National College of Ireland

Project Submission Sheet

Student Name:	Ansh Ashwini Jain		
Student ID:	233308320		
Programme:	Msc in Cybersecurity	**Year:**	2025
Module:	Malware Analysis		
Lecturer:	Mr. Vikas Sahani		
Submission Due Date:	9th March 2025		
Project Title:	CA1 Malware Analysis		
Word Count:	2939		

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the references section. Students are encouraged to use the Harvard Referencing Standard supplied by the Library. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action. Students may be required to undergo a viva (oral examination) if there is suspicion about the validity of their submitted work.

Signature:	Ansh Ashwini Jain
Date:	9th March 2025

PLEASE READ THE FOLLOWING INSTRUCTIONS:

1. Please attach a completed copy of this sheet to each project (including multiple copies).
2. Projects should be submitted to your Programme Coordinator.
3. **You must ensure that you retain a HARD COPY of ALL projects**, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer. Please do not bind projects or place in covers unless specifically requested.
4. You must ensure that all projects are submitted to your Programme Coordinator on or before the required submission date. **Late submissions will incur penalties.**
5. All projects must be submitted and passed in order to successfully complete the year. **Any project/assignment not submitted will be marked as a fail.**

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

AI Acknowledgement Supplement

Malware Analysis

CA1 Malware Analysis

Your Name/Student Number	Course	Date
Ansh Ashwini Jain/23308320	Msc In Cybersecurity	9th March 2025

This section is a supplement to the main assignment, to be used if AI was used in any capacity in the creation of your assignment; if you have queries about how to do this, please contact your lecturer. For an example of how to fill these sections out, please click here.

AI Acknowledgment

This section acknowledges the AI tools that were utilized in the process of completing this assignment.

Tool Name	Brief Description	Link to tool
ChatGPT	To generate human like responses from questions asked	www.chatgpt.com

Description of AI Usage

This section provides a more detailed description of how the AI tools were used in the assignment. It includes information about the prompts given to the AI tool, the responses received, and how these responses were utilized or modified in the assignment. **One table should be used for each tool used**.

CHATGPT	
To gain more understanding about different sandboxes available.	
list of Top 10 malware analysis sandboxes. Create a table with the information of the malware, Uniqueness, release date, free or paid, downloadable or online and link to the tool	A table with information of different sandboxes and their comparison within each other
mention the common practices and the unique practices followed in the following malware sandboxes: Cuckoo Joe GFI Tria.ge CAPEv2 Hybrid Analysis Cisco Threat Grid	Comparison Table of different sandboxes with information present.

Evidence of AI Usage

This section includes evidence of significant prompts and responses used or generated through the AI tool. It should provide a clear understanding of the extent to which the AI tool was used in the assignment. Evidence may be attached via screenshots or text.

Evidence of table prompt:

Tool Name	Uniqueness	Release Date	Availability	Access Method	Link
Cuckoo Sandbox	Open-source automated malware analysis system	2010	Free	Downloadable	Cuckoo Sandbox
ANY.RUN	Interactive online malware analysis with real-time monitoring	2016	Free/Paid	Online	ANY.RUN
Hybrid Analysis	Cloud-based platform utilizing Falcon Sandbox technology	2017	Free	Online	Hybrid Analysis
Joe Sandbox	Advanced malware analysis with detailed behavioral reporting	2011	Paid	Downloadable/Online	Joe Sandbox
VirusTotal	Aggregates results from multiple antivirus scanners	2004	Free	Online	VirusTotal
VMRay Analyzer	Evasion-resistant dynamic analysis using hypervisor-based monitoring	2013	Paid	Downloadable/Online	VMRay Analyzer
FireEye AX Series	Multi-vector analysis with customizable environments	2004	Paid	Downloadable	FireEye AX Series
Cisco Threat Grid	Combines dynamic and static analysis with threat intelligence	2014	Paid	Downloadable/Online	Cisco Threat Grid
Tria.ge	Automated malware analysis with quick triaging capabilities	2020	Free/Paid	Online	Tria.ge
CAPEv2 Sandbox	Open-source tool focusing on payload execution and analysis	2019	Free	Downloadable	CAPEv2 Sandbox

