

Malware Analysis System

Submitted in partial fulfilment of the requirements of Edinburgh Napier University for the Degree of BEng (Hons) Computer Security and Forensics

KYAW HEIN-40501802
INFO MYANMAR UNIVERSITY
AUGUST 2022

Contents

Authorship Declaration.... 6

Data Protection Declaration.... 7

Acknowledge.... 8

Abstract.... 9

Chapter 1: Introduction.... 10

1.1Background.... 10

1.1.1Ransomware.... 12

1.1.2 Emotet Malware.... 13

1.2 Aims and objectives.... 14

1.3 Dissertation Structure.... 15

Chapter 2: Literature Review.... 16

2.1What is Malware?.... 16

2.2 Evolution of Malware.... 17

2.2Types of Malwares.... 19

2.2.1Virus.... 19

2.2.2Worms.... 20

2.2.3Trojan.... 21

2.2.4Spyware.... 22

2.2.7Adware.... 22

2.2.5Botnet.... 24

2.2.6Ransomware.... 24

2.2.8 Reveton.... 25

2.2.9 CryptoLocker.... 26

2.2.10Fileless Malware.... 27

2.2.11Backdoor.... 27

2.3Cyber Key chain.... 28

2.4Life Cycle of Malware Attack....29
2.4.1 Type of Analysis....30
2.4.2 Static analysis and Dynamic analysis....30
2.5: Approaches to Malware Analysis....32
Chapter 3: Environment Design....34
3.1 Methodology....34
3.2 Analysis Tools....35
3.3 Malware Analysis Design....35
Chapter 4: System Implementation....36
4.1 Malware Sample Selection....36
4.2 Analysis System Implementation....37
4.2.1 Hardware and Virtual Box configuration....37
4.2.2Host configuration....38
4.2.3Guest Configuration....38
Chapter 5: Evaluation....40
5.1 Initial Run – Medium Timeout set....40
5.2 Second Run – Long Timeout set....44
Chapter 6: Conclusion....48
6.1Overall Conclusion....48
6.2Limitation....49
6.3Future Work....49
Appendix 1 – Project Overview....50
Appendix 2 – Gantt chart....51
Appendix 3 – Project Diary....52
Appendix 4 – Project Diary....53
Appendix 5 – Project Diary....54
Appendix 6 – Project Diary....55

Reference.....56

List of Tables

TABLE 1: MALWARE SAMPLE FOR ANALYZING 36
TABLE 2: SPECIFICATION FOR ANALYSIS 37

List of Figures

Figure 1: REvil ransomware (CISA. (n.d) 2022) 12
Figure 2 : Virus (Fortinet,14 July 2022) 19
Figure 3: Botnet (Docs.microsoft.com. 2022) 20
Figure 4: Trojan (Bates, 1990) 21
Figure 5: Adware (BleepingComputer, 2022) 23
Figure 6 : Reveton (Saengphaibul, V. 2022) 25
Figure 7: CryptoLocker (Saengphaibul, V. 2022) 26
Figure 8: strategy of analysis (T. Mokoena, 2017) 31
Figure 9 : Scientific Experiment Methodology (Ali (2021, November 14)) 34
Figure 10: Malware Analysis Design 35
Figure 11: iptables configuration 38
Figure 12: Running Cuckoo web interface 39
Figure 13: Running Cuckoo 39
Figure 14: Adware (run 1) 40
Figure 15: Trojan (run 1) 41
Figure 16: Trojan (run 1) 41
Figure 17: Spyware (run 1) 42
Figure 18: Spyware (run 1) 42
Figure 19: Ransom (run 1) 43
Figure 20: Ransom (run 1) 43
Figure 21: Adware (run 2) 44
Figure 22: Trojan (run 2) 44
Figure 23: Behavior Analysis (run 2) 45
Figure 24: Process memory dump (run 2) 45
Figure 25: Ransom (run 2) 46
Figure 26: Ransom (run 2) 46
Figure 27: Gantt chart 51

Authorship Declaration

I, Kyaw Hein, confirm that this dissertation and the work presented in it are my own

Achievement.

Where I have consulted the published work of others this is always clearly attributed;

Where I have quoted from the work of others the source is always given. With the exception of such quotations this dissertation is entirely my own work;

I have acknowledged all main sources of help;

If my research follows on from previous work or is part of a larger collaborative research project, I have made clear exactly what was done by others and what I have contributed myself;

I have read and understand the penalties associated with Academic Misconduct.

I also confirm that I have obtained informed consent from all people I have involved in the work in this dissertation following the School's ethical guidelines

Signed: Kyaw Hein

Date:

Matriculation no: 40501802

Data Protection Declaration

Under the General Data Protection Regulation (GDPR) (EU) 2016/679, the University cannot disclose your grade to an unauthorized person. However, other students benefit from studying dissertations that have their grades attached.

Please sign your name below one of the options below to state your preference.

The University may make this dissertation, with indicative grade, available to others.

The University may make this dissertation available to others, but the grade may not be

disclosed.

The University may not make this dissertation available to others.

Acknowledge

I am Kyaw Hein, I would like to thank you my supervisor, Dr. Nyo Nyo Htwe. I has struggled and stressed to take the project throughout my formation, and finally, I finished the project with your help. Thank for all support and patience, I was able to push myself to apply the skills gained through my degree to produce this work.

I would like to thank Gordon Russell, thanks for the support and guidance provided to become my second marker and complete the project. Last but not least, I would like to thank my friends and parents for their support.

Abstract

Nowadays, Many malicious and Malware attacks are developing every single day, and many threats are increasing network security. They mainly target to the user's data or organization's data. There have two reasons, one is to steal data and the other is to destroy system. Technologies are invented to serve humankind, but there are always people who misuse them. We can say that the bad guys in the cyber world do this. Every time the developer develops new antivirus tools and techniques but at the same time, the hacker also develops new attacking ways.

The attackers are upgrade various type of attack such as Malware. Nothing happens when the users do not have security knowledge until the information system uses the best security protection. The main reason for this project is to try to explain the types of Malware and how they attack the data. Then it will explain the detection system and prevention system for information security. After that, the user will know the best way to detect and protect data from malware.

First of all, this dissertation is to approach the analysis and detection of Malware with the use of open sources tools and configure in the safety environment. Before the implementation, the dissertation paper present the characteristics and evolutions of Malware, in order to understand different types of Malware and their behavior. The purpose of the safety and secure environment is hosting analysis malware and detection systems. Moreover, it is also discussed about the cyber security, cyber-crime cases and how to protect the data by the law. The last but not least, in the analysis system is mainly use the Cuckoo Sandbox analysis tools. It is need the Linux host for Cuckoo Sandbox to be installed on and it is requirement for VirtualBox.

Chapter 1: Introduction

Although technologies are created to benefit humanity, there are always some who misuse technology. This is something that the bad people in the cyber world do. Cyber related crime cases are very dangerous and very popular at that time. During the COVID-19, everyone are working from home. Also you know they can face many issues because some of the data must be secret. If one of the employees attacked by someone, that will be effect on all of it. Nowadays, the hacker are upgrade various types of Malware. Nothing happens when the users do not have security knowledge until the information system uses the best security protection. So, the end users is really important to protect the data. The fact of this project will help the users and the organization by learning malware attack.

1.1Background

Currently, malware is largely made to target private or sensitive financial, business, or personal information, usually for financial benefit. Malware attacks are driven by money in 71% of cases. Identity theft, cyberwarfare, espionage, and service interruption with a focus on particular businesses are some further goals. Governments, businesses, or private individuals may all be the victims. The majority of businesses and people run the danger of having malware on their systems. According to a Microsoft research, malware may now be included in one out of every fourteen online downloads. The American people continued to file a record number of complaints with IC3 in 2021: 847,376 registered complaints, a 7% increase over 2020, with possible losses totaling more than $6.9 billion. Ransomware, business e-mail compromise (BEC) schemes, and the illegal usage of cryptocurrencies are some of the most often reported occurrences among the 2021 complaints. BEC scams generated 19,954 complaints in 2021, with an adjusted loss of close to $2.4 billion.

As a result of ITU (International Telecommunication Union), a billion of people were online and online harassment remains a persistent problem: in the United States of America in 2020, “41% of Americans have personally experienced some form of online harassment” and at least 1 in 10 women in the European Union have faced online harassment (*Global cybersecurity index 2022 - itu.int*.). In a survey of adults in 32 countries, one in five adults reported experiencing online hate speech. Globally, 100 countries have adopted legislation criminalizing instances of online harassment and abuse, 17 are in the process of drafting and implementing these measures and 77 have no legislation on the subject.

In 2018, as a result of the global cyber security index of the Asian region. Our country rank is 26 in Southeast Asian regional and Global runk is 128. As a result of cyber-related crime forensics cases in Myanmar (Myanmar. NCSI. (n.d.). Retrieved January 31, 2022).

- ✔ In 2013 – 2 cases
- ✔ In 2014 – 6 cases
- ✔ In 2015 – 53 cases
- ✔ In 2016 – 281 cases
- ✔ In 2017 – 553 cases
- ✔ In 2018 – 744 cases

Cybercrime cases are increasing every year. Most of them are Sexual Harass menu, Defamation, and phishing. As a result of the country's keys digital statistical indicator, 93% of people were using mobile devices. Among them, 26% of people are using online but most of them are lack security knowledge (Myanmar. NCSI. (n.d.). Retrieved January 31, 2022).

The government needs corporations with a private organizations. Therefore, some organizations or users are attacked by someone. At the time, they need some help from the government but they haven't a good corporation with a private organization. So, it is more difficult to explain it.

1.1.1Ransomware

The type of malware called Ransomware is made to encrypt files on a device, making any files and the systems that depend on them useless. Then, malicious actors demand a ransom in return for the decryption (CISA. (n.d) 2022). Ransomware behaves similarly like malware and spreads infection through similar channels. But unlike malware, which normally operates silently on a computer system, Ransomware alerts the victim only when its operations are complete. Threatening to sell or disclose stolen data or credentials if the ransom is not paid is a common tactic used by Ransomware practitioners (*Malwarebytes cybersecurity, 2022*). Ransomware has played a central role in news articles in recent months, but there have been years of impact on national, local governments and key infrastructure groups.

According to the cyber security firm and News, some of the most significant Ransomware attacks in 2020–21 were perpetrated by the REvil Ransomware group (CISA. (n.d) 2022) (*Malwarebytes cybersecurity, 2022*). REvil Ransomware hit the Kaseya cloud-based MSP platform that affects MSP and its customers. It is file blocking malware that encrypts files after infected and discard a ransom attack messages. It explain that victim's user or organization need to pay a ransom in Bitcoins and the demand will doubles when the victims don't paid in time.



Figure 1: REvil ransomware (CISA. (n.d) 2022)

1.1.2 Emotet Malware

Malware designed for Windows called Emotet originally surfaced in 2014 as a banking Trojan. Since then, Emotet has developed into modular malware that can now carry out a variety of tasks, such as stealing information, acting as a spambot, and loading more malware (*Malwarebytes cybersecurity, 2022*). The malicious emails that included it spread through malspam and typically pretended to be trade bills or bank transfer information in order to trick consumers into clicking on different links. Its first targets were primarily small German and Austrian banks and their respective clients (Duncan, B. (2022, May 12)).

It was primarily targeted at Deutsche Bank users and spread banking Trojans through Emotet. Mealybug used Trojan horses at the time. Mealybug began focusing on Swiss banking users in 2015 and developed Emotet into more specialized malware. The updated version of Emotet included distinct modules for its loader, malicious spam, distributed denial-of-service (DDoS) attacks, email login theft, and theft of financial data. The updated version of Emotet included separate modules for loaders, malicious spam, and distributed denial of service (DDoS) attacks, email login theft, and financial data theft.

Emotet is quick. The TCP ports and IP addresses used by its botnets for command and control (C2) communications are frequently updated. Furthermore, Emotet frequently changes the URLs that host the infection, often using hundreds of different URLs each day. Malicious attachments or links to malicious files can be found in emails disseminating Emotet. Microsoft Office items like Word documents or Excel spreadsheets are most frequently included in these mails. Malicious macro code is present in these Office documents. When a victim allows macros, the code is intended to infect a Windows host that is weak to infection.

As of January 27, 2021, the Emotet botnet's infrastructure has been destroyed, essentially stopping the malware's spread. In order to take control of the dead computer servers used by the cybercrime group, law enforcement agencies from across Europe including those from Germany, Ukraine, France, Lithuania, the Netherlands, and the United Kingdom worked together with American authorities.

1.2 Aims and objectives

This project's main goal is to thoroughly analyze the research on different Malwares iterations and families in order to determine the optimal strategy and build, implement, and test an analysis system. In order to build intrusion prevention datasets, the analysis system will be a stand-alone secure environment where Malwares samples can be submitted for study. The project aims to understand Malware and the defense ways. It will mainly discuss the different types of malware and their behavior. Then it will help to learn what malware is, how it works, how it infects the computer system, and how to protect it.

It's mainly targeted to daily internet users and organizations. As far as I know, our country is a developing country and the people have just started trying to use the latest technology and the internet. Most of the people haven’t general security knowledge. Therefore, there have many criminal cases in my country because of a lack of knowledge on surfing internet safety and weak procedural law. That is why the project aims to increase security knowledge and to avoid crime cases.

1.3 Dissertation Structure

Chapter 1: including introduction, Aims and objective and problem statement.

