

MALWARE ANALYSIS

*A project report submitted in partial fulfillment of the requirements for the
award of the degree of*

POST GRADUATE DIPLOMA IN CYBERSECURITY AND FORENSICS (PG-DCSF)

Submitted by

SAMEER VASUDEV TALASHILKAR	(230960940044)
KRUSHNA SANJAY DEORE	(230960940024)
MOKSH AGARWAL	(230960940028)
ANDAVARAPU SAI SIVA MARDHAV	(230960940005)
SOUMYA AGNIHOTRI	(230960940050)



Under the supervision of
Prof. Sreedeeep A L

Department of Cyber Security & Forensics

Centre for Development of Advanced Computing
Technopark Trivandrum, Technopark Rd, opp. Thejaswini, Technopark
Campus, Kazhakkootam, Thiruvananthapuram, Kerala

Acknowledgement

We would like to express our deepest appreciation to all those who provided us the possibility to complete this project. Special gratitude to our project supervisor and **Prof. Sreedeeep A L**, whose contribution in simulating suggestions and encouragement helped us to coordinate our project especially in writing this report.

Furthermore we would also like to acknowledge with much appreciation the crucial role of our Cybersecurity specialist **Jayaram P**, also help us initiate our project work special thanks go to a facility provided suggestions and tips in for the enhancing of project we would also like to show gratitude towards of fellow classmates and our parents for helping us stay attentive and goal oriented in our pursuit of this project.

Candidates Declaration

We hereby declare that the work presented in this project report titled “**Malware Analysis**” submitted as in partial fulfillment of the requirement for the award of the post graduate diploma PG diploma in department of cyber security and forensics Centre for development of Advanced computing is an authentic record of our thesis carried out under the guidance of **Prof. Sreedeeep A L** ,Cyber security and forensic department

Date

SAMEER VASUDEV TALASHILKAR	(230960940044)
KRUSHNA SANJAY DEORE	(230960940024)
MOKSH AGARWAL	(230960940028)
ANDAVARAPU SAI SIVA MARDHAV	(230960940005)
SOUMYA AGNIHOTRI	(230960940050)

CERTIFICATE

It is to certify that the project entitled "Vulnerability Analysis and Penetration Testing on Crypto Bank" which is being submitted by (**SAMEER TALASHILKAR, KRUSHNA SANJAY DEORE, MOKSH AGARWAL, ANDAVARAPU SAI SIVA MARDHAV, SOUMYA AGNIHOTRI**) to Centre for Development of Advanced Computing in the partial fulfillment and of the requirement of postgraduate diploma PG diploma is a record of project work carried by them under my guiders and supervision the matter presented in the project report has not be submitted either in part of full to any university or institute for award of any degree.

TABLE OF CONTENTS

Topics	Page No.
1.Abstract	06
2.Introduction	07
3.Methodologies	13
4.Conclusion	26

ABSTRACT

Malware analysis is a pivotal aspect of cybersecurity aimed at understanding, dissecting, and mitigating malicious software threats. This Master's project report delves into the multifaceted domain of malware analysis, encompassing various methodologies, techniques, and tools employed to dissect and comprehend the intricate nature of malware.

The report begins by elucidating the fundamentals of malware, delineating its taxonomy, propagation mechanisms, and potential impact on systems and networks. It then progresses to discuss the significance of malware analysis as a proactive defense mechanism against evolving cyber threats.

Subsequently, the report explores the diverse approaches to malware analysis, including static analysis, dynamic analysis, and hybrid techniques. Static analysis involves examining the binary code and structure of malware without execution, whereas dynamic analysis involves running malware in a controlled environment to observe its behavior. Hybrid techniques combine elements of both static and dynamic analysis to provide comprehensive insights into malware functionalities.

Furthermore, the report highlights the pivotal role of malware analysis in incident response and forensic investigations, facilitating the identification of malicious artifacts, attribution of attacks, and development of effective countermeasures.

INTRODUCTION

What Is Malware?

Malware is a code that performs malicious actions; it can take the form of an executable, script, code, or any other software. Attackers use malware to steal sensitive information, spy on the infected system, or take control of the system. It typically gets into your system without your consent and can be delivered via various communication channels such as email, web, or USB drives.