Evidence of Comparison Prompt

📊 Comparison Summary:

Feature	Cuckoo	Joe Sandbox	GFI	Tria.ge	CAPEv2	Hybrid Analysis	Cisco Threat Grid
Open Source	✅ Yes	❌ No	❌ No	❌ No	✅ Yes	❌ No	❌ No
Anti-Evasion	⚠️ Limited	✅ Advanced	⚠️ Basic	✅ Good	✅ Excellent	✅ Moderate	✅ Strong
Memory Dumping	✅ Yes	✅ Yes	❌ No	✅ Partial	✅ Advanced	✅ Yes	✅ Yes
Payload Extraction	⚠️ Basic	✅ Yes	❌ No	✅ Limited	✅ Excellent	✅ Yes	✅ Yes
Speed	⚠️ Moderate	⚠️ Slow (in-depth)	✅ Fast	✅ Very Fast	✅ Fast	✅ Fast	✅ Fast
Commercial Support	❌ No (Community)	✅ Yes	✅ Yes	✅ Yes	❌ No	✅ Yes	✅ Yes
Cloud Option	✅ (Self-hosted)	✅ Cloud & On-prem	✅ Yes	✅ Cloud-only	✅ (Self-hosted)	✅ Cloud & Private	✅ Cloud & On-prem

ANAYSIS OF AWFULSHRED

Ansh Ashwini Jain
23308320
Msc. In Cybersecurity
National College of Ireland
Dublin, Ireland
x23308320@student.ncirl.ie

***Abstract*—The idea of analyzing a piece of malware called AwfulShred to understand its behavior in a controlled lab setup of Windows and Kali virtual Machines**

Keywords—AwfulShred, Malware Analysis, tools, Sandbox

I. INTRODUCTION

There are various ways into which a malware is analysed, one of them is through a process called sandbox which is to create a testing environment for the unsecure malware to run so that we understand what exactly goes down in it to affect the system. One such malware is AwfulShred, which is a Linux wiper used on a Ukrainian energy provider in early April of 2022. We first will go through different sandboxes and setting up a laboratory to conduct our tests and then will be exploring AwfulShred.

II. SANDBOX ANALYSIS

I have conducted an analysis on seven of the many sandboxes available online and here are my findings. TABLE I consists of the good practices that each available sandbox provides, and tools installed on them which help make the sandbox useful.

III. LAB SETUP

For any malware testing, a concrete and a strong laboratory setup is a much-needed requirement, after careful analysis of the options available, I decided to go ahead with the following Virtual Machine's setup:

1. VirtualBox
2. Windows 10
3. Kali – Linux

A. VirtualBox

My decision for VirtualBox was mainly because it provided a safe and a controlled environment for me to run my malware on. Main features I took advantage of were running virtual machines simultaneously, snapshots to rollback in case of failure and Host Network, in my case I called it “VirtualBox Host-Only Ethernet Adapter” for isolation between the machines to communicate only between them.

B. Windows 10

Using this as a target machine because as it holds the highest market share, it’s the most vulnerable to cyberattacks. I downloaded the Windows 10x64 ISO file from the Microsoft website and created a VDI with size 50GB and 2GB Memory. Created a guest user called 'RobinGuest' to perform task there. Also disabled windows defender to prevent any interference during analysis plus disabled User Access Control.

Fig. 1. Windows 10 Setup

C. Kali

Using this VM specifically to perform static analysis on the file and to set it up I downloaded the ISO File for Kali and setup for Debian x64, with fixed size of 35GB and 2GB Memory.

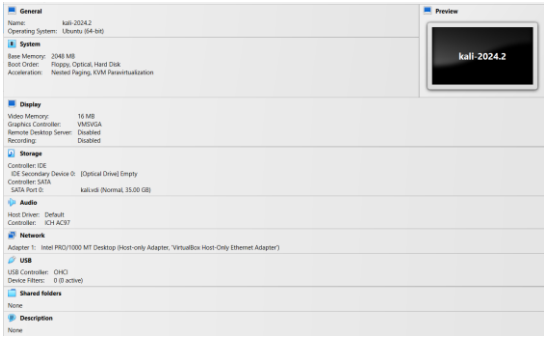

Fig. 2. Kali Linux Setup

For both the VM's I Disconnected any USB devices and connected the machine to the Host Only Adapter set up above to isolate from the network. Also ensured to disable shared folders and clipboard

sharing to ensure the malware does not escape. Also, for easy rollback I took a snapshot of the VM's before starting analysis to ensure no issues when rolling back.

