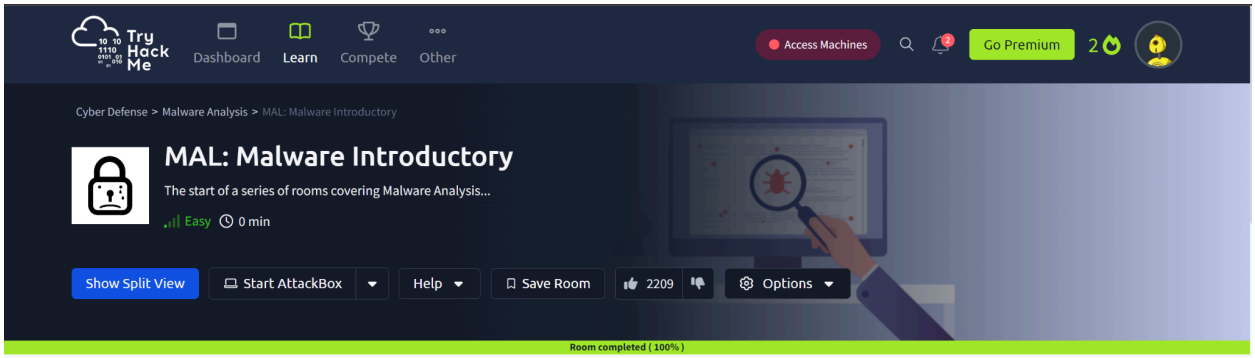
MAL: MALWARE INTRODUCTORY

ASSIGNMENT REPORT



Peter Kinyumu,
cs-sa07-24067,
July 27th, 2024

1. INTRODUCTION

This assignment introduces malware analysis, why it is important, and the various tools and techniques that can be used to analyze a malicious piece of code while it is executing and without executing it.

2. ANSWERS TO QUESTIONS

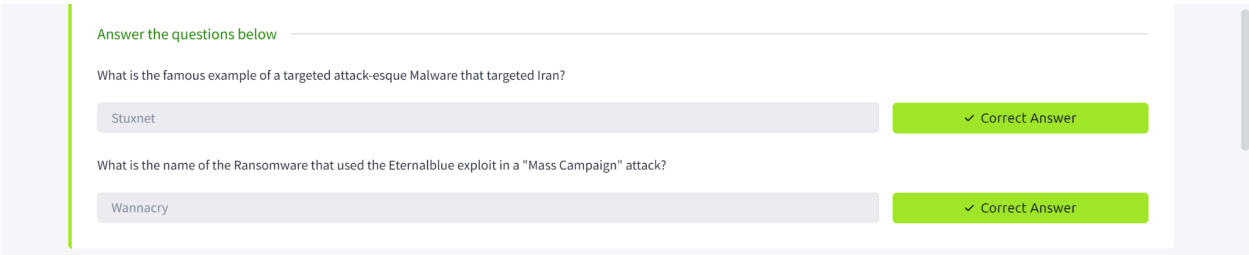
Understanding Malware campaigns

a. What is the famous example of a targeted attack-esque Malware that targeted Iran?

- `Stuxnet`

b. What is the name of the Ransomware that used the Eternalblue exploit in a "Mass Campaign" attack?

- `Wannacry`



Identifying if a malware attack has happened

a. Name the first essential step of a Malware Attack.

- `Delivery`

b. Now, name the second essential step of a Malware Attack.

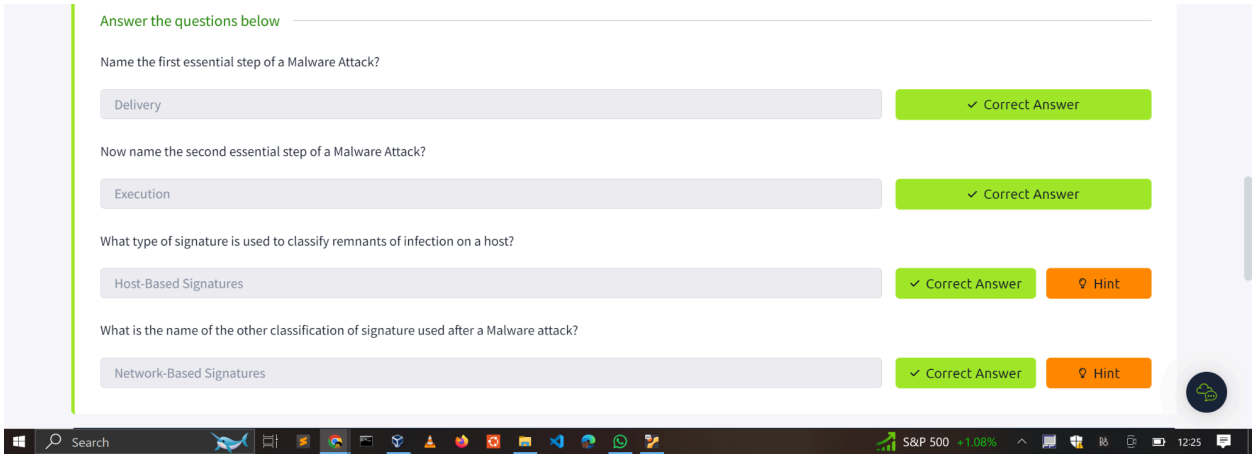
- `Execution`

c. What type of signature is used to classify remnants of infection on a host?