Chapter 2: Analysis of malware and this chapter will show the life cycle of Malware attack. Then it is explained how hacker distribute and infect data. Then it will explain about the business modules.

Chapter 3: It begins by extending the literature review to talk about the platforms and approaches that are most appropriate for design. Based on the findings of literature reviews and the outcomes of experiments, the design of the analysis and detection system environment is described below.

Chapter 4: implement the Analysis environment and their configuration. Then it is show the testing result. Describe the step by step detection and preventing ways. Implement and testing it.

Chapter 5: gives a report on the implementation of the analysis techniques in understanding Malware.

Chapter 6: summarize the main things of the project and their conclusion. Then it's discussed the future work.

Chapter 2: Literature Review

Introduction

In order to have a better overview of the project, this chapter provides a literature analysis of the background knowledge on malware and the security challenges related to it that is necessary. In order to comprehend historical trends in cybercrime and forecasts for the future, the first section will evaluate research on the evolution of malware overall.

2.1What is Malware?

Malware is a biggest and dangerous threat to the internet and technology users. It is malicious software that was created to damage computers, mobile, servers, and networks by distributing without permission. If the system is very vulnerable, it checks for weaknesses and infects the system after it has gained access. Cybercriminals generally use it to extract data that they can use to gain financial advantage over their victims. Financial information, healthcare records, personal emails, and passwords are just some of the types of information that can be hacked. Generally, Malware can classified two generations as first and second generations (D. Deka, N. Sarma and N. J. Panicker). The author explain the different classification of Malware and different types of second generation malware such as Encrypted Malware, Oligomorphic Malware Polymorphic Malware and Metamorphic Malware.

Malware refers to various sorts of malicious software, including viruses, and it is used by cybercriminals for a variety of objectives. Such as-

- Persuading a victim to provide personal information in order to commit identity theft.
- Stealing credit card or other financial information from consumers
- Taking control of a large number of computers in order to perform denial-of-service attacks against other networks
- Infecting computers and mining bit coin or other crypto currency with them

At a time when the globe is becoming more technologically adept, the number of malware attacks is also increasing, and this trend is continuing. Malware developers are constantly working to improve malware programs in order to avoid malware detection and analysis tools.

2.2 Evolution of Malware

Every day during our lives, we make use of technology. However, technologies were created to benefit humanity, and there are always others who misuse them. There is something that the bad people in the cyber world do. One of the few universally understood technical terminology is "computer virus," which even young children can understand. Everyone immediately associates that term with something unpleasant (*ic3, 2022*). It frequently refers to something harmful to the technology we all use, such as a laptop, smartphone, app, or gaming system, illustrating how pervasive computers and technology are in our daily lives. Computer viruses multiply and can spread from one host to another, just like their biological counterparts, causing issues that can range from bothersome to downright destructive.

The most widely accepted definition of malware is simply "undesirable software," with Elk Cloner, who infected the Apple II system via a floppy disk in 1982. (Fortinet, 14 July 2022)Although not necessarily damaging to the computer, it constituted an intrusion and met the definition of malware that most people would accept. Malware increased dramatically between 2000 and 2010, both in terms of quantity and the speed at which infections spread. Internet and email worms made international news at the start of the new century. We have once more seen a considerable development in the sophistication of malware between 2010 and the present. (Love, P. by J., & Love, J. (2019, September 19)) With vast, well-funded development teams, organized crime and state sponsors significantly increased the ante. These criminal workgroups are still active today, creating sophisticated software that employs evasion strategies to defeat various anti-virus programs.

These days we frequently hear about the malware attacks, and some of these attacks affect millions of users throughout the world. Malware has already existed in the early day of computing, but it was rarely a source of concern for end-users. Malware attacks mostly targeted the banking, government, finance, and accounting industries in the early days. Every year, new technologies are developed in the modern world. Many organizations and users are uses different technologies devices such as laptops, desktops, phones, tablets, HDD, and Sticks. They always kept the critical information on their own devices and in the cloud. As a result, data has become the most valuable resource in our daily lives, and it has become the major target of malware.

The Malware ecosystem has changed significantly over time. It was appeared that everything about money and it is only target to the organization and government system. (Engin Kirda, and Christopher Kruegel. 2012) But now, it is also target to the end users data. Cybercrime case are very dangerous and very popular at that time. This project aims to increase security knowledge and to avoid cybercrime cases. (D. Deka, N. Sarma and N. J. Panicker) there are two reasons to do cybercrime, one is steal the data and the other is destroy data. There has a lot of case happen in Myanmar and around the globe (Mohanta A., Saldanha A. (2020)).

They are-

- ✔ Steal the data for money
- ✔ Steal the personal data for decreasing dignity.
- ✔ Human Trafficking
- ✔ Export money from women by threating its sexual.
- ✔ Pornographic photos sharing on social media.
- ✔ Fraud
- ✔ Theft
- ✔ Inquest and Homicide
- ✔ Drugs and Murder
- ✔ Website and Email

There are frequently happen cybercrime case around the globe. Defamation case is mostly happened case in Myanmar. Today, many malicious software and techniques are developed by an attacker. At the same time, many anti-malware techniques are also developed by software developers. But it is not everything and it doesn't enough to explain the cybercrime case. If the user does not have security knowledge, nothing happens until the user uses the best security techniques and devices. Nowadays, many anti-virus software and devices are out there, but they doesn't enough to protect from malware. Because every time the developer develop the new technologies and then hacker are also use the same technologies to protect their malware and to prevent from malware analysis and making it harder to develop effective malware signature.

2.2Types of Malwares

All threats, including viruses, worms, botnets, Ransomware, and other malicious software-related threats are collectively referred to as malw0061re.

- ✔ Virus
- ✔ Worm
- ✔ Trojan
- ✔ Spyware
- ✔ Botnet
- ✔ Adware
- ✔ Ransomware
- ✔ Reveton
- ✔ CryptoLocker
- ✔ Fileless Malware
- ✔ backdoor

2.2.1Virus

Early day of computing, virus is the first of product of malware. A virus is typically delivered by an email attachment that contains the virus payload, or the element of the malware that executes the dangerous operation. The device is infected once the victim opens the file. Viruses live by infecting and inserting themselves into other files on the system that are otherwise healthy. These infected healthy software run, execute and provide the expected functionality when run, but they can also run the virus in the background (D. Deka, N. Sarma and N. J. Panicker). Without human intervention, whether through clicking a link, opening an attachment, running a program, or downloading a file, a virus cannot propagate.

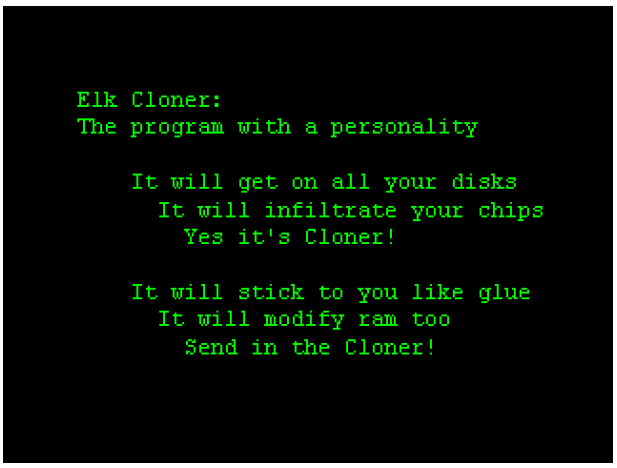


Figure 2 : Virus (Fortinet,14 July 2022)

2.2.2Worms

Worms are Malware and they can infect themselves from computer to machine through the internet or physical devices (eg. USB, HDD) by exploiting a security vulnerability in software or an OS (Mohanta A., Saldanha A. (2020)). A worm can duplicate on its own, burrow deeply into systems, and migrate across devices without the assistance of a human. According to the research of security firm, the first worm in history was created by Robert Morris, this worm has no bad intentions. It was developed as a Proof of Concept to test the viability of hands-free reproduction.

The worm introduced a number of firsts. It carried out modern malware activities, such as searching for existing infections and exploiting holes in various programs and services. Morris coded the worm for persistence because he was concerned that system administrators would quarantine it and disregard the infestation. The self-replication process, however, could not be stopped, which resulted in huge loads on devices that rendered them unusable and a denial-of-service (DoS) in networks as it propagated from machine to machine.

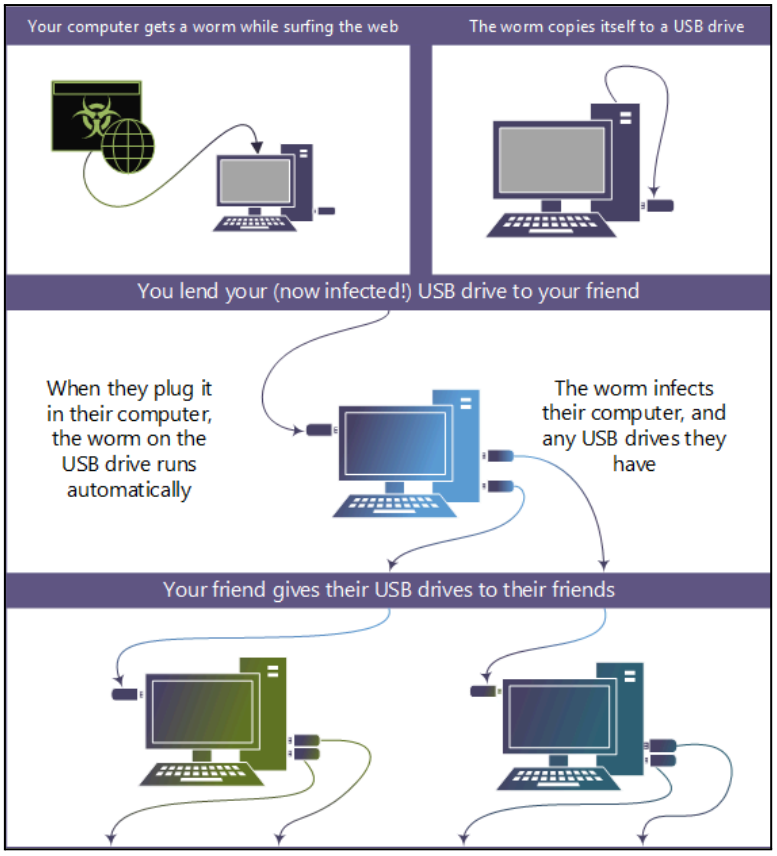


Figure 3: Botnet (Docs.microsoft.com. 2022)

2.2.3Trojan

Trojan is Malware that act as benign applications to deceive users into downloading and installing them. It is installed with the user's knowledge, but the user is unaware of the infection's true dangerous intents. The name of the Trojan is coming from an old story of Greek. When a Trojan horse is executed, malware is installed despite its disguise as useful software. Although the virus is installed and executing, the Trojan horse may occasionally be tried to capitalize on beneficial applications, which makes it much more difficult to detect. Additionally, not the original creator of the malware must use the exploitation. Some hackers search networks for anomalies that someone else may have left behind in order to gain access to a remote machine.

The AIDS Trojan made its debut in 1989, making it the first known Ransomware. Coincidentally, a United States-based ISP called The World made internet connection publicly available for the first time in 1989 (Bates,1990). But it wasn't until 2005 that Ransomware started using internet connectivity to find its victims and infect them. Another

famous Trojan virus debuted in the 1990s as a straightforward Whack-A-Mole game. A version of NetBus, a program that enables remote control of a Microsoft Windows computer system through a network, was concealed by the program. With remote access, the attacker might unlock a computer's CD tray among many other things.

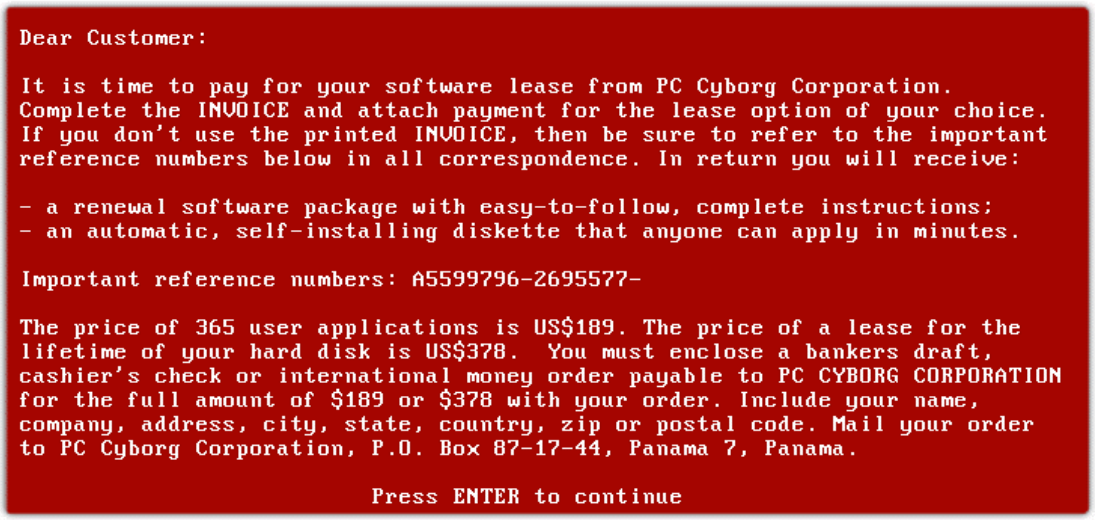


Figure 4: Trojan (Bates, 1990)

2.2.4Spyware

Spyware is a program that is spies on victim computer without permission and steal personal information from victim computer. Spyware allows its users to keep track on all communications on the target device. Usernames, passwords, photos, and documents are all examples of data that malware can target. By the early 2000s, cybersecurity firms were using the term "spyware" in a manner similar to how we may use it today, for example, as a phrase for some type of undesirable software application created to spy on your computer activity.