The following are some of the malicious actions performed by malware: Disrupting computer operations Stealing sensitive information, including personal, business, and financial data Unauthorized access to the victim's system Spying on the victims Sending spam emails Engaging in distributed-denial-of-service attacks (DDOS) Locking up the files on the computer and holding them for ransom Malware is a broad term that refers to different types of malicious programs such as trojans, viruses, worms, and rootkits. While performing malware analysis, you will often come across various types of malicious programs; some of these malicious programs are categorized based on their functionality and attack vectors as mentioned here:

Virus or Worm: Malware that is capable of copying itself and spreading to other computers. A virus needs user intervention, whereas a worm can spread without user intervention.

Trojan: Malware that disguises itself as a regular program to trick users to install it on their systems. Once installed, it can perform malicious actions such as stealing sensitive data, uploading files to the attacker's server, or monitoring webcams.

Backdoor / Remote Access Trojan (RAT): This is a type of Trojan that enables the attacker to gain access to and execute commands on the compromised system.

Adware: Malware that presents unwanted advertisements (ads) to the user. They usually get delivered via free downloads and can forcibly install software on your system.

Botnet: This is a group of computers infected with the same malware (called bots), waiting to receive instructions from the command-and-control server controlled by the attacker. The

attacker can then issue a command to these bots, which can perform malicious activities such as DDOS attacks or sending spam emails.

Information stealer: Malware designed to steal sensitive data such as banking credentials or typed keystrokes from the infected system. Some examples of these malicious programs include key loggers, spyware, sniffers, and form grabbers.

Ransomware: Malware that holds the system for ransom by locking users out of their computer or by encrypting their files.

Rootkit: Malware that provides the attacker with privileged access to the infected system and conceals its presence or the presence of other software.

Downloader or dropper: Malware designed to download or install additional malware components.

What Is Malware Analysis?

Malware analysis is the study of malware's behavior. The objective of malware analysis is to understand the working of malware and how to detect and eliminate it. It involves analyzing the suspect binary in a safe environment to identify its characteristics and functionalities so that better defenses can be built to protect an organization's network.

Why Malware Analysis?

The primary motive behind performing malware analysis is to extract information from the malware sample, which can help in responding to a malware incident. The goal of malware analysis is to determine the capability of malware, detect it, and contain it. It also helps in determining identifiable patterns that can be used to cure and prevent future infections. The following are some of the reasons why you will perform malware analysis:

To determine the nature and purpose of the malware. For example, it can help you determine whether malware is an information stealer, HTTP bot, spam bot, rootkit, keylogger, or RAT, and so on.

To gain an understanding of how the system was compromised and its impact.

To identify the network indicators associated with the malware, which can then be used to detect similar infections using network monitoring. For example, during your analysis, if you determine that a malware contacts a particular domain/IP address, then you can use this domain/IP address to create a signature and monitor the network traffic to identify all the hosts contacting that domain/IP address.

To extract host-based indicators such as filenames, and registry keys, which, in turn, can be used to determine similar infection using host-based monitoring. For instance, if you learn that a malware creates a registry key, you can use this registry key as an indicator to create a signature, or scan your network to identify the hosts that have the same registry key.

To determine the attacker's intention and motive. For instance, during your analysis, if you find that the malware is stealing banking credentials, then you can deduce that the motive of the attacker is monetary gain.

Types Of Malware Analysis

To understand the working and the characteristics of malware and to assess its impact on the system, you will often use different analysis techniques. The following is the classification of these analysis techniques:

Static analysis: This is the process of analyzing a binary without executing it. It is easiest to perform and allows you to extract the metadata associated with the suspect binary. Static analysis might not reveal all the required information, but it can sometimes provide interesting information that helps in determining where to focus your subsequent analysis efforts. Chapter

2, Static Analysis, covers the tools and techniques to extract useful information from the malware binary using static analysis.

Dynamic analysis (Behavioral Analysis): This is the process of executing the suspect binary in an isolated environment and monitoring its behavior. This analysis technique is easy to perform and gives valuable insights into the activity of the binary during its execution. This analysis technique is useful but does not reveal all the functionalities of the hostile program.

Chapter 3, Dynamic Analysis, covers the tools and techniques to determine the behavior of the malware using dynamic analysis.

Code analysis: It is an advanced technique that focuses on analyzing the code to understand the inner workings of the binary. This technique reveals information that is not possible to determine just from static and dynamic analysis. Code analysis is further divided into Static code analysis and Dynamic code analysis. Static code analysis involves disassembling the suspect binary and looking at the code to understand the program's behavior, whereas Dynamic code analysis involves debugging the suspect binary in a controlled manner to understand its functionality. Code analysis requires an understanding of the programming language and operating system concepts.