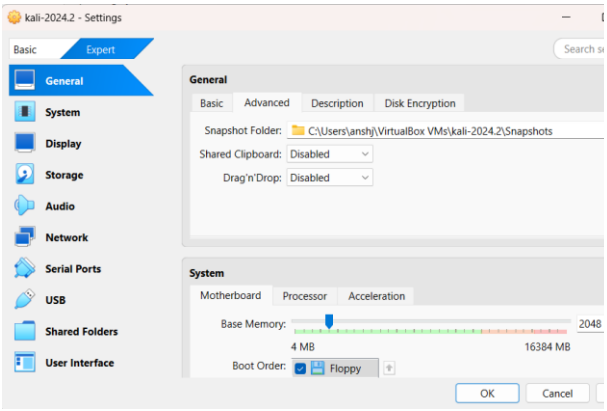

Fig. 3. Additional Settings

IV. TOOLS

There are various tools that are available online which can be used for all stages of a malware analysis which includes analysis before running the malware which is static analysis, and the tools used after running which are known as dynamic analysis. Following is the justification for each tool and how they are unique to the scenario while performing the analysis.

Static Analysis

PEStudio: This one helps with examining the executables without even performing a run on them as it identifies the suspicious API calls, or any digital signatures present in the file.

Ghidra: As the AwfulShred file or any other malware file has the possibility of containing malware binaries, this tool here will specifically come in advantage to convert it into readable code. Any malware file can be packed and encrypted, and this will support in decompiling for further extraction of the same.

Dynamic Analysis

ProcMon: Also called as ProcessMonitor, ProcMon is a helpful tool to use when the malware analysis is running to view many such settings like file creation, network access, any activity or registry changes. This helps with understanding how the malware can infect the system and what all changes is it causing to do [9].

Process Explorer: As ProcMon, this too is a part of the Sysinternals suite, and it stands out by detecting any processes. For AwfulShred those processes will be related to file shredding which are sdelete.exe or cipher.exe.

Wireshark: This tool here can be used on both the machines and is helpful in analysing the incoming and the outgoing network traffic for both. If the malware is communicating with any external servers, this tool will help capture the same.

VirusTotal: Is an online malware scanning service which helps in detecting and analysing various files by getting its results from various antivirus engines and different sandbox environments. It helps in becoming a one stop shop for all the information to get you started with about the malware. This tool help give me a boost with my malware information gathering.

V. TESTING

Before starting off my analysis, I had to make sure that the VM's are completely isolated without any disturbances and there will be no leakage of malware during the analysis. For that I tried dragging and dropping the text between the VM's which I disabled in Fig.3 and that did not work which was a good indicator. Next was to ping to the internet which again did not work so isolation from the network as well. Now to test the communication between the two VM's I decided to use the ping function of Linux as I had IP address of both.