The first anti-spyware program was made available in June 2000. A study was conducted in October 2004 by America Online and the National Cyber-Security Alliance. In each computer, there are approximately 93 percent of spyware components, and 89 percent of computer users are ignorant that they are there (*ic3, 2022*). This means that approximately 80 percent of all Internet users have spyware on their system. Nearly all, or 95% of the impacted parties, admitted that they never gave authorization to install them.

Due to its widespread use, spyware programs are now the preferred target for Windows operating systems. However, in recent years, Apple's platforms and mobile devices have also attracted the attention of spyware makers.

2.2.7Adware

Adware is a type of Malware. Adware is software that allows your computer to display unwanted advertisements when you download software from a third-party website. Adware is installed behind the scenes while installing the downloaded software.

Adware is just free software that shows ads and gathers data. Most of the time, we download adware on purpose. When you accept the conditions of a service that grants you access to run free applications in return for receiving adverts, this occurs. Other times, malware automatically installs itself on your computer or phone without your permission and may carry out dangerous actions in addition to displaying adverts (BleepingComputer,2022). 29 fraudulent apps with over 10 million downloads were removed from the Google Play Store on October 1st, 2019. Of those, 24 were said to contain hidden malware, while the remaining five were adware.

The goal of hidden applications is to show user full-screen advertisements even if the apps were not in use (Gorrie, M, 2022). These hidden apps are mostly found in photography categories, hide their icon after the user initially launches them in order to prevent getting uninstalled easily and they instead create a shortcut on the home screen. Initially, there is no way to close these ads and the app also takes a longer time to display the close ad button (BleepingComputer, 2022). These are continuous and even if you close one and another pops up. They utilize heavy data usage and drain the battery of smartphones. Advertisements are the gateway to enter into the user’s phone for the Adware.

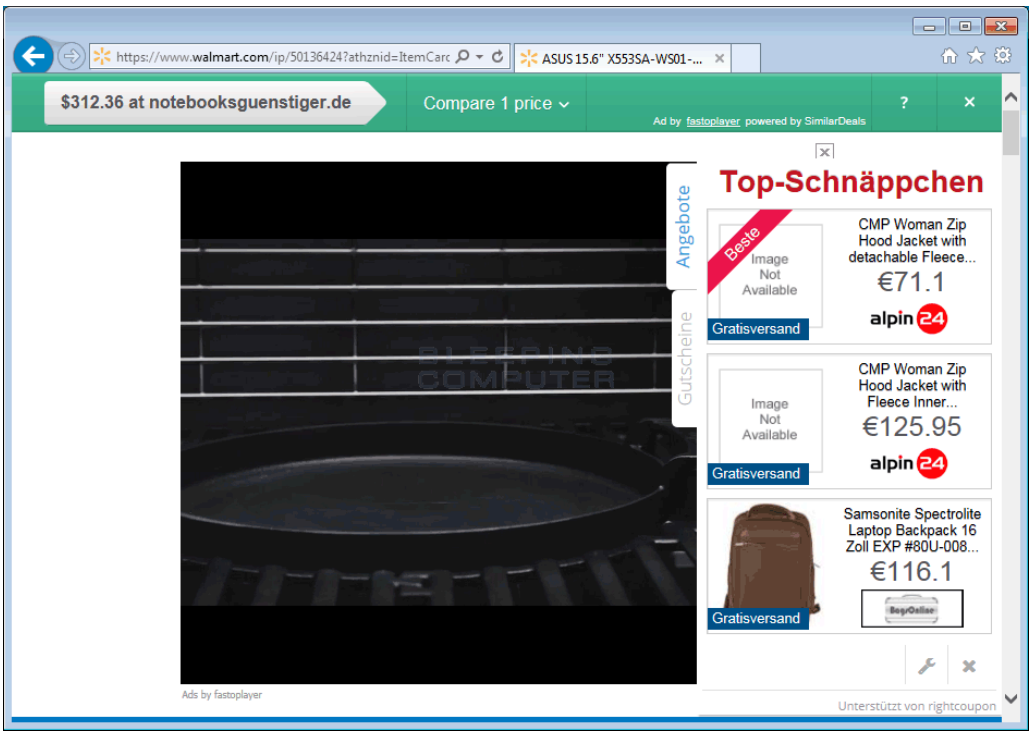


Figure 5: Adware (BleepingComputer, 2022)

2.2.5Botnet

Botnet is a bot network that have been spread with the malicious software propagate by a Botmasters through the under control of the malware owner (Mohanta A., Saldanha A. (2020)). The main purpose of Botnet is for the controlling criminal for financial or impostor to use bots for fraudulent internet activity. Botnet can be used for the various activities like DDoS attack, malicious software (Spyware, Trojan horse, etc.)

A group of infected computers that are under the direction and control of an operator is known as a botnet. Botnets were easy to use back then. The majority of the botnet malware

connected to an Internet Relay Chat command and control server to obtain instructions before infecting and spreading to other devices.

The EarthLink Spam botnet, which originally appeared in 2000, was the first one to be noticed. Its simple mission was to send out a ton of spam. At the time, the EarthLink Botnet was responsible for 25% of all email spam, or over 1.25 billion messages (Avast Blog, 2022). The GTbot was introduced in 1999, making it the true original botnet. It was fairly simplistic in terms of malware. In effect, it spread to other computers and took commands over IRC. GTbot controllers exploited this network of harmed devices to carry out these orders and perform distributed denial-of-service (DDoS) attacks.

2.2.6Ransomware

Ransomware works by encrypting data, files, and other system resources on the victim's computer and demanding a Ransom in exchange for their decryption. Ransomware is difficult to deal with because once data is encrypted, it creates significant losses for users and needs a significant amount of effort to repair the damage and recover the system to its previous state.

It can be immediately stopped and asked to pay for access to your system or data. Services are seriously affected by Ransomware. The WannaCry Ransomware attack, which infected hundreds of thousands of computers globally in May 2017 using older Windows system flaws, was the most well-known malware attack. Most famously, the malware destroyed the English National Health Services' computer systems, creating a medical emergency. This attack completely destroyed the majority of systems throughout the world. Attacks of this nature are increasing in frequency, thus we must be ready to defend against them.

The Ransomware program consists of DiskCryptor, an open source disk encryption software wrapped in a program that installs and initiates disk encryption in the background using a key chosen by an attacker (CISA.2022). The attacker uses a command-line option to deliver the encryption key. The malware installs an encryption service and extracts a number of files. About one or more minutes after the installation of DiskCryptor, the Ransomware program restarts the computer to finish installing the drivers. The encryption key and shutdown time variables are stored in the configuration file and can be read after about one or

more hours until the second reboot (CISA.2022). After rebooting, the encryption will be completed and the ransom note will be displayed.

2.2.8 Reveton

Malware known as "Reveton" Ransomware, which first appeared in 2012, sent communications to its victims purporting to be US police enforcement and accusing them of watching unlawful pornography (Saengphaibul, V. 2022). In certain instances, it turned on the user's camera to give the impression that they had been videotaped. Additionally, it requested payment from the victim in order to avoid legal action. Reveton also received a lot of media attention since it appeared to be controlled by a skilled group of cybercriminals. It not only looked professional, but it also made use of templates, which was a first.



Figure 6 : Reveton (Saengphaibul, V. 2022)

2.2.9 CryptoLocker

The first Ransomware to request payment using Bitcoin was CryptoLocker. The CryptoLocker Ransomware's introduction to victims in 2013 marked the beginning of the next significant evolution. Public-key encryption and bitcoin Ransomware payments were merged in CryptoLocker (Saengphaibul, V. 2022). Before the introduction of CryptoLocker, Ransomware payments were made using e-wallets, prepaid debit cards, money transfers, gift cards, and other means that were challenging for threat actors to profit on a large scale. The invention of Bitcoin in 2009 made quick, fictitious-anonymous payments possible. Before the

Federal Bureau of Investigation (FBI) dismantled the gang's operations in 2016, CryptoLocker's operators were able to take an estimated $27 million thanks to a mix of bitcoin ransom demands and robust encryption.



Figure 7: CryptoLocker (Saengphaibul, V. 2022)

2.2.10Fileless Malware

Fileless Malware doesn’t require malicious file to infect system. The activation of tools, software, and apps that are already incorporated into your operating system is more sophisticated with Fileless malware. After then, the malware hides on your system. In 2017, fileless malware became a common form of attack, but many of these attack techniques had been present for some time.

Fileless threats are a type of low-observable characteristics attacks, a class of stealth attack that is difficult to detect by most security programs and has an influence on forensic investigation efforts. Although not a virus, fileless malware behaves similarly to viruses in that it runs in memory. Fileless infections go directly into memory without being stored in a file or loaded on the computer, and the dangerous content never ever touches the hard disk. Microsoft Windows PowerShell is a legal and practical technology used by administrators for task automation and configuration management, but many LOC attacks make use of it. PowerShell gives enemies access to practically everything and anything in Windows using a command-line shell and related scripting language.

2.2.11Backdoor

A backdoor is an untrusted entry point through which an attacker can get access to the victim's computer system. Malware, for example, can open a network port on the system with shell access, which the attacker can use to obtain access to the system.

After gaining access to the system, the attacker will frequently install a backdoor to facilitate future attacks. With this access, the attacker can steal data and information from the business. The malicious behavior will only be activated under the chosen input keys in this form of attack, and the application and basic tests will stay unaltered to prevent discovery. Even if you are aware that your system has been breached, you might not be aware that it also has a backdoor. If it does, you must lock it up right away to prevent chaos.

According to a research released by Kaspersky on January 16, 2020, a new phishing tactic that tempts the victim to install or renew website security certificates is being used to spread new backdoor and Trojan malware variants. The warning states that the website's security certificate is out-of-date and advises installing a security certificate update to continue.

2.3Cyber Key chain

The Cyber Kill Chain is a Lockheed Martin model that describes the many stages of an APT attack carried out by an attacker outside the target organization. It identifies all of the steps that attackers must take in order to complete their mission, which could include data exfiltration or spying. If security professionals can identify and block any of the intermediary processes, they can compromise the entire attack operation. Seven steps of cyber kill chain are-

Reconnaissance – this is the first steps of cyber kill chain. The attackers will start with identifying the vulnerable target and gathering information from numerous sources. This step give some information like server IP and some detail information, software information use in Organization and then possible vulnerable information. Then this process may include gathering personal information from company employees in order to identify possible social engineering targets.

Weaponization – Based on the vulnerable information gathered during the reconnaissance phase, the attacker created a weapon (malware).

Delivery – this step is delivering the weaponized to victims devices into the target. It is trunsmit by spam mail, USB, web, etc.

Exploiting – this step is to deliver the malicious code to the victim's system and execute it. After that, the attacker can gain access to the victim's system by installing tools and executing the exploit.

Installation malware – This step is to install malware on the asset that provides access to the attacker. The malware that was installed was designed to stay hidden and undetected in the target network for a longer period.

Command and control – The establishment of communication between the victim system and the attacker is known as command-and-control (Mohanta A., Saldanha A. (2020)). The attacker gains access to the network and systems of the company. The malware is now prepared to accept commands from the attacker.

Action on objectives – Finally, the attacker gains privileged access to take control and execute the system and extracts the data from the system. The objective includes spying, encrypting data from the victim's computer.

2.4Life Cycle of Malware Attack

Attackers are always trying to take control of the user's computer by making the following steps.

Development

Every malware attack starts with the development state. Developers are creating new technologies to protect malware but at the same time, malware developers used the same way to upgrade their malware and protect it from the anti-malware system.

Distribution strategies

After the development state, malware developer distribute their malware to the target users. There have many distribution ways. Such as –

1. Phishing email and malicious attachment
2. Drive by downloads from compromise website
3. USB and other removal devices
4. Online Advertisement and other social engineering techniques

Infection methods

Malware developers are always gathering the target user's information and their system weakness. After collect the data, attacker make a plan to infect the system. There have several infection methods. They are –

Social Engineering and user mistake

Malware authors frequently use deception to get users to download malicious files. Then the authors use the removal devices for distribution. So, some of the infection are come from the user mistakes by using the malicious removal devices or file download.

Operating system vulnerabilities and software flaws

Most malware are created to take advantage of weaknesses in the most popular operating systems on the market, as this allows them to infect millions of machines running a vulnerable program at the same time. Many malware try to spread and infect all computers with the same characteristics by attacking security flaws, or design defects in systems or application software.

2.4.1 Type of Analysis

Analysis is the best things to know about the malware and their behavior. Malware analysis is major important things of cyber security. Because the analysis ways will show, how it behaves and how they infect and distribute? There has the two basically analysis ways. There are Static Analysis and Dynamic Analysis.