Memory analysis (Memory forensics): This is the technique of analyzing the computer's RAM for forensic artifacts. It is typically a forensic technique, but integrating it into your malware analysis will assist in gaining an understanding of the malware's behavior after infection. Memory analysis is especially useful to determine the stealth and evasive capabilities of the malware.

Static analysis is the technique of analyzing the suspect file without executing it. It is an initial analysis method that involves extracting useful information from the suspect binary to make an informed decision on how to classify or analyze it and where to focus your subsequent analysis efforts.

Following techniques can reveal different information about the file.

1.Determining the File Type:

During your analysis, determining the file type of a suspect binary will help you identify the malware's target operating system (Windows, Linux, and so on) and architecture (32-bit or 64-bit platforms). For example, if the suspect binary has a file type of Portable Executable (PE), which is the file format for Windows executable files (.exe, .dll, .sys, .drv, .com, .ocx, and so on), then you can deduce that the file is designed to target the Windows operating system.

Most Windows-based malware are executable files ending with extensions such as .exe, .dll, .sys, and so on. But relying on file extensions alone is not recommended. File extension is not the sole indicator of file type. Attackers use different tricks to hide their file by modifying the file extension and changing its appearance to trick users into executing it. Instead of relying on file extension, File signature can be used to determine the file type.

2. Fingerprinting the Malware

Fingerprinting involves generating the cryptographic hash values for the suspect binary based on its file content. The cryptographic hashing algorithms such as MD5, SHA1 or SHA256 are considered the de facto standard for generating file hashes for the malware specimens.

File hash is frequently used as an indicator to share with other security researchers to help them identify the sample.

File hash can be used to determine whether the sample has been previously detected by searching online or searching the database of multi Anti-virus scanning service like VirusTotal.

Generating Cryptographic Hash Using Tools

On a Linux system, file hashes can be generated using the md5sum, sha256sum, and sha1sum utilities:

```
$ md5sum log.exe
```

```
6e4e030fbd2ee786e1b6b758d5897316 log.exe
```

```
$ sha256sum log.exe
```

```
01636faaae739655bf88b39d21834b7dac923386d2b52efb4142cb278061f97f log.exe
```

```
$ sha1sum log.exe
```

```
625644bacf83a889038e4a283d29204edc0e9b65 log.exe
```

For Windows, various tools for generating file hashes can be found online. HashMyFiles (http://www.nirsoft.net/utils/hash_my_files.html) is one such tool that generates hash values for single or multiple files, and it also highlights identical hashes with same colors.

3. Multiple Anti-Virus Scanning

Scanning the suspect binary with multiple anti-virus scanners helps in determining whether malicious code signatures exist for the suspect file. The signature name for a particular file can provide additional information about the file and its capabilities. By visiting the respective antivirus vendor websites or searching for the signature in search engines, you can yield further details about the suspect file. Such information can help in your subsequent investigation and can reduce the analysis time.

VirusTotal (<http://www.virustotal.com>) is a popular web-based malware scanning service. It allows you to upload a file, which is then scanned with various anti-virus scanners, and the scan results are presented in real time on the web page.

4. Extracting Strings

Strings are ASCII and Unicode-printable sequences of characters embedded within a file. Extracting strings can give clues about the program functionality and indicators associated with a suspect binary. For example, if a malware creates a file, the filename is stored as a string in the binary. Or, if a malware resolves a domain name controlled by the attacker, then the domain name is stored as a string. Strings extracted from the binary can contain references to filenames, URLs, domain names, IP addresses, attack commands, registry keys, and so on. Although strings do not give a clear picture of the purpose and capability of a file, they can give a hint about what malware is capable of doing.