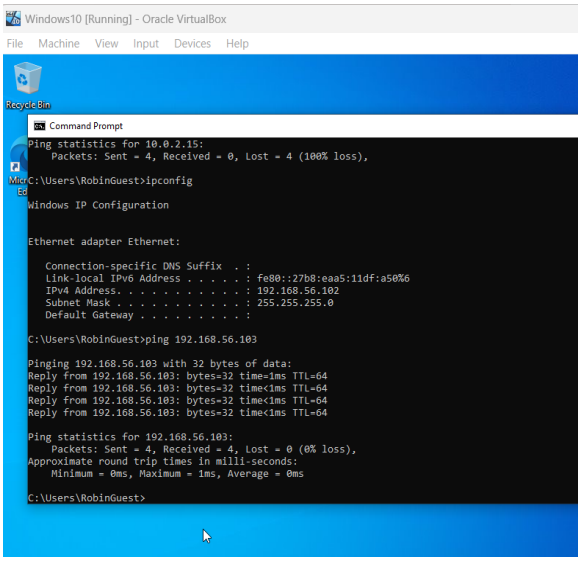

Fig. 4. For Windows

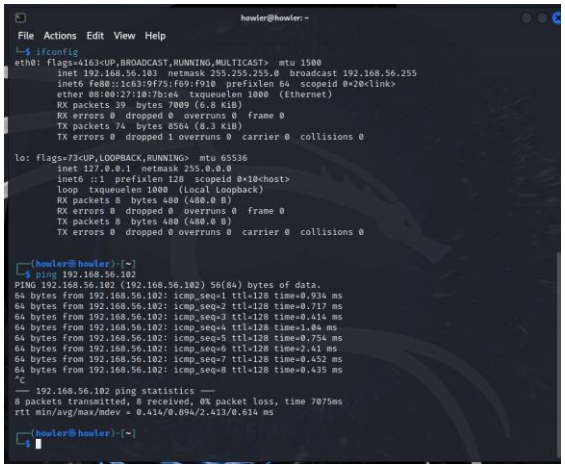

Fig. 5. For Kali

As the only communication that took place was between the VM's and no other external source, I was able to conclude the testing of the VM's Isolation successfully.

VI. AWFULSHRED

A Linux wiper based malware used in April 2022 with many other malwares combined into a Industroyer2 attack, used by Russia to attack an energy facility in a cyberwarfare on Ukraine, AwfulShred is a 422 line bash script, which was used as a wiper in the attack. The Attacker being Sandworm APT, a Russian based cyber-espionage group, targeted the energy facility with various other malwares. As per Virus Total, 34 out of the 61 security vendors that are present, to name a few are ALYac, AVG, BitDefender, Cynet etc have tagged this malware as malicious [7].

TABLE II. AWFULSHRED DESCRIPTION

Name	AwfulShred
First Seen	April 2022
Type	SH - Bourne-Again shell script, ASCII text executable
SHA-256	bcdf0bd8142a4828c61e775686c9892d89893ed0f5093bdc70bde3e48d04ab99
SHA-512	b183e4f345ac70667f83110abcc04a1e25b99671d4b1cbdd59a85af903a18a4a47b7c1de1305893d666acfe756d0f591738b45923eaebb7cc4ca9036d7f339af
MD5	73561d9a331c1d8a334ec48dfd94db99
Size	9.81 KB
Alternate File Names	AWFULSHRED_original.sh wobf.sh 73561d9a331c1d8a334ec48dfd94db99.vir
SSDEEP	192:jNhE21baNxtrilGAL4WDnEHgCyLslERTJx+f4:jNS4OxtOlTE6EAJsp4
TLSH	T1912242CCE1913DB0301609AEEECBA068761D120B484869DA7E9D26D53FA426DC3F1F1D
APT Responsible	Sandworm (Black Energy, UAC-0082)

VII. ORIGIN

As per the emergency response team of Ukraine, CERT-UA AwfulShred was used by a group named "Sandworm" operated allegedly by Russian intelligence orders against a Ukrainian energy facility in April 2022. To target the high-voltage electrical substations and electronic computers, Malware's Industroyer2 & Caddywiper were used and to target the servers operating on Linux, AwfulShred, OrcShred & SoloShred are used [1].

VIII. ARCHITECTURE

Following is an analysis as provided for the Awfulshred malware as to understand what exactly the malware does and the overall steps it follows once it's in the machine [8].

1. The first step the file takes is to self-destruct its own file, which is clearly done to remove any evidence of its existence when an analysis is conducted. It does by shredding it using the shred command and then removing the file.

2. Then the clearance of the ~/bash-history file is done by first clearing and then disabling the history of bash with the command "history -c" and setting the environment variables HISTSIZE, HISTFILESIZE to 0. Then the page cache is cleared using the "/proc/sys/vm/drop_cache" kernel system request and any swapping between the known devices is disabled with the swapoff-a command [2].

3. Then the main wiping process starts off where 4 conditions are checked in the following order:

a. First to check if the script is running with root privileges present.

b. Using the commands "uname -s" and "uname -kernel-release", bash version is higher than 3 and Linux kernel version is 2.6.27 or higher.

c. The commands, "sed","uname","dd" are present.