2.4.2 Static analysis and Dynamic analysis

Static analysis is the one of the analysis ways, it is analysis the malware without executing it. They analysis with the two ways. First of all, it is using the anti-virus tools to identify malware. The anti-virus tools and anti-virus website are very useful to analysis the malware signature automatically (Manuel Egele, Theodoor Scholte, et. 2012). Second of all, static analysis is use the hashes, file strings, functions and headers information to analysis the malware without executing such as Virus Tools, Filealyzer. At One research paper, there has two static analysis, such as Basic static analysis and advanced static analysis. Basic static analysis is an analysis without running malware binaries and advanced static analysis needs it. (D. Deka, N. Sarma and N. J. Panicker)

Strings, API names, assembly code, and numerous irregularities in the files are examined during static analysis. user need to learn reverse engineering, It is described as the method of obtaining data from malware while it is not actively executing by examining the malware's source code to ascertain its true purpose. Examining disassembly listings, extracting extracted strings, obtaining virus signatures, figuring out the target's architecture and the compiler that was used, as well as many other aspects of malware, are all examples of information extraction from malware. During this phase, the malware program or artifact is not run, necessitating the use of specialized tools to execute an in-depth analysis of the malware.

Dynamic analysis is the opposite of static analysis because it is analysis malware by executing it. Executing is means using the safety environment to analyze malware. In

Dynamic analysis paper, the author mainly explain the different between the manual dynamic analysis and automated dynamic analysis. In one research paper, dynamic malware analysis isn't very accurate because it has some limit and it cannot be analyze due to the network restriction (Babak Sadeghiyan, and David Baptiste. 2019). The author said that the control environment is not beneficial due to the complex nature of malware (M. Ijaz, M. H. Durad and M. Ismail). The malware analyzer can find the detail information of malware in the safety environment. The safety environment is mainly work to run the malicious software without infection the host. There have the two ways to create the safety environment. First, it is using the virtualization such as VMware and virtual box. Second, it is use the cloud environment for testing malware. There have a lot of tools are used in dynamic analysis –

- Wireshark
- INetSim
- Sandboxes
- OSSEC
- Splunk
- Snort
- Pfsense

In contrast to the static analysis technique, which only provides a summary of the malware being analyzed, this procedure involves running the malware artifact in a safe, isolated environment (T. Mokoena and T. Zuva,). As information about the malware is obtained while the virus is executing, dynamic analysis offers an extensive view of the infection's genuine aim, characteristics, and operation. Since malware unpacks itself during runtime dynamic malware analysis avoids the limitations of static analysis, which include unpacking and obfuscation issues. The figure below show the method in (T. Mokoena et al. 2017). This strategic of analysis is very realistic for the enterprise system.

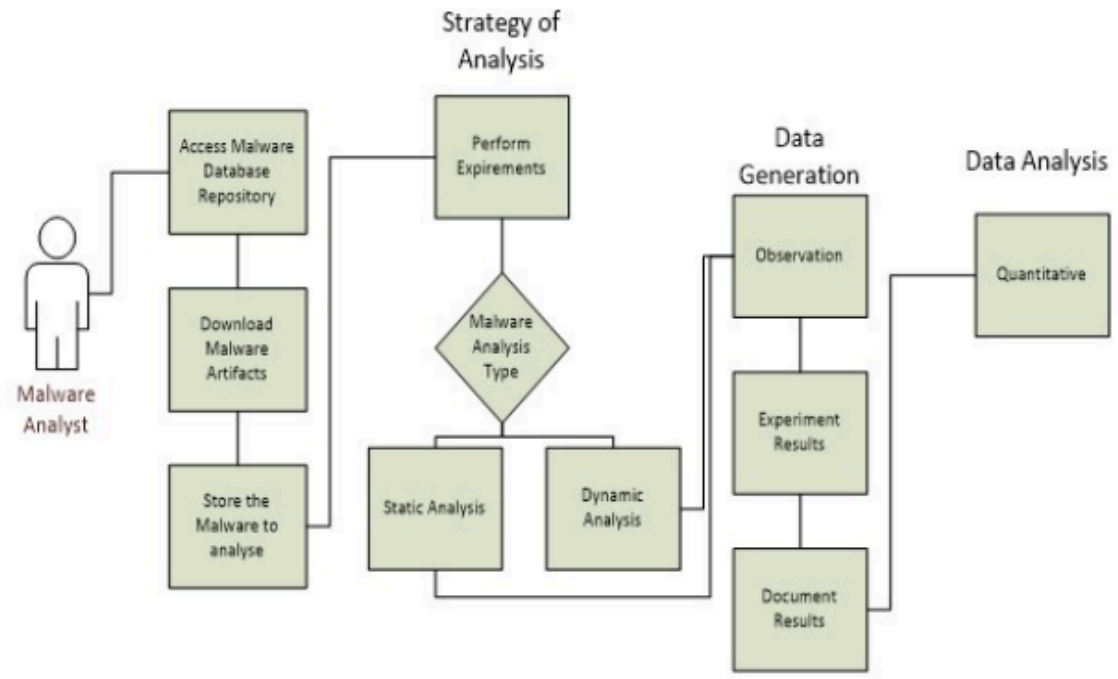


Figure 8: strategy of analysis (T. Mokoena, 2017)

2.5: Approaches to Malware Analysis

If the analyst or researcher needs to examine the behavior of the malicious file that has been executed, use dynamic analysis. If the organization or analyst lacks the necessary skills to analyze the malicious file's source code. If an analyst or organization must address or respond to a security breach or malware attack incident, they must be able to identify the malware infection in order to apply corrective measures. (S. Jamalpur, Y. S. Navya, P. Raja, G. Tagore and G. R. K. Rao)

In 2018, the result paper of International Conference on Inventive Communication and Computational Technologies, It is advised to set up a specialized environment that is isolated from other computers and network resources that will not be taken into account throughout the course of the investigation before beginning any virus analysis. For any analyst, having a specialized environment for malware analysis is essential. Careful planning will be necessary to determine what is necessary from a technological and ethical standpoint. There have a two options to analysis the system. They are using hardware or virtual machine platform.

Physical setups make it possible to examine malware behavior on compromised hosts in the real world. The ability of malware to look different on virtual machines, such as shutting down or executing different behavioral patterns to avoid examination, is another

advantage of real devices. The disadvantages of physical designs include the added cost of obtaining the necessary resources, as well as configuration and maintenance. Backup techniques are necessary since malware in physical settings can be more impossible to prevent.

Analysts VM configurations, particularly for dynamic analysis, which is described in a later section. This decision is easily justified by a few key characteristics, one physical machines can configure and manage numerous virtual machines, and snapshots make it simple to roll back to earlier, even clean configurations. The VM environment enables interconnection of machines running different OS while keeping them cut off from a production network. It has been noticed that some recent viruses that can detect virtual machines may also be able to exploit the host computer through the VM software. This capability can be avoided by following appropriate security update and repair procedures.

Conclusion

In literature review, it is mainly discuss the history of Malware has been established, enabling a better comprehension of the development of such attacks, the predicted behavior, and the ways to be taken into consideration for analysis. In a recent paper, the paper discuss about the classification of malware (D. Deka, N. Sarma and N. J. Panicker). In the area of computer security, malware analysis has been a highly difficult research thing to solve. Understanding the context and threat level of the malware intrusion incident is the result of the malware analysis. The primary goal of malware analysis is to gather details on every compromised system's infected file, the virus's internal operations, and its behavior.

Chapter 3: Environment Design

3.1 Methodology

This project is use the scientific Experiment Methodology. As online resources, the scientific method is an experimentation technique that is used to investigate observations and find answers to problems (Ali. (2021, November 14)). To complete the project, it is need to use the scientific method systematically. In figure 2.2, there have four steps. First, its need to identify the types of Malware. Second step is formulate the Hypothesis. In this step, its implement the safety environment design for testing Malware. The final step is analyze the testing result, this step is show the result of testing and complete the project.

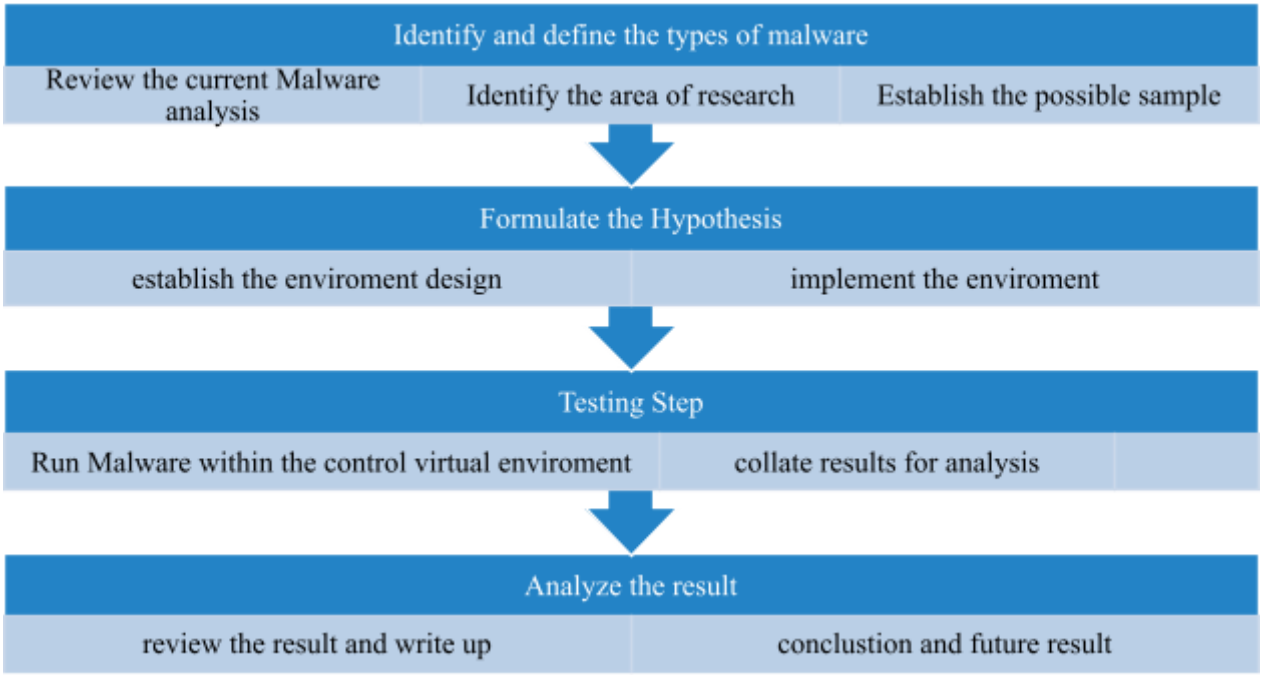


Figure 9 : Scientific Experiment Methodology (Ali (2021, November 14))

3.2 Analysis Tools

In the cyber security networking, Hackers and malicious online criminals utilize malware as a guaranteed tool when attacking businesses and organizations. Unfortunately, virus analysis takes a while in today's cyber security environment. To understand the scope and depth of persistent malware analysts and security experts may spend several months trying to comprehend a single piece of malware. These difficulties highlight the necessity of employing Cuckoo Sandbox to automate malware investigation. Cuckoo was used in the virtual network environment and it analyzing the different malicious files under Linux. Its works by configuring a virtual sandbox environment inside Virtual Box, inserting and running the suspicious file of your choice, and then reporting the behavior of the file.

3.3 Malware Analysis Design

The Cuckoo sandbox is mainly use in this design. In design, it is require VirtualBox to implement the system. Kali Linux/ Ubuntu is will be the host OS. Then Linux OS will be install Cuckoo sandbox for analyzing malware.

Sandboxing technology to detect the malicious code and determining their behavior by using cuckoo sandbox (P. Raja, G. Tagore and G. R. K. Rao, 2018). Basically, there have three types of sandboxes, such as Virtualization-based sandboxes, Emulation-based sandboxes and Bare-Metal sandboxes. There have many open source sandboxes are out there such as, Cuckoo, Malwr, Joesandbox and Threatexpert.

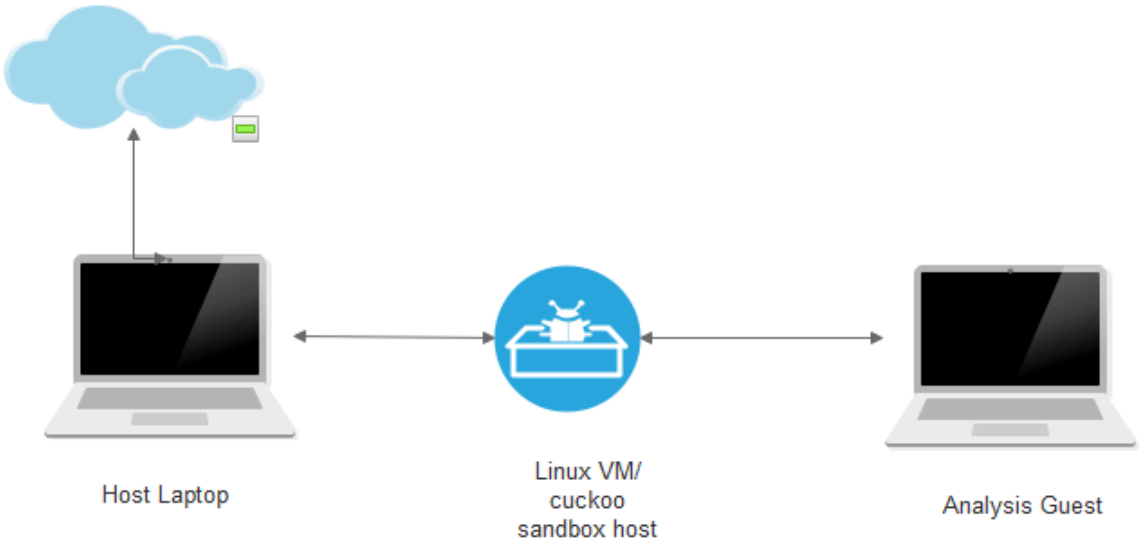


Figure 10: Malware Analysis Design

Chapter 4: System Implementation

Introduction

A method for analyzing and detecting malware in a secure environment was established in the previous chapter. This chapter's purpose is to show how the suggested environments for the analysis and detection systems were put into practice. To do this, the chapter is divided into multiple section. The first section looking the sample and selection Malware to implement of the system. The second section, is the configuration of the specified tools, like it was described in the chapter before. At final section, the chapter concludes with a review of the implementation, problems, and if the design was generally effective and capable of carrying out the experiments as defined in Chapter 3.