pestudio 8.54 - Malware Initial Assessment - www.wintor.com

File Help

c:\users\test\desktop\mult.exe

	type	size	loc...	blacklisted (61)	item (372)
indicators (3/9)	unicode	7	-	x	AppData
vinustotal (n/a)	unicode	45	-	x	Software\Microsoft\Windows\CurrentVersion\Run
dos-stub (64 bytes)	unicode	38	-	x	netsh firewall delete allowedprogram "
file-header (20 bytes)	unicode	4	-	x	.exe
optional-header (224 bytes)	unicode	30	-	x	cmd.exe /c ping 0 -n 2 & del "
directories (5/15)	unicode	35	-	x	netsh firewall add allowedprogram "
sections (3)	unicode	13	-	x	Execute ERROR
libraries (1)	unicode	14	-	x	Download ERROR
imports (1)	unicode	5	-	x	start
exports (n/a)	unicode	12	-	x	Update ERROR
exceptions (n/a)	unicode	7	-	x	[ENTER]
tls-callbacks (n/a)	ascii	40	-	-	!This program cannot be run in DOS mode.
resources (1)	ascii	5	-	-	.text
strings (61/372)	ascii	7	-	-	@.reloc
debug (n/a)	ascii	4	-	-	3ji)
manifest (invoker)					



The *strings* utility ported to Windows by Mark Russinovich (<https://technet.microsoft.com/en-us/sysinternals/strings.aspx>) and PPEE (<https://www.mzrst.com/>) are some of the other tools that can be used to extract both ASCII and Unicode strings.

5. Determining File Obfuscation

Even though string extraction is an excellent technique to harvest valuable information, often malware authors obfuscate or armor their malware binary. Obfuscation is used by malware authors to protect the inner workings of the malware from security researchers, malware analysts, and reverse engineers. These obfuscation techniques make it difficult to detect/analyze the binary; extracting the strings from such binary results in very fewer strings, and most of the strings are obscured. Malware authors often use programs such as Packers and Cryptors to obfuscate their file to evade detection from security products such as anti-virus and to thwart analysis.

Dynamic Analysis

Dynamic analysis have two technique:

(I). Monitoring the malware interaction with environment:

1. Process 2. File system 3. Registry 4. Network

(II). Examining the system after the malware has executed

Process monitoring: Involves monitoring the process activity and examining the properties of the result process during malware execution.

File system monitoring: Includes monitoring the real-time file system activity during malware execution.

Registry monitoring: Involves monitoring the registry keys accessed/modified

and registry data that is being read/written by the malicious binary.

Network monitoring: Involves monitoring the live traffic to and from the system during malware execution.

4. Dynamic Analysis Steps

During dynamic analysis (behavioral analysis), you will follow a sequence of steps to determine the functionality of the malware. The following list outlines the steps involved in the dynamic analysis:

Reverting to the clean snapshot: This includes reverting your virtual machines to a clean state.

Running the monitoring/dynamic analysis tools: In this step, you will run the monitoring tools before executing the malware specimen. To get the most out of the monitoring tools covered in the previous section, you need to run them with administrator privileges.

Executing the malware specimen: In this step, you will run the malware sample with administrator privileges.

Stopping the monitoring tools: This involves terminating the monitoring tools after the malware binary is executed for a specified time.

Analyzing the results: This involves collecting the data/reports from the monitoring tools and analyzing them to determine the malware's behavior and functionality

To do dynamic analysis we need sandbox

We can use online sandbox like any. run or offline sandbox like cuckoo sandbox

But sandboxes have disadvantage:


- Sandbox evasion technique like num of desktop icon, system run time, mouse interaction
- Delaying execution: common technique used to delay the execution


METHODOLOGIES

Scanning the Suspect Binary with VirusTotal





VirusTotal ([http:// www. virustotal. com](http://www.virustotal.com)) is a popular web-based malware scanning service. It allows you to upload a file, which is then scanned with various anti-virus scanners, and the scan results are presented in real time on the web page. In addition to uploading files for scanning, the VirusTotal web interface provides you the ability to search their database using hash, URL, domain, or IP address. VirusTotal offers another useful feature called VirusTotal Graph, built on top of the VirusTotal dataset. Using VirusTotal Graph, you can visualize the relationship between the file that you submit and its associated indicators such as domains, IP addresses, and URLs. It also allows you to pivot and navigate over each indicator; this feature is extremely useful if you want to quickly determine the indicators associated with a malicious binary. For more information on VirusTotal Graph, refer to the documentation: [https:// support. virustotal. com/ hc/ en- us/ articles/ 115005002585- VirusTotal- Graph](https://support.virustotal.com/hc/en-us/articles/115005002585-VirusTotal-Graph).

How might you start investigating this suspicious file by using free online resources?