4. Then if shred is available then it is used as the preferred wiping technique else dd comes into the picture [3].

5. Then the actual destruction starts out by checking three services called: apache, http and ssh.

a. For all of the three services, they are forced stop, then disabled using the commands "systemctl stop" and "systemctl disable" with the systemd files removed first and then restarted back.

b. Then using the rm -rf command, the directories, /boot, /home and /var/log are deleted using the delete from ".service" configuration files.

6. It then follows a set of procedures to look for any disks present on the system and as soon as atleast one disk is found, parallel wiping takes place.

7. The root directory, rm -rf / --no-preserve-root, is recursively deleted as well.

8. Then as a final task, the wiper is checked to be removed again as done in Step 1

9. Taking advantage from the magic SysRq key trick, an immediate system reboot is triggered [4].

IX. MITRE ATT&CK

MITRE ATT&CK (Adversarial Tactics, Techniques and Common Knowledge) is a globally recognized framework which is used in the cybersecurity domain to understand various behaviours [5]. There are various categories like Tactics, Techniques and Procedures which help out the security professionals in detecting and responding. TABLE III of tactics which are related to AwfulShred and the following techniques which are related to it. Here is also a little description of the ID's mentioned:

- T1053.001: Scheduled Task/Job At Linux
- T1059: Executes the "sed" command which is used to modify input streams
- T1543.002: Executes "systemctl" command which is used for controlling the systemd system and service manager
- T1055: Spawns processes
- T1070: Deletes various log files.
- T1003: Enumerates the various processes within the "proc" file system
- T1082: Executes the "uname" command used to read OS and architecture name, Read CPU information, Read system information
- T1071: Uses HTTPS and perform DNS lookups

TABLE III. MITRE ATT&CK

ID	**Tactics**	**Description**	**Technique ID's**
TA0002	Execution	Execute malicious code like powershell scripts and DLL injections	T1053.001, T1059, T1064
TA0003	Persistence	Ensure the access to backdoors and tasks are maintained	T1053.001, T1543.002
TA0004	Privilege Escalation	Gain higher privileges and root access	T1053.001, T1055
TA0005	Defense Evasion	Avoid any detection by disabling logging	T1036, T1055, T1064, T1070, T1562
TA0006	Credential Access	To Steal username and passwords	T1003
TA0007	Discovery	Learn and understand more about the system and the network	T1082, T1083, T1518
TA0011	Command and Control	Establish remote control over the system	T1071, T1095, T1573

X. YARA RULES

YARA (Yet Another Recursive Acronym) is a pattern matching tool, which is used to identify suspicious malware and files. These rules are made up of conditions and signatures to detect any known possible threats associated with the malware. YARA Rules are more of detection than mitigation as once a threat is diagnosed using YARA rules,

organizations must apply firewall rules and patching to help mitigate the risk. Following are a set of strings as deduced that can be considered as YARA Rules to detect Awfulshred [6].

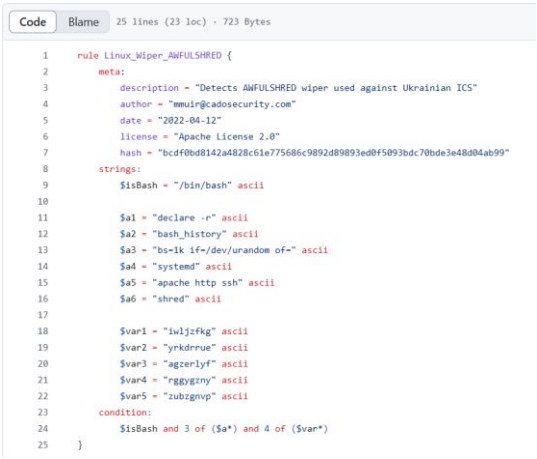

Fig. 6 YARA RULES

XI. CONCLUSION

My overall knowledge on how to extract information out of a malware by setting up a complex and secure lab for analysis has definitely increased from before. Although I never downloaded the malware and used them on any tools or machine's. If I did download the sample, I would debug and analyze the reaction in real time and try and spot exploits which are not already known. I would use the different tools as well mentioned earlier to check out how the malware reacts with each. For Testing by isolation perspective, I also performed a nmap scan to check if there are any open ports present and connect the VM's through a shell. One isolation testing I would like to perform will be to create another VM and deliberately infect it to see if it is spreading or not. Reverting back will always be with the snapshots, so I'll be careful of that. Hands-on perspective wise I would like to explore the REMNUX OS as it looks like a powerful package of all of the required tools.