4.1 Malware Sample Selection

In the implementation, some files are needed In order to give the Malware samples enough time to be analyzed. Now, this step is the collection of Malware sample for analyzing. There have four samples of malware are running in the cuckoo sandbox analysis environment. Samples are taken from multiple a reliable source of information online (Malware Traffic Analysis; VirusShare, Virtustotal, Cuckoo). The following table is show the types of Malware, the SHA56 Value of each obtained and their publish date.

Malware	SHA56	Publish Date
Adware	37ea273266aa2d28430194fca27849170d609d338abc9c6c43c4e6be1bcf51f9	2016-9-8
Trojan	e7def648f10c23a32125e7d663327c87b092f2aeb71c87af19a6c4c03828e7d8	2017-10-14
Spyware	dc030778938b8b6f98236a709d0d18734c325accf44b12a55ecc2d56b8bb9000	2016-10-17
W32/Ransom Trojan	da386efced7535a1262ae9ede6988e27bdc6fca3411da14e6db02158aa37a5c9	2017-5-9

Table 1: Malware Sample for analyzing

4.2 Analysis System Implementation

4.2.1 Hardware and Virtual Box configuration

The analysis environment is set up on the VirtualBox and is hosted on the Ubuntu host OS. The Ubuntu host OS that served the physical host was connected throughout the implementation, thus the host OS received the physical host's CPU, RAM, and installed NIC. Installed on the virtual machine, the guest operating systems' networks are set up as host-only network interfaces that divide the physical network of the cuckoo host from the virtual network. The cuckoo agent serves as a conduit for communication between the cuckoo guest and cuckoo host.

Specification	Host OS	VirtualBox Guest OS
OS	Ubuntu 22.04	Windows 8 Enterprise
CPU	Intel Core i3-7100U CPU2.40GHz	
Hard Disk	1TB	Virtual size: 80 GB
RAM	12 GB	2 GB
Network	192.168.56.1 (Gateway)	192.168.56.101 (Host-only adapter)
Software	VirtualBox	Python, Microsoft Office

Table 2: Specification for analysis

It is necessary to have an appropriate version of Python and their setup tools installed because the Cuckoo host components are entirely written in Python. This standard is used to configure iptables on the Ubuntu host to enable network connectivity for the guest machine. The physical arrangement used a specialized Wi-Fi network that was separate from any other devices and networks in order for connecting to happen in a secure.

Analysis Tools Configuration

4.2.2Host configuration

Running Malware samples required installing and configuring Cuckoo Sandbox on the Ubuntu host OS. So, the host OS need to install python and their setup tools. According to the Cuckoo configuration instructions, Mongodb and PostgreSQL are necessary to use the Django-based web interface and PostgreSQL database, and then a VirtualBox interface with the IP address 192.168.56.1 also needed to be set up on the host. After that, Host machines need to install tcpdump to record network activity that occurs while the malware is being executed.

After installation cuckoo, it will use iptables to set network forwarding rules .The following step is configure IP forwarding. So, internet connection can gets routed from the host machine to the guest Virtual Machine.

```
kyawhein@kyawhein-X541UVK:~$ sudo iptables -t nat -A POSTROUTING -o eth0 -s 192.168.56.0/24 -j MASQUERADE
[sudo] password for kyawhein:
kyawhein@kyawhein-X541UVK:~$ sudo iptables -P FORWARD DROP
kyawhein@kyawhein-X541UVK:~$ sudo iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
kyawhein@kyawhein-X541UVK:~$ sudo iptables -A FORWARD -s 192.168.56.0/24 -j ACCEPT
kyawhein@kyawhein-X541UVK:~$ sudo iptables -A FORWARD -s 192.168.56.0/24 -d 192.168.56.0/24 -j ACCEPT
kyawhein@kyawhein-X541UVK:~$ sudo iptables -A FORWARD -j LOG
kyawhein@kyawhein-X541UVK:~$
```

Figure 11: iptables configuration

4.2.3Guest Configuration

For the Cuckoo guest component to function effectively, Python is a necessary requirement. It is also need to configure the network interface assigned with the same subnet. A Python script called Cuckoo's agent is set up to run every time the guest OS boots up. It is also need to install python pillow. Because pillow is utilized to take screenshots of the Windows desktop during the analysis. The guest machines must have to disable Windows Firewall and Automatic Updates on the Guest is an additional step to take as their traffic and processes can "damage the environment" the network analysis.

To do analysis, the configuration files must be set. The machine name and IP address are added to the virtualbox.conf file to make sure that cuckoo will recognize and launch the appropriate VM. The memory.conf and cuckoo.conf files are modified in this implementation to enable Volatility to analyze memory dumps in order to track the malware. After configuration, cuckoo can start run on the host machines and analyze using sample files on the cuckoo sandbox web interface.

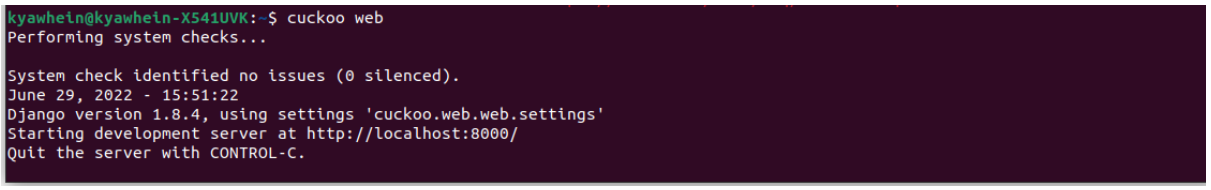


Figure 12: Running Cuckoo web interface

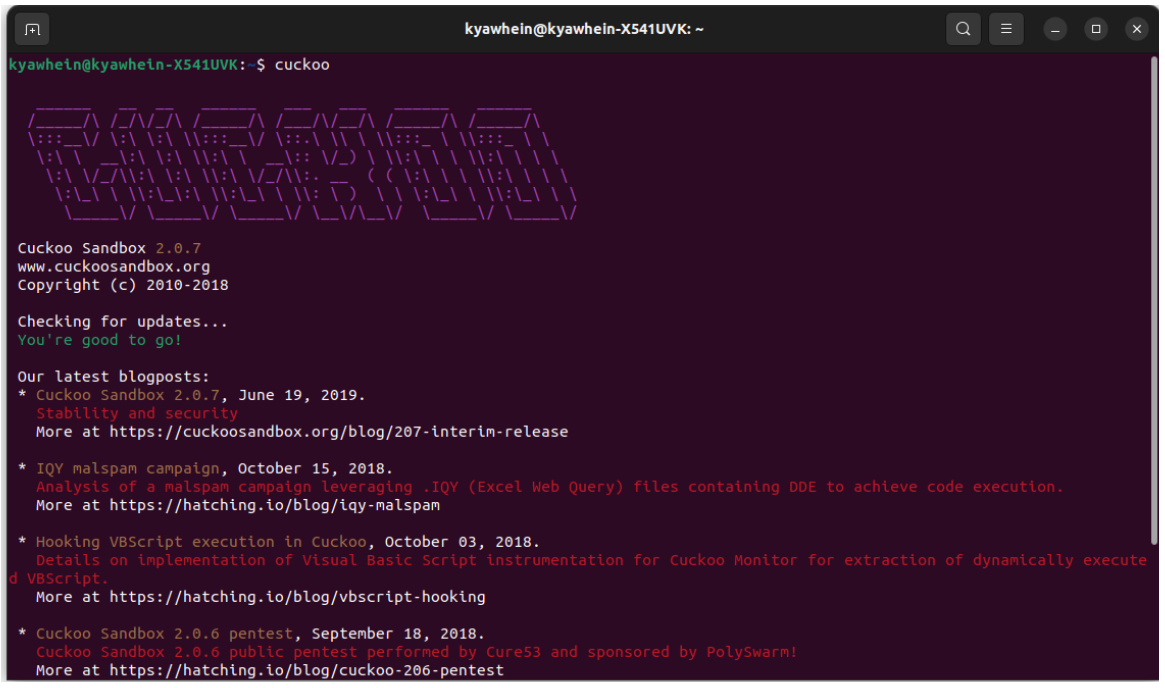


Figure 13: Running Cuckoo

Chapter 5: Evaluation

Introduction

Results from the test carried out will be given and thoroughly discussed in this chapter. It's important to know that the results of the analysis system were necessary for implementing and evaluating the detection system in the previous chapter. According to the previous chapter's description, the four Malware samples will be used to analyze each system. Each sample was run twice through the analysis system, each time with a different timeout setting, providing additional results for comparison. The detection system's performance can be evaluated based on the configuration options implemented and informed by the analysis's results.

5.1 Initial Run – Medium Timeout set

The first experiment run of each sample allows for automatic timeouts for files inserted in Cuckoo. It gives an overview of some of the research results from the research. Figure 5.1 is provide a summary of some of the findings obtained from conducting the experiments. It has only one memory dumps files with the malicious URL. In addition, it's successfully create a file under the C: partition. The analysis process is only take 166 seconds long.

Adware (SHA56) - 37ea273266aa2d28430194fca27849170d609d338abc9c6c43c4e6be1bcf51f9

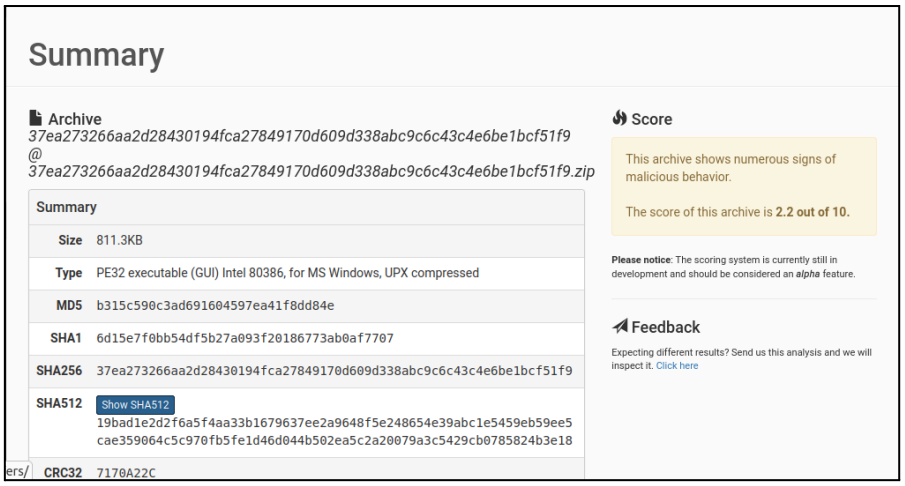


Figure 14: Adware (run 1)

This step is analyzing the Trojan Malware. It can see the summary of the analysis for windows. The score of the analysis is 5.2 out of 10 that is mean malicious state. This process is happen in 228 seconds.

Trojan (SHA56) - **e7def648f10c23a32125e7d663327c87b092f2aeb71c87af19a6c4c03828e7d8**

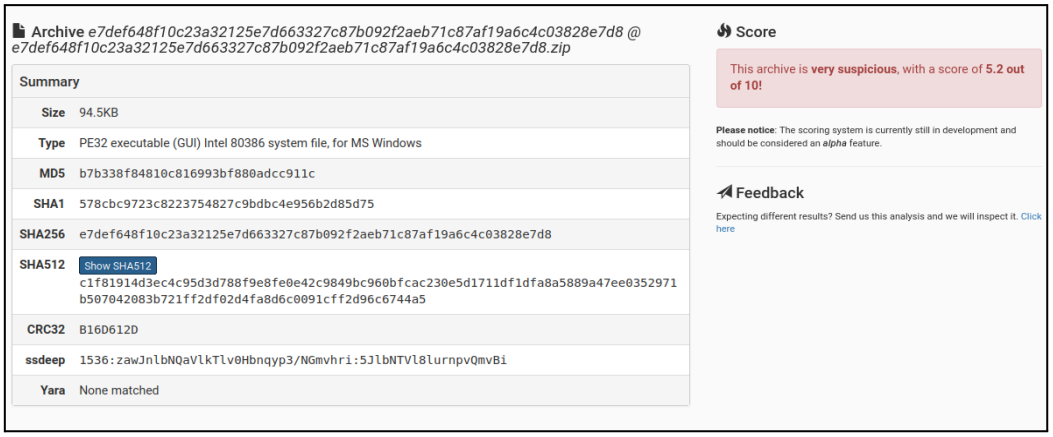


Figure 15: Trojan (run 1)

As a result of cuckoo, Malware install itself unexpected files in the windows. Then it show file name try to remove evidence of files from internet. Moreover, it's created a windows hook that monitors keyboard input. Then the status is show one of the file are open and it's dropped buffer in the windows.