1e9f21f514ee4793cfae7bbaa21549be0d9b432c59513d2efed860c2b1501da39



vdaudio.dll

DETECTION	DETAILS	COMMUNITY 3
Ad-Aware	 Gen:Variant.Symmi.87557	
AhnLab-V3	 Trojan/Win32.Proxy.C906282	
ALYac	 Gen:Variant.Symmi.87557	
Arcabit	 Trojan.Symmi.D15605	

Exports

- gewayX
- gewayZ
- vdaudio

The following screenshot shows the detection names for a malware binary, and it can be seen that the binary was scanned with 70 Anti-virus engines; 63 of them detected this binary as malicious.

virustotal.com/gui/file/be22645c61949ad6a077373a7d6cd85e3fae44315632f161adc4c99d5a8e6844/detection

JURL, IP address, domain, or file hash

63 / 70

63 security vendors and 4 sandboxes flagged this file as malicious

Reanalyze Similar More

be22645c61949ad6a077373a7d6cd85e3fae44315632f161adc4c99d5a8e6844

Size: 224.00 KB | Last Analysis Date: 8 days ago

EXE

peexe checks-cpu-name runtime-modules detect-debug-environment long-sleeps direct-cpu-clock-access checks-user-input calls-wmi persistence

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 28 +

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: trojan.wannacryptor/wannacry Threat categories: trojan ransomware Family labels: wannacryptor wannacry wanna

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Trojan.Win32.WannaCryptor.R199610	Alibaba	Ransom:Win32/Wanna.f9fe677e
ALYac	Trojan.Ransom.WannaCryptor	Antiy-AVL	Trojan[Backdoor]/Win32.Farfil
Arcabit	Trojan.Ransom.WannaCryptor.D	Avast	Win32:Trojan-gen
AVG	Win32:Trojan-gen	Avira (no cloud)	TR/AD.WannaCry.vgssx
BitDefender	Trojan.Ransom.WannaCryptor.D	BitDefenderTheta	Gen:NN.Zexaf.36744.oq0@a8h6Gnji

Activate Windows
Go to Settings to activate Windows

If you wish to use the VirusTotal Graph on the binary to visualize indicator relationships, just click on the VirusTotal Graph icon and sign in with your VirusTotal (community) account.

virustotal.com/gui/file/be22645c61949ad6a077373a7d6cd85e3fae44315632f161adc4c99d5a8e6844/details

URL, IP address, domain, or file hash

DETECTIONDETAILSRELATIONSBEHAVIORCOMMUNITY28+

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Basic properties

MD5	5c7fb0927db37372da25f270708103a2
SHA-1	120ed9279d85cbfa5e5b7779ffa716207417a29
SHA-256	be22645c61949ad6a077373a7d6cd85e3fae44315632f161adc4c99d5a8e6844
Vhash	025046656d157058z27271z15z37z
Authentihash	7e9f8747fa2d7a35e87ddc8fa62d4d4b8da3b0cf3fa62f1df0a59b50e913bb7
Imphash	e858a14f217810d78466806d95d7fceb
Rich PE header hash	cbf5f3d2ba2423b2dfb5a475e1cc61c0
SSDEEP	3072:Y059femWRwTsldbeljOX8j/84pcRXPIU3Upt3or4H84IK8PtpLzLsR/EfcZ:+5RwTs/dSXj84mRXPermxdBIPVlZLeZ
TLSH	T1A024015A7A61877FD0B20532746194FB4EFE0DD3F5A89A4FE74D0A501F048884BE3A9B
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (GUI) Intel 80386, for MS Windows
TrID	Win32 Executable MS Visual C++ (generic) (37.8%) Microsoft Visual C++ compiled executable (generic) (20%) Win64 Executable (generic) (12.7%) Win32 Dynamic ...
DetectItEasy	PE32 Compiler: EP:Microsoft Visual C/C++ (6.0 (1720-9782)) [EXE32] Compiler: Microsoft Visual C/C++ (12.00.9782) [C++] Linker: Microsoft Linker (6.00.8047) T...
File size	224.00 KB (229376 bytes)
PEID packer	Microsoft Visual C++

History

Creation Time	2009-07-14 00:03:18 UTC
First Seen In The Wild	2021-01-31 08:24:26 UTC
First Submission	2017-04-28 10:52:07 UTC
Last Submission	2024-02-22 15:29:18 UTC
Last Analysis	2024-02-15 05:15:51 UTC

Activate Windows
Go to Settings to activate

virustotal.com/gui/file/be22645c61949ad6a077373a7d6cd85e3fae44315632f161adc4c99d5a8e6844/relations