REFERENCES

[1] lalelong, "Industroyer 2 : the Russian Cyberattack on Ukraine Infrastructure," *Headmind Partners*, May 31, 2022. https://www.headmind.com/industroyer-2/

[2] "CERT-UA," *cert.gov.ua*. https://cert.gov.ua/article/39518

[3] "jet," *Github.io*, 2022. https://0xjet.github.io/3OHA/2022/12/18/post.html (accessed Mar. 09, 2025)

[4] "Threat Update: AwfulShred Script Wiper | Splunk," *Splunk*, 2024. https://www.splunk.com/en_us/blog/security/threat-update-awfulshred-script-wiper.html (accessed Mar. 09, 2025).

[5] MITRE, "Techniques - Enterprise | MITRE ATT&CK®," *attack.mitre.org*, 2023. https://attack.mitre.org/techniques/enterprise/

[6] cado-security, "DFIR_Resources_Industroyer2/YARA/AWFULSHRED.yara at main · cado-security/DFIR_Resources_Industroyer2," *GitHub*, 2022. https://github.com/cado-security/DFIR_Resources_Industroyer2/blob/main/YARA/AWFULSHRED.yara (accessed Mar. 09, 2025).

[7] "VirusTotal - File - bcdf0bd8142a4828c61e775686c9892d89893ed0f5093bdc70bde3e48d04ab99." Accessed: Feb. 06, 2025. [Online]. Available: https://www.virustotal.com/gui/file/bcdf0bd8142a4828c61e775686c9892d89893ed0f5093bdc70bde3e48d04ab99

[8] P. Knapczyk, "Overview of the Cyber Weapons Used in the Ukraine -Russia War." Accessed: Mar. 09, 2025. [Online]. Available: https://www.trustwave.com/hubfs/Web/Library/Documents_pdf/18974_8_25cyber-weapons-used-in-the-ukraine-russia-war.pdf

[9] J. MacLennan and J. Zhang, "Path-Safe: Enabling Dynamic Mandatory Access Controls Using Security Tokens," NAECON 2024 - IEEE National Aerospace and Electronics Conference, Dayton, OH, USA, 2024, pp. 7-11, doi: 10.1109/NAECON61878.2024.10670691.

APPENDIX

TABLE I. SANDBOX ANALYSIS

Tool Name (Release Date)	Access Methods	Availability	Tools Installed	Good Practices Followed
Cuckoo Sandbox (2010)	Downloadable	Free	YARA rules PCAP SIEM, IDS ELK Stack Volatility Framework Docker API Integration	-Dynamic and Static Analysis -Multi-Environment Support -Logging and Reporting -Memory Dumping -API Integration (SIEM, IDS) -Customizability
TRIAGE SANDBOX (2020)	Cloud	Paid / Free	Yara Rules PCAP C2 communication detection API Integration Evasion Detection	-Multi-Environment Support -Behavioral Reports -Quick Analysis -Multi-Sample Support -Modular Pipeline
CAPEV2 SANDBOX (2019)	Downloadable	Free	Process Hollowing Detection TLS & SSL Decryption YARA Rules Docker Support REST API	-Dynamic & Static Analysis -Network Monitoring -Payload Extraction -Anti-Evasion Tactics -Enhanced Memory Forensics
HYBRID ANALYSIS (2017)	Cloud	Free	YARA Rules Network Analysis API Hooking Automated Execution Falcon Sandbox Intelligence	-Multi-Environment Support -Behavioral & Static Analysis -Falcon Intelligence Integration -Public & Private modes -Automated Malware Classification
CISCO THREAT GRID SANDBOX (2014)	Downloadable / Cloud	Paid	File Structure Analysis Network Traffic Monitoring Reputation Based Detection	-Multi-Platform Analysis -Behavioral Observation -Global Threat Intelligence -File Reputation Matching