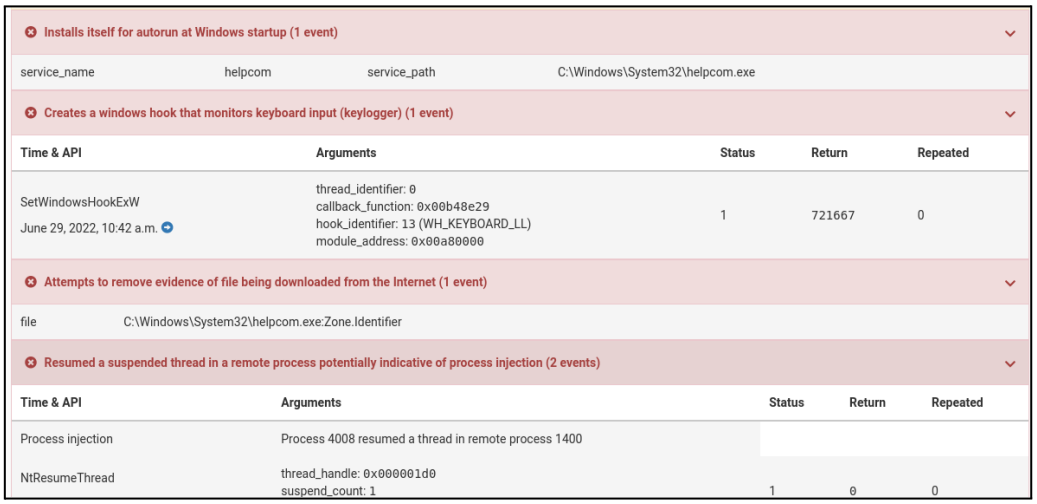


Figure 16: Trojan (run 1)

This step is the analysis of spyware in the cuckoo sandbox. The result is show the malicious status that is steal personal information from guest machine local internet browser. Its collect credentials from the local ftp client application. In this process, there have 50 out of 62 events at the first run. Moreover, its show the result of the collection of data about installed application.

Spyware (SHA56) - dc030778938b8b6f98236a709d0d18734c325accf44b12a55ecc2d56b8bb9000

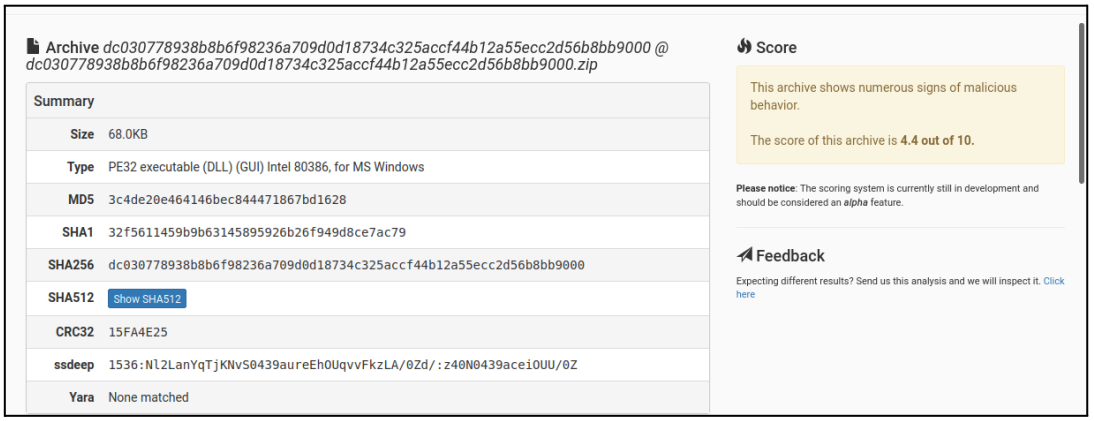


Figure 17: Spyware (run 1)

The following picture is show the behavior analysis. Its show their API values, Argument and show the process status and the return values. Although the results of the network, file, and system analyses seem to be lacking, processes were started and XML data was found in the Strings analysis, demonstrating that it does not require administrative permissions to execute.

Time & API	Arguments	Status	Return	Repeated
SetUnhandledExceptionFilter June 28, 2022, 12:58 a.m.			0	0
SetErrorMode June 28, 2022, 12:58 a.m.	mode: 32769 (SEM_FAILCRITICALERRORS|SEM_NOOPENFILEERRORBOX)	1	32775	0
GetFileAttributesW June 28, 2022, 12:58 a.m.	file_attributes: 4294967295 filepath_r: C:\Users\kyawhein\AppData\Local\Temp\dc030778938b8b6f98236a709d0d18734c325accf44b12a55ecc2d56b8bb9000.dll.manifest filepath: C:\Users\kyawhein\AppData\Local\Temp\dc030778938b8b6f98236a709d0d18734c325accf44b12a55ecc2d56b8bb9000.dll.manifest		4294967295	0

Figure 18: Spyware (run 1)

As a result of analysis, win32 Ransom malware exit at the very suspicious state. It is only run in the 190 seconds. The result is display the process memory dump found URL related to Tor. It found the Ransom message that is written on the disk.

Ransom (SHA56) da386efced7535a1262ae9ede6988e27bdc6fca3411da14e6db02158aa37a5c9

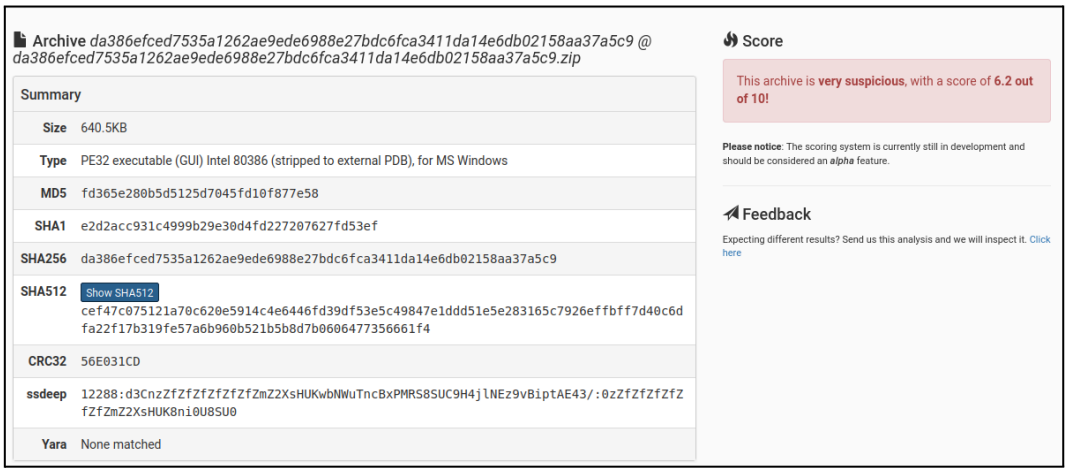


Figure 19: Ransom (run 1)

As a result, Malicious is dropped 333 files in the victim Windows. Then we can see the location of the dropped files and its size.

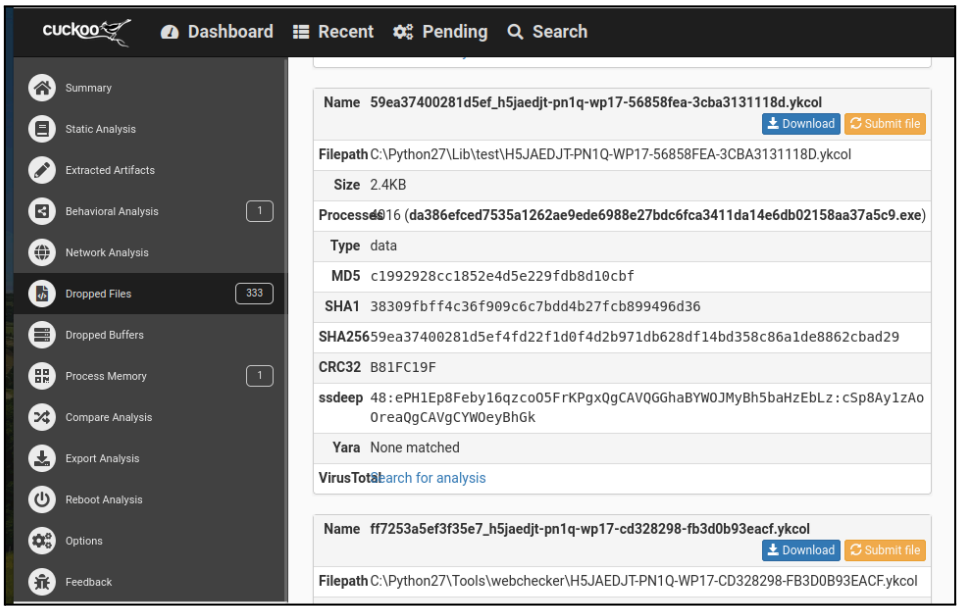


Figure 20: Ransom (run 1)

5.2 Second Run – Long Timeout set

As the report did not generate, it had to be assumed to be similar to Run 1. At the second run with the long timeout set, it has slightly different from the first test. After the second test, there have two memory dump process. 8 events URL malicious were found in the process memory dump. The analysis process is take 173 seconds.

Adware (SHA56) - 37ea273266aa2d28430194fca27849170d609d338abc9c6c43c4e6be1bcf51f9

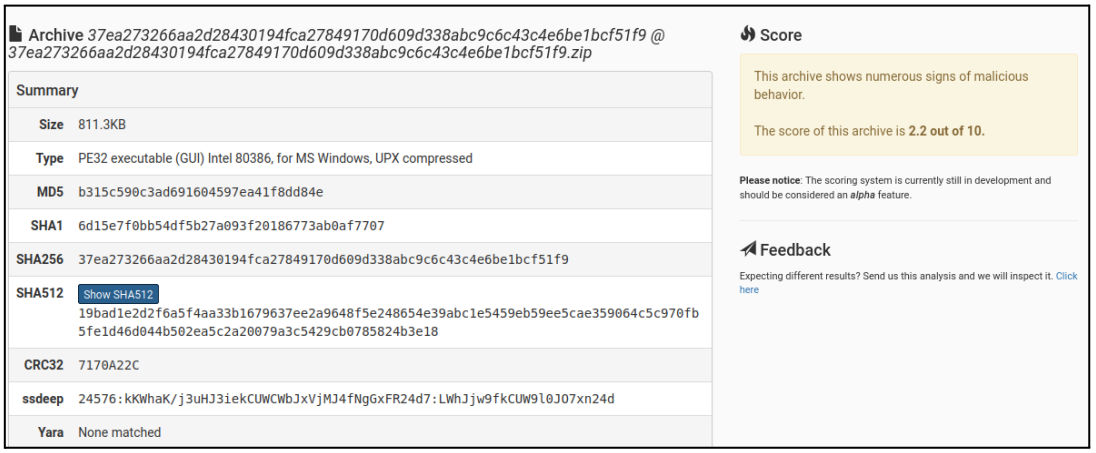


Figure 21: Adware (run 2)

This process is take 393 seconds. Its take longer time to analyze the second run. So the return values of the keylogger is more than the first run.

Trojan (SHA56) - **e7def648f10c23a32125e7d663327c87b092f2aeb71c87af19a6c4c03828e7d8**

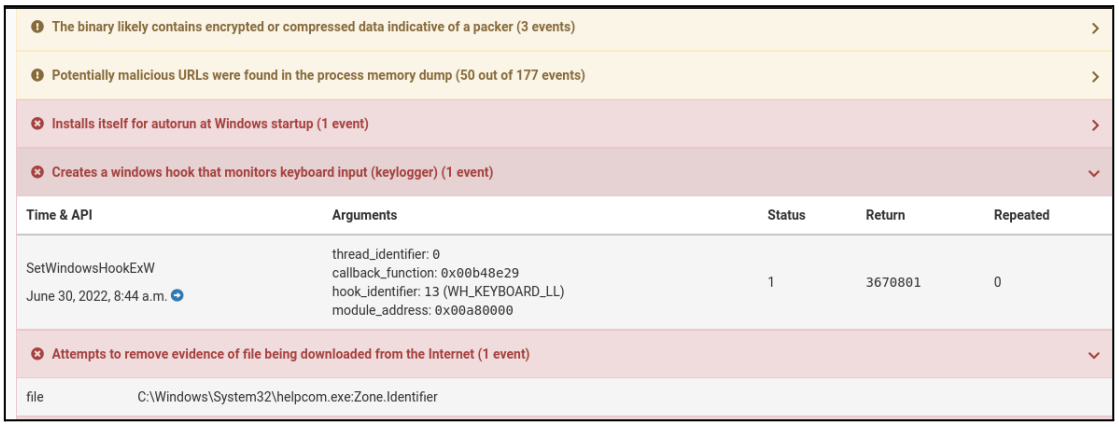


Figure 22: Trojan (run 2)

This second run is happen in 360 seconds. The process (50 out of 183 events) were found related with malicious URL. It provide greatly increased the amount of information available about the behavior when executing on a victim's computer. It found the volume of Directories, Registries, and Files accessed during both tests when the encryption process took control of the system.