URL, IP address, domain, or file hash

DETECTIONDETAILSRELATIONSBEHAVIORCOMMUNITY28+

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Contacted URLs (5)

Scanned	Detections	Status	URL
2024-02-17	0 / 92	200	http://www.microsoft.com/pki/certs/MicCodSigPCA_08-31-2010.crt
2024-02-17	0 / 92	200	http://crt.sectigo.com/SectigoPublicCodeSigningCAR36.crt
2024-02-17	0 / 92	200	http://crt.sectigo.com/SectigoPublicCodeSigningRootR46.p7c
2024-02-17	0 / 92	200	http://www.microsoft.com/pki/certs/MicrosoftTimeStampPCA.crt
2024-02-23	0 / 92	-	http://172.16.1.2:5357/048da2fc-03cd-4f4f-9037-fcd5f0ea1411/

Contacted Domains (8)

Domain	Detections	Created	Registrar
crt.sectigo.com	0 / 90	2018-08-16	CSC CORPORATE DOMAINS, INC.
fp2e7a.wpc.2be4.phicdn.net	0 / 90	2014-11-14	GoDaddy.com, LLC
fp2e7a.wpc.phicdn.net	0 / 90	2014-11-14	GoDaddy.com, LLC
microsoft.com	0 / 90	1991-05-02	MarkMonitor Inc.
query.prod.cms.rt.microsoft.com	0 / 90	1991-05-02	MarkMonitor Inc.
sectigo.com	0 / 90	2018-08-16	CSC CORPORATE DOMAINS, INC.
tse1.mm.bing.net	0 / 90	1997-09-03	MarkMonitor Inc.
www.microsoft.com	0 / 90	1991-05-02	MarkMonitor Inc.

IRL, IP address, domain, or file hash

Contacted IP addresses (27)

IP	Detections	Autonomous System	Country
104.18.14.101	0 / 90	13335	-
104.86.182.43	1 / 90	20940	US
104.86.182.8	1 / 90	20940	US
13.107.39.203	1 / 90	8068	US
13.107.4.50	8 / 90	8068	US
131.253.33.203	3 / 90	8068	US
172.16.1.2	0 / 90	-	-
184.25.191.235	0 / 90	16625	US
192.168.0.159	0 / 90	-	-
192.168.0.35	0 / 90	-	-



Execution Parents (21)

Scanned	Detections	Type	Name
2023-05-22	4 / 58	unknown	40MB.img
2022-10-22	34 / 72	Win32 EXE	a398385971fc8034c24551d08e9e189bWindows Wallpaper.exe
2023-04-17	29 / 56	ISO image	Malware Repo.iso
2023-06-29	25 / 56	ISO image	malware pack.iso
2023-01-10	52 / 66	ZIP	c6f67bf814bd8afee4085335266b3850.zip
2023-11-27	40 / 59	RAR	virus.rar
2022-08-16	50 / 71	Win32 EXE	don.exe
2023-12-16	30 / 55	ISO image	Malware Collection.iso
2023-03-04	44 / 70	Win32 EXE	yo.exe
2023-12-25	39 / 60	ZIP	Unconfirmed 985536.crdownload

DETECTION DETAILS RELATIONS **BEHAVIOR** COMMUNITY 28

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Display grouped sandbox reports

<input checked="" type="checkbox"/> C2AE	0 0 0 0 0 1 0	<input checked="" type="checkbox"/> CAPA	0 3 0 0 0 0 0
<input checked="" type="checkbox"/> CAPE Sandbox	0 5 0 0 0 6 5	<input checked="" type="checkbox"/> Lastline	2 0 0 0 0 0 0
<input checked="" type="checkbox"/> Microsoft Sysinternals	0 0 0 0 0 99+ 31	<input checked="" type="checkbox"/> Rising MOVES	0 0 0 0 0 0 0
<input checked="" type="checkbox"/> Sangfor ZSand	0 0 0 0 0 99+ 0	<input checked="" type="checkbox"/> VMRay	1 6 0 0 0 0 97
<input checked="" type="checkbox"/> VirusTotal Cuckoofork	0 0 0 0 0 0 1	<input checked="" type="checkbox"/> VirusTotal Jujubox	0 0 0 0 0 1 0
<input checked="" type="checkbox"/> Yomi Hunter	1 6 0 2 3 5	<input checked="" type="checkbox"/> Zenbox	3 10 0 0 99+ 3

