRTI, Vol.2, Issue 6, ISSN: 2456-3315, 2017.

[17] Webroot, "MSP Guide: Stopping Crypto Ransomware Infections in SMBs, 16 Easy Actions for MSPs", White Paper, 2017

[18] A. Anubhav and R. Ellur, "Cerber: Analyzing a Ransomware Attack Methodology To Enable Protection", Threat Research, Advanced Malware, FireEye, 2016.

[19] U.K. Singh, C. Joshi, and S.K. Singh. "Zero-day Attacks Defense Technique for Protecting System against Unknown Vulnerabilities", International Journal of Scientific Research in Computer Science and Engineering, 5(1), 2017.

[20] Malwarebytes, "Cybercrime tactics and techniques", Report, Q1 2017.

Authors Profile

Mr. Baris Celiktas pursued Bachelor of Science in Systems Engineering - Electric and Electronic from Turkish Military Academy, Turkey in 2008 and Master of Science in Cyber Security & International Relations from Karadeniz Technical University in 2016. He is currently pursuing Master of Science Programme in the Institute of Informatics, Department of Applied Informatics, Istanbul Technical University, and working as IT System and Security Manager. His main research work focuses on Information Security, Malware Analysis, Cyber Security, and Network Security. He has 2 years of teaching experience in cybersecurity.

Mr. Nafiz Unlu pursued Bachelor of Science at Electrical Engineering from Yildiz Technical University in 1982, Master of Science at Electronics and Telecommunication from Uludag University in 1985, Master of Science at Artificial Intelligence with Engineering application from the University of Wales in 1991 and Ph.D. at Electronics from Istanbul University in 1995. He is currently working as Assistant Professor in Institute of Informatics, Department of Cyber Security Engineering and Cryptography, Istanbul Technical University since 2015. His main research work focuses on Network Security, Artificial Intelligence, Knowledge-Based Systems, Autonomous Robots, and Disaster Management. He has 23 years of teaching experience.

Mr. Ertugrul Karacuha pursued Bachelor of Science at Electronics and Communication Engineering from Istanbul Technical University in 1986, Master of Science at Electronics and Telecommunication Engineering from Istanbul Technical University in 1990, Master of Science at Economics from the Istanbul University in 1992, Ph.D. at Economics from the Istanbul University in 1992, Ph.D. at Electronic Engineering from Çukurova University and Istanbul Technical University in 1993. He is currently working as Professor in Institute of Informatics and Head of Applied Informatics Department, Istanbul Technical University. His main research work focuses on Electromagnetic Fields and Microwave, Electronic Communication Regulations, Inverse Scattering Problems.