Spyware (SHA56) - dc030778938b8b6f98236a709d0d18734c325accf44b12a55ecc2d56b8bb9000

Time & API	Arguments	Status	Return	Repeated
GetFileAttributesW June 28, 2022, 12:58 a.m.	file_attributes: 4294967295 filepath_r: C:\Users\kyawhein\AppData\Local\Temp\dc030778938b8b6f98236a709d0d18734c325accf44b12a55ecc2d56b8bb9000.dll.manifest filepath: C:\Users\kyawhein\AppData\Local\Temp\dc030778938b8b6f98236a709d0d18734c325accf44b12a55ecc2d56b8bb9000.dll.manifest		4294967295	0

Figure 23: Behavior Analysis (run 2)

Process memory dump for **rundll32.exe** (PID 316, dump 1)

Extracted/injected images (may contain unpacked executables)
Download #1

URLs found in process memory

```
http://users.ocsp.d-trust.net03
http://crl.ssc.lt/root-b/cacrl.crl0
http://crlmain01.ipsca.com/crl/main01.crl06
http://fedir.comsign.co.il/crl/ComSignAdvancedSecurityCA.crl0
https://crl.anf.es/AC/ANFServerCA.crl0
http://crl.securetrust.com/STCA.crl0
http://crl.securetrust.com/SGCA.crl0
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0?
http://www.ibsensoftware.com/
http://www.ssc.lt/cps03
http://www.microsoft.com/pki/certs/MicrosoftRootCert.crt0
http://www.informatik.admin.ch/PKI/links/CPS_2_16_756_1_17_3_1_0.pdf0
http://www.certificadodigital.com.br/repositorio/serasaca/crl/SerasaCAII.crl0
http://ocsp.suscerte.gob.ve0
http://ac.economia.gob.mx/last.crl0G
http://crl.startcom.org/sfsca-crl.crl0
http://www.digsigtrust.com/DST_TRUST_CPS_v990701.html0
https://iecvlist.microsoft.com/ie10/201206/iecompatviewlist.xml
http://ca.mtin.es/mtin/DPCyPoliticas0
http://crl.comodo.net/AAACertificateServices.crl0
http://ns.adobe.com/xap/1.0/mm/
http://www.pkioverheid.nl/policies/root-policy0
http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz0
http://www.ecee.gov.pt/dpc0
http://www.e-szigno.hu/SZSZ/0
http://www.microsoft.com/pki/certs/MicRooCerAut_2010_06_23.crt07
```

Figure 24: Process memory dump (run 2)

As a result of analysis, it take long 399 seconds. Therefore, its remove the mime type of the 1262 file, which is a sign that Ransomware is writing the encrypted file back to disk. When viewing behaviour and dropped files, its generated more process within the extended simulation times. Additionally, its provide the screenshots that it was the proces of Ransom attack.

Ransom (SHA56) da386efced7535a1262ae9ede6988e27bdc6fca3411da14e6db02158aa37a5c9

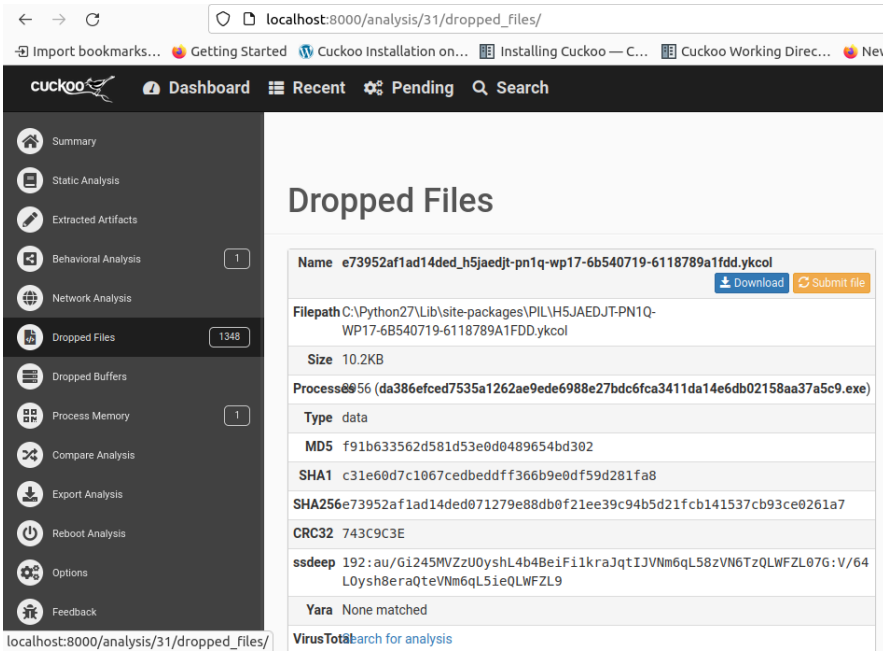


Figure 25: Ransom (run 2)

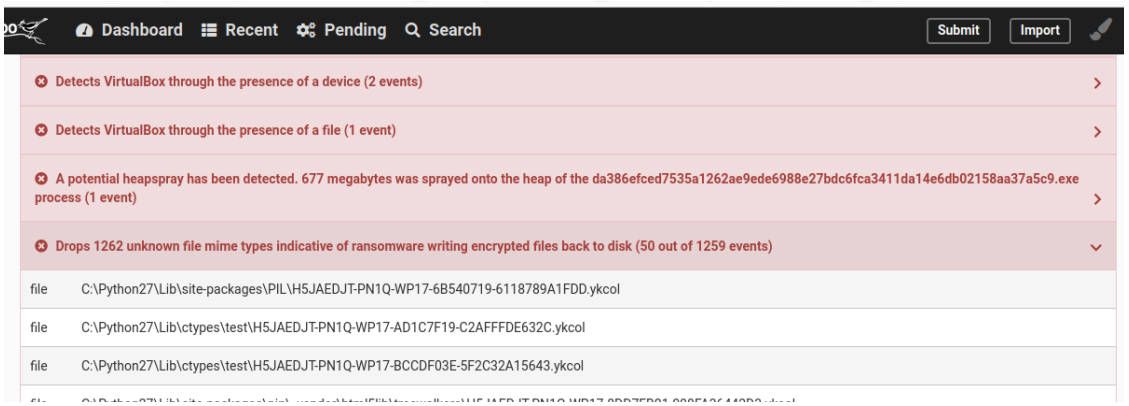


Figure 26: Ransom (run 2)

Chapter 6: Conclusion

6.1Overall Conclusion

The reason for this project is to develop the best understanding of malware analysis and possible methods of analysis and detection by using open sources security tools. Malware are very trend and popular in the cybersecurity environment. In the previous chapter 2, it's provided to understand what malware is and how types of malware are developed year by year and how cybercriminals have continuously improved to keep one step ahead of security professionals.

Moreover, chapter 3 is discussed the methodology to create the project and explain the design for malware analysis. The rest of this chapter 4 and 5, it finishes up the overall project. It begins by examining the Introduction's Aims and Objectives and analyzing whether they were accomplished. Each objective's findings will be evaluated critically, and any difficulties that were encountered will be discussed. Finally, the project end with suggestions for future research.

Due to the increasing frequency of cyber-attacks, the analysis of malware samples is time consuming and costly. It require total malware protection when working with malware for analysis. The automated behavior analysis using the cuckoo sandbox offers a customizable option for malware analysis. It produces a comprehensive report based on a series of tests it performed while the malicious code sample was being executed.

Malware closely relates to the need for a specialized malware analysis environment, which is discussed. Additionally, the methods of static and dynamic analysis were given and debated. The chapter is mainly discuss about trend of malware and it was taken into consideration for analysis when comparing the work finished with the Initial Project Overview (Appendix 1). Different types of malware are closely relates to the need for a specialized analysis environment, which is discussed.

When attempting to do analysis on live malware samples, there are numerous obstacles to be aware of. Before doing tests, there are ethical and security considerations to considers, just like with malware research. For this reason, it was necessary to discuss the right design and implementation of a controlled environment. Finally, the study done for the literature review and the methods presented in Chapter 3 gave a thorough understanding that helped effectively build and deploy two systems specifically made for Malware analysis.

6.2Limitation

This project is also has some limitation, Cuckoo Sandbox was selected as the primary analysis system after considering the requirement for a secure environment to execute analysis. Additional security measures, such as operating the system entirely from a virtual machines (virtualbox), were created and put into place. Moreover, it was presented samples of malware for malware analyzing. It provides the legitimacy of the choices and experimental methods to be adopted. While choosing the right samples was a difficult process, several malware samples were identified by sandbox such as VirusTotal, Cuckoo.

So, it only has to analyze all available feature and system support by cuckoo sandbox. The advantages of this project is not need the extra devices for analyzing and it is only need a one devices (such as Laptop, Desktop, etc) for analysis by setting sandbox tools with the suitable requirements.

6.3Future Work

The malware developers are currently always one step ahead of computer security experts by applying new strategies to hide dangerous malware. As a result, the approaches and tools for analyzing malware that are now available are insufficient or ineffective, which presents a tough problem for anti-malware solutions in the field of computer and network security. According to this study, the deployment of more effective and complex autonomous countermeasures is required to reduce the rate of malware attacks. The development of autonomous approaches to somewhat reduce malware issues is made possible by current advancements in malware analysis tools, machine learning, and data mining techniques.

Later, I want to make further research for my system. I'll learn and research different tools and techniques for the analysis. And I want to create different powerful news tools by integrated with machine learning and AI.

Appendix 1 – Project Overview

Initial Project Overview

SOC10101 Honours Project (40 Credits)

Title of Project: Supervised vs. Unsupervised Machine Learning in Cyber Attack Detection

Overview of Project Content and Milestones

The goal of this project is to determine whether supervised or unsupervised machine learning (ML) is more effective in an intrusion detection system (IDS). To do this I will need to research current uses of supervised and unsupervised machine learning in intrusion detection. Three possible datasets have been selected, two of which are from University of New Brunswick called CSE-CIC-IDS2018 on AWS and CICIDS2017. The third is called UNSW-NB15 created by the Australian Centre for Cyber Security. The dataset will be tested in different algorithms which all handle the data in different ways: Artificial Neural Networks, Random Forest, Support Vector Mechanism, Density Based, Linear Regression, and Apriori. To understand how well the algorithms work, there will be a series of metrics used to allow for comparison between the algorithms, these will be: accuracy, precision vs. recall, F1 score, confusion matrix, and area under curve. Some of the metrics work with binary classification while others work with multi-class classification which will allow me to progress the project from a binary to multi-class classification intrusion detection system. To help maintain a plan a Gantt chart will be produced which will also give a timeline and the goals set out by the project.

The Main Deliverable(s):

The main deliverable of the project is to produce a study which compares how effective different ML algorithms are in terms of intrusion detection and evaluating whether supervised or unsupervised provides the best result. This could be used to facilitate future research in this area or as a potential basis for a new IDS.

The Target Audience for the Deliverable(s):

The goal is for this project to help the research being undertaken into using machine learning as a method of intrusion detection. The main target audience for this project is for future academic work or for companies looking at how they can make use of ML in their IDS.

The Work to be Undertaken:

The initial work to be undertaken is research and an investigation into what papers are available in this sector. This will help me find gaps in research that I could fill. A detailed plan will be produced explain what needs to be done and how it will be done with a timeline to help illustrate this. I will need to create the training data that will then be processed through the different machine learning models to find which is most effective at intrusion detection.

[Cyber Security and Forensics] 07/07/2020 1

Additional Information / Knowledge Required:

Machine Learning is a fairly new topic for me and is not covered in my course so I shall gain new knowledge and skills throughout the project. I will need to understand the foundations of machine learning as well as how it can be used in cyber-attack detection.

I will be working in Matlab to implement the ML. I have previously worked with Matlab so feel confident in using this software and I will be able to expand on my skills with this software.

Information Sources that Provide a Context for the Project:

Da Costa, K., Papa, J., Lisboa, C., Munoz, R., & De Albuquerque, V. (2019). Internet of Things: A survey on machine learning-based intrusion detection approaches. *Computer Networks, 151*, 147-157.

Song, J., Takakura, H., Okabe, Y., & Nakao, K. (2013). Toward a more practical unsupervised anomaly detection system. *Information Sciences, 231*, 4-14.

Aamir, M., & Zaidi, S. (2019). DDoS attack detection with feature engineering and machine learning: The framework and performance evaluation. *International Journal of Information Security, 18*(6), 761-785.

Ghanchi, J. (2019). The Possibilities of AI and Machine Learning for Cyber Security. Retrieved 11th September 2019.

Brown, M. (2017). An Innovative Approach to Insider Threat Detection Using Data Mining and Machine Learning.

The Importance of the Project:

Machine Learning and AI technology is already prevalent in the modern world and so are cyber-attacks. With the growing number of attacks also comes more advanced and sophisticated attacks making more difficult for humans to monitor it. With the help that machine learning could provide this could make detection of attacks more successful and potentially lower the number of attacks that take place.

The Key Challenge(s) to be Overcome:

- Due to this being a new topic for me there will be a few challenges, but planning will help minimise the disruption of this.
- Will need to spend time making sure the test data is sufficient to teach the ML models.
- I will also need to identify a dataset that is suitable, e.g. not biased or too old, for testing the ML models.