Activity Summary

Download Artifacts Full Reports Help

3 Detections

3 MALWARE 3 RANSOM
1 EVADER

Mitre Signatures

4 HIGH 15 LOW 47 INFO

IDS Rules

NOT FOUND

Sigma Rules

1 MEDIUM 1 LOW

Dropped Files

723 OTHER 1 CAB 1 SCRIPT
1 PE_EXE 1 TEXT 1 LNK
1 ODT 1 DOS_COM 1 ZIP

Network comms

5 HTTP 5 DNS 34 IP

Behavior Tags

calls-wmi checks-cpu-name checks-user-input detect-debug-environment direct-cpu-clock-access long-sleeps persistence runtime-modules

Dynamic Analysis Sandbox Detections

- The sandbox Zenbox flags this file as: MALWARE RANSOM EVADER
- The sandbox VMRay flags this file as: RANSOM
- The sandbox Yomi Hunter flags this file as: MALWARE
- The sandbox Lastline flags this file as: MALWARE RANSOM

MITRE ATT&CK Tactics and Techniques

- + Execution TAO002
- + Persistence TAO003
- + Privilege Escalation TAO004

Activate Windows
Go to Settings to activate Windows

URL, IP address, domain, or file hash

Activity Summary

- + Execution TA0002
- + Persistence TA0003
- + Privilege Escalation TA0004
- + Defense Evasion TA0005
- + Credential Access TA0006
- + Discovery TA0007
- + Collection TA0009
- + Command and Control TA0011
- + Impact TA0034
- + Impact TA0040

Capabilities ⓘ

- + Host-Interaction
- + Data-Manipulation
- + Communication
- + Executable
- + Load-Code
- + Linking
- ▼






URL, IP address, domain, or file hash

Activity Summary






Download

Network Communication ⓘ





HTTP Requests

- +  http://172.16.1.2:5357/048da2fc-03cd-4f4f-9037-fcd5f0ea1411/
- +  http://crt.sectigo.com/SectigoPublicCodeSigningCAR36.crt
- +  http://crt.sectigo.com/SectigoPublicCodeSigningRootR46.p7c
- +  http://www.microsoft.com/pki/certs/MicCodSigPCA_08-31-2010.crt
- +  http://www.microsoft.com/pki/certs/MicrosoftTimeStampPCA.crt

DNS Resolutions

- +  crt.sectigo.com
- +  fp2e7a.wpc.2be4.phicdn.net
- +  fp2e7a.wpc.phicdn.net
- +  query.prod.cms.rt.microsoft.com
- +  tse1.mm.bing.net

IP Traffic

- +  104.86.182.43:443 (TCP)
- +  104.86.182.8:443 (TCP)
- +  13.107.39.203:80 (TCP)
- +  13.107.4.50:80 (TCP)

URL, IP address, domain, or file hash

Activity Summary

Download Artifacts ▾

Behavior Similarity Hashes ⓘ

C2AE	03ec53c6fd87b2e43af5925c1b15135f
CAPA	ed4e3e9abd82faacd76bd0d21daa4ae1
CAPE Sandbox	651a5df39e93c388c3cab03417c1d2a4
Lastline	cd82830d519ab10a4ddf68d8b5b3c2f4
Microsoft Sysinternals	336d4dabbcce3034e7cf9fc73b3071e3
Sangfor ZSand	2101ffd1cf4936c93653d5594f704003
VirusTotal Jujubox	7cc233780810e280613ea4e40573d7cb
VMRay	f4999fd0f7127442a3404f1422f9c136
Yomi Hunter	91ec1f51a8a4e992feb05c118a2dee7
Zenbox	68f5c5ac9fa67b048af8413898b8a526

File system actions ⓘ

Files Opened

- 📄 !Please Read Me!.txt
- 📄 !WannaDecryptor!.exe.Ink
- 📄 00000000.eky
- 📄 00000000.pky
- 📄 00000000.res
- 📄 100131493376744.bat
- 📄 231011590117708.bat
- 📁 C:\
- 📄 C:\!Please Read Me!.txt
- 📄 C:\!WannaDecryptor!.exe.Config

URL, IP address, domain, or file hash

Activity Summary

Dr









Process and service actions ⓘ

Processes Created

-  !WannaDecryptor!.exe
-  !WannaDecryptor!.exe v
-  !WannaDecryptor!.exe c
-  !WannaDecryptor!.exe f
-  "C:\Users\user\Desktop\61949ad6a077373a7d6cd85e3fae44315632f161adc4c99d5a8e6844.exe" /r
-  "C:\Users\user\Desktop\executable.exe" /r
-  "C:\Users\user\Desktop\file.exe" /r
-  "C:\Users\user\Desktop\software.exe" /r
-  %SAMPLEPATH%\!WannaDecryptor!.exe
-  %SAMPLEPATH%\!WannaCryptor v1.0.exe



Shell Commands

- 
-  !WannaDecryptor!.exe
-  !WannaDecryptor!.exe v
-  !WannaDecryptor!.exe c
-  !WannaDecryptor!.exe f
-  !WannaDecryptor!.exe v
-  "%SAMPLEPATH%\!WannaCryptor v1.0.exe"
-  "%SAMPLEPATH%\be22645c61949ad6a077373a7d6cd85e3fae44315632f161adc4c99d5a8e6844.exe"



virustotal.com/gui/file/be22645c61949ad6a077373a7d6cd85e3fae44315632f161adc4c99d5a8e6844/behavior

URL, IP address, domain, or file hash

Activity Summary

Processes Tree

- 1060 - C:\Windows\SysWOW64\cscript.exe
 - 1076 - 45e0edaca8702e6e90d1d98cf3647d5f.exe
 - 1132 - cscript //nologo c.vbs
 - 1136 - cde09bcd5f5fde1e2eac52c0f93362b79.exe
 - 1216 - 5b9f015e93669c54a087658dcaf0b3de.exe
 - 1236 - C:\Windows\SysWOW64\Wbem\WMIC.exe
 - 1308 - C:\Windows\SysWOW64\cmd.exe
 - 1356 - C:\Windows\SysWOW64\taskkill.exe
 - 1440 - C:\Windows\Explorer.EXE
 - 1444 - C:\Windows\SysWOW64\taskkill.exe taskkill /f /im sqlwriter.exe

Synchronization mechanisms & Signals ⓘ

Mutexes Created

- CDBurnNotify
- Global\C::Users\Louise\AppData\Local\Microsoft\Windows\Explorer:thumbcache_1024.dbldfMaintainer
- Global\C::Users\Louise\AppData\Local\Microsoft\Windows\Explorer:thumbcache_256.dbldfMaintainer
- Global\C::Users\Louise\AppData\Local\Microsoft\Windows\Explorer:thumbcache_32.dbldfMaintainer
- Global\C::Users\Louise\AppData\Local\Microsoft\Windows\Explorer:thumbcache_96.dbldfMaintainer
- Global\C::Users\Louise\AppData\Local\Microsoft\Windows\Explorer:thumbcache_idx.db\ThumbnailCacheInit
- Global\C::Users\Louise\AppData\Local\Microsoft\Windows\Explorer:thumbcache_idx.db\rwWriterMutex

CONCLUSION

WannaCry ransomware posed a significant threat to individuals and organizations worldwide, exploiting a critical vulnerability in Microsoft Windows Server Message Block (SMB) protocol. Its rapid propagation capabilities, robust encryption scheme, and extortion tactics underscored the evolving sophistication of cyberattacks.

Impact and Recommendations:

The WannaCry outbreak served as a stark reminder of the widespread susceptibility to cyberattacks and the importance of implementing robust cybersecurity measures. Here are some key recommendations:

- * **Regular System Patching:** Applying security updates promptly is crucial to address vulnerabilities exploited by malware.
- * **Network Segmentation:** Segmenting networks can limit the spread of malware by restricting lateral movement within the network.
- * **Strong Passwords and Multi-Factor Authentication:** Enforcing strong passwords and implementing multi-factor authentication can significantly hinder unauthorized access attempts.
- * **Data Backups:** Regularly backing up critical data allows for recovery in case of ransomware attacks or other data breaches.
- * **Cybersecurity Awareness Training:** Educating users about cyber threats and best practices can significantly reduce the risk of falling victim to social engineering attacks and phishing attempts.

By implementing these recommendations, organizations and individuals can significantly enhance their cybersecurity posture and mitigate the risks associated with sophisticated cyberattacks like WannaCry.

In conclusion, this Master's project report serves as a comprehensive exploration of malware analysis, encompassing its methodologies, techniques, tools, and significance in combating malicious software threats. By equipping cybersecurity professionals with the knowledge and skills necessary to analyze and mitigate malware, this report contributes to enhancing the resilience of systems and networks against evolving cyber threats.