Appendix 2 – Gantt chart

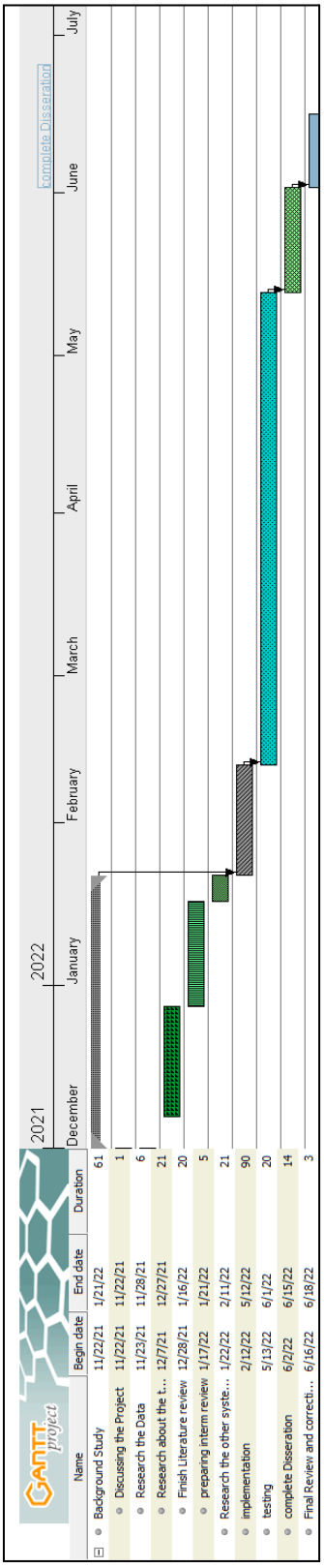


Figure 27: Gantt chart

Appendix 3 – Project Diary

EDINBURGH NAPIER UNIVERSITY

SCHOOL OF COMPUTING

PROJECT DIARY

Student: Kyaw Hein **Supervisor: Dr.Nyo Nyo Htwe**

Date: 20/1/2022 **Last diary date: 10/1/2022**

Objectives:

- Determine and describe the analysis environment is secure to run malware
- Discuss about the testing

Progress:

- Determined that virtual environment is used for implementation

Supervisor's Comments:

Appendix 4 – Project Diary

EDINBURGH NAPIER UNIVERSITY

SCHOOL OF COMPUTING

PROJECT DIARY

Student: Kyaw Hein **Supervisor: Dr.Nyo Nyo Htwe**

Date: 20/2/2022 **Last diary date: 10/2/2022**

Objectives:

- Determine if use of cuckoo sandbox is a better option for malware analysis

Progress:

- Determined that cuckoo sandbox to be used for implementing testing
- Literature review is complete.

Supervisor's Comments:

Appendix 5 – Project Diary

EDINBURGH NAPIER UNIVERSITY

SCHOOL OF COMPUTING

PROJECT DIARY

Student: Kyaw Hein **Supervisor: Dr.Nyo Nyo Htwe**

Date: 29/5/2022 **Last diary date: 20/5/2022**

Objectives:

- Discussing analysis system implementation
- Discussing the problem between host and guest configuration

Progress:

- Fixing the problem of configuration

Supervisor's Comments:

Appendix 6 – Project Diary

EDINBURGH NAPIER UNIVERSITY

SCHOOL OF COMPUTING

PROJECT DIARY

Student: Kyaw Hein **Supervisor: Dr.Nyo Nyo Htwe**

Date: 12/3/2022 **Last diary date: 7/3/2022**

Objectives:

- Discussing about the Analysis techniques, such as static and dynamic analyses
- Discussing the topic of the project, how to approaches Malware analysis
- Asking about the some idea of malware analysis technique.

Progress:

- Understand the different types of techniques for analysis

Supervisor's Comments:

Reference

- "Cuckoo Sandbox Overview." *Cuckoo Sandbox Overview*, www.varonis.com, 26 May 2021, https://www.varonis.com/blog/cuckoo-sandbox.
- "What Is Malware? Types of Malware Attacks | Fortinet." *Fortinet*, www.fortinet.com, https://www.fortinet.com/resources/cyberglossary/malware. Accessed 14 July 2022.
- Ali. (2021, November 14). *The scientific method of research: Steps of scientific method*. ResearcherPort. Retrieved February 1, 2022, from https://www.researcherport.com/2021/10/scientific-method-of-research.html
- Amir Afianian, Salman Niksefat, Babak Sadeghiyan, and David Baptiste. 2019. Malware Dynamic Analysis Evasion Techniques: A Survey. ACM Comput. Surv. 52, 6, Article 126 (November 2020), 28 pages. DOI:https://doi.org/10.1145/3365001
- Analysis of Malware: Detecting Behavior & Anti-Reversing Techniques, http://niiconsulting.com/checkmate/2014/04/analysis-of malware-detecting-behaviour-anti-reversing-techniques.
- *Automated malware analysis*. Cuckoo Sandbox - Automated Malware Analysis. (n.d.). Retrieved July 29, 2022, from https://www.cuckoosandbox.org/
- Bates, J., 1990. Trojan Horse : AIDS Disk AIDS Disk - Issues Pertaining to. , (January)
- crowdstrike.com. 2022. *Malware Analysis Explained | Steps & Examples | CrowdStrike*. [online] Available at: <https://www.crowdstrike.com/cybersecurity-101/malware/malware-analysis/> [Accessed 23 July 2022].
- *Cuckoo sandbox book - read the docs*. (n.d.). Retrieved July 29, 2022, from https://media.readthedocs.org/pdf/cuckoo/latest/cuckoo.pdf
- D. Deka, N. Sarma and N. J. Panicker, "Malware detection vectors and analysis techniques: A brief survey," 2016 International Conference on Accessibility to Digital World (ICADW), 2016, pp. 81-85, doi: 10.1109/ICADW.2016.7942517.

- Dansimp. (n.d.). *Worms*. Microsoft Docs. Retrieved July 25, 2022, from https://docs.microsoft.com/en-us/microsoft-365/security/intelligence/worms-malware?view=o365-worldwide
- Docs.microsoft.com. 2022. *Worms*. [online] Available at: <https://docs.microsoft.com/en-us/microsoft-365/security/intelligence/worms-malware?view=o365-worldwide> [Accessed 27 July 2022].
- Duncan, B. (2022, May 12). *Emotet summary: November 2021 through January 2022*. Unit 42. Retrieved July 27, 2022, from https://unit42.paloaltonetworks.com/emotet-malware-summary-epoch-4-5/
- FireEye Malware Analysis, http://www.fireeye.com/products/malwareanalysis.html.
- *Global cybersecurity index 2020 - itu.int*. (n.d.). Retrieved January 31, 2022, from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf
- *Global cybersecurity index*. ITU. (n.d.). Retrieved January 31, 2022, from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
- Gorrie, M. (n.d.). *Twitter title what is adware?* Official Site. Retrieved July 26, 2022, from https://us.norton.com/internetsecurity-emerging-threats-what-is-grayware-adware-and-madware.html
- Greamo, C., Ghosh, A., Sandboxing and Virtualization: Modern Tools for Combating Malware, Security & Privacy, IEEE,April 2011, Volume:9, Issue: 2, pp.79-82.
- Hinguruduwa, Lahiru. “Setting up Cuckoo Sandbox For Dummies (Malware Analysis).” *Medium*, medium.com, 10 Mar. 2020, https://medium.com/@oshara.16/setting-up-cuckoo-sandbox-for-dummies-malware-analysis-3daa99e950b5.
- *Home Page*. Home Page | InfoSecWriters.com. (n.d.). Retrieved July 26, 2022, from https://www.infosecwriters.com/
- *How to remove a Trojan, virus, Worm, or other malware*. BleepingComputer. (n.d.). Retrieved July 26, 2022, from

https://www.bleepingcomputer.com/tutorials/how-to-remove-a-trojan-virus-worm-or-malware/

- *Internet crime complaint center(ic3): Home Page*. FBI and IC3 Seals. (n.d.). Retrieved July 27, 2022, from https://www.ic3.gov/
- Kävrestad J. (2020) Malware Analysis. In: Fundamentals of Digital Forensics. Springer, Cham. https://doi.org/10.1007/978-3-030-38954-3_21
- Kolbitsch, C., Comparetti, P. M., Kruegel, C., Kirda, E., Zhou, X. Y., & Wang, X. (2009, August). Effective and Efficient Malware Detection at the End Host. In USENIX security symposium (Vol. 4, No. 1, pp. 351-366)
- *List of available regions*. Avast Blog. (n.d.). Retrieved July 26, 2022, from https://blog.avast.com/
- Love, P. by J., & Love, J. (2019, September 19). *A brief history of malware-its evolution and impact*. Lastline. Retrieved July 15, 2022, from https://www.lastline.com/blog/history-of-malware-its-evolution-and-impact/#_edn1
- M. Ijaz, M. H. Durad and M. Ismail, "Static and Dynamic Malware Analysis Using Machine Learning," 2019 16th International Bhurban Conference on Applied Sciences and Technology (IBCAST), 2019, pp. 687-691, doi: 10.1109/IBCAST.2019.8667136.
- *Malwarebytes cybersecurity for home and business: Anti-malware & antivirus*. Malwarebytes Cybersecurity for Home and Business | Anti-Malware & Antivirus. (n.d.). Retrieved July 24, 2022, from https://www.malwarebytes.com/
- Manuel Egele, Theodoor Scholte, Engin Kirda, and Christopher Kruegel. 2008. A survey on automated dynamic malware-analysis techniques and tools. ACM Comput. Surv. 44, 2, Article 6 (February 2012), 42 pages. DOI:https://doi.org/10.1145/2089125.2089126
- Mohanta A., Saldanha A. (2020) Malware Analysis Lab Setup. In: Malware Analysis and Detection Engineering. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-6193-4_2
- Mourad Hassan; Dr. Leune, Kees; Sleeping Your Way out of the Sandbox, SANS Institute, 2015, http://www.sans.org/readingroom/ whitepapers/malicious/sleeping-sandbox-35797.

- Myanamr responsiblebusiness- Retrieved January 31, 2022, From, https://www.myanmar-responsiblebusiness.org/news/legal-framework-for-cybersecurity.html
- *Myanmar presentation - coe*. (n.d.). Retrieved January 31, 2022, from https://rm.coe.int/03-myanmar-presentation/168072bd20
- *Myanmar*. NCSI. (n.d.). Retrieved January 31, 2022, from https://ncsi.ega.ee/country/mm/
- Practical malware analysis, https://www.blackhat.com/presentations/bhdc-07/Kendall_McMillan/Presentation/bh-dc-07-Kendall_McMillan.pdf.
- *Project Guide for steps of the scientific method*. Science Buddies. (n.d.). Retrieved February 1, 2022, from https://www.sciencebuddies.org/science-fair-projects/science-fair/steps-of-the-scientific-method
- Rakesh Singh Kunwar and Priyanka Sharma. 2016. Malware Analysis: Tools and Techniques. In Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies. Association for Computing Machinery, New York, NY, USA, Article 144, 1–4. DOI:https://doi.org/10.1145/2905055.2905361
- Ramakoteswara Rao G.et al., “Enhancing The Impregnability of Linux Servers" International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.2, March 2014, pp.21-31, DOI : 10.5121/ijnsa.2014.6202 2.
- *Resources*. CISA. (n.d.). Retrieved July 24, 2022, from https://www.cisa.gov/stopransomware/resources
- S. Jamalpur, Y. S. Navya, P. Raja, G. Tagore and G. R. K. Rao, "Dynamic Malware Analysis Using Cuckoo Sandbox," 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), 2018, pp. 1056-1060, doi: 10.1109/ICICCT.2018.8473346.
- S. Jamalpur, Y. S. Navya, P. Raja, G. Tagore and G. R. K. Rao, "Dynamic Malware Analysis Using Cuckoo Sandbox," 2018 Second International Conference on Inventive

Communication and Computational Technologies (ICICCT), 2018, pp. 1056-1060, doi: 10.1109/ICICCT.2018.8473346.

- Saengphaibul, V. (2022, March 15). *A brief history of the evolution of malware: FortiGuard Labs.* Fortinet Blog. Retrieved July 29, 2022, from https://www.fortinet.com/blog/threat-research/evolution-of-malware
- Saengphaibul, V. (2022, March 15). *A brief history of the evolution of malware: FortiGuard Labs.* Fortinet Blog. Retrieved July 27, 2022, from https://www.fortinet.com/blog/threat-research/evolution-of-malware
- Steven Floek, November 2016. "Ransomware Analysis and Detection System". Edinburgh Napier University.
- *Stop ransomware*. CISA. (n.d.). Retrieved July 25, 2022, from https://www.cisa.gov/stopransomware
- T. Mokoena and T. Zuva, "Malware Analysis and Detection in Enterprise Systems," 2017 IEEE International Symposium on Parallel and Distributed Processing with Applications and 2017 IEEE International Conference on Ubiquitous Computing and Communications (ISPA/IUCC), 2017, pp. 1304-1310, doi: 10.1109/ISPA/IUCC.2017.00199.
- T. Mokoena and T. Zuva, "Malware Analysis and Detection in Enterprise Systems," 2017 IEEE International Symposium on Parallel and Distributed Processing with Applications and 2017 IEEE International Conference on Ubiquitous Computing and Communications (ISPA/IUCC), 2017, pp. 1304-1310, doi: 10.1109/ISPA/IUCC.2017.00199.
- *Virustotal*. VirusTotal. (n.d.). Retrieved July 29, 2022, from https://www.virustotal.com/
- Wagener, G., State, R. & Dulaunoy, A. Malware behaviour analysis. J Comput Virol 4, 279–287 (2008). https://doi.org/10.1007/s11416-007-0074-9
- *Welcome to Virtualbox.org!* Oracle VM VirtualBox. (n.d.). Retrieved July 29, 2022, from https://www.virtualbox.org/
-