- `Host-Based Signatures`

d. What is the name of the other classification of signature used after a Malware attack?

- `Network-Based Signatures`



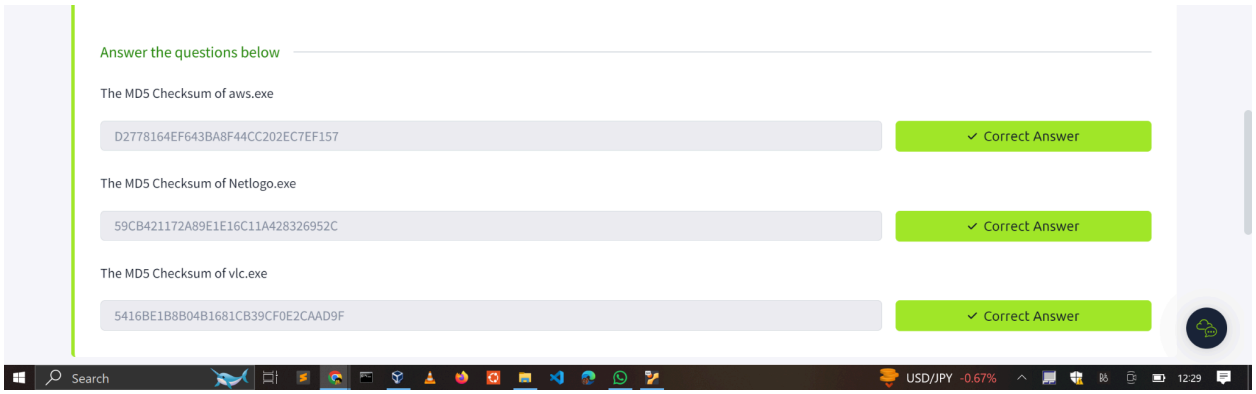
Obtaining MD5 checksums of provided files

Identify the MD5 Checksums of the three files provided in "Task 7" (You can use Ctrl + C & Ctrl + V over RDP)

a. **The MD5 Checksum of aws.exe**
   - `D2778164EF643BA8F44CC202EC7EF157`

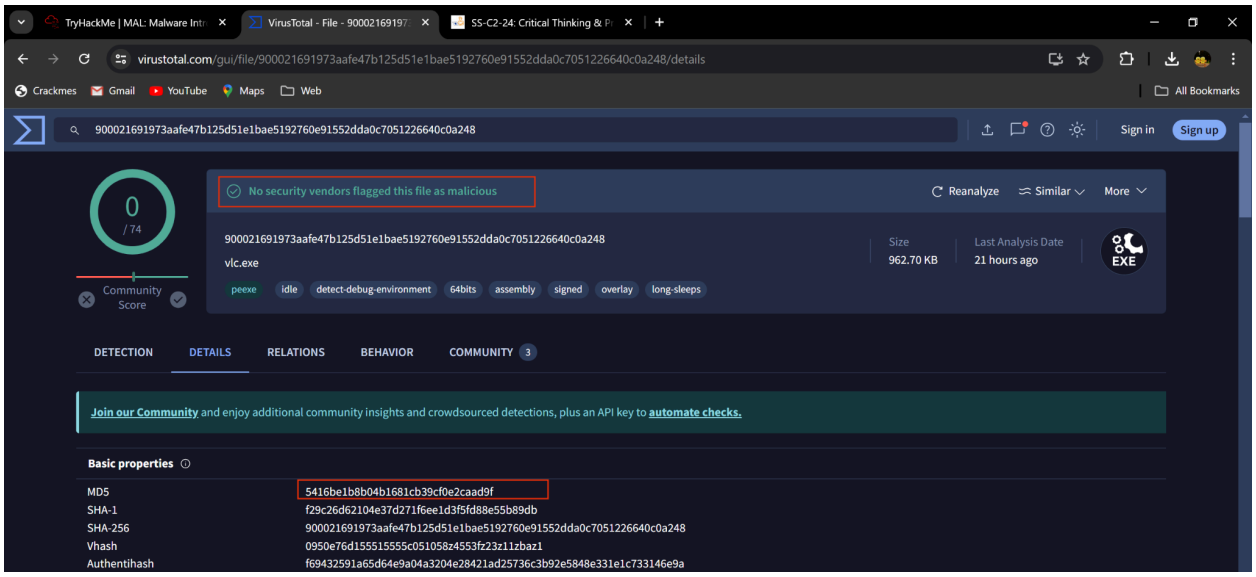
b. **The MD5 Checksum of Netlogo.exe**
   - `59CB421172A89E1E16C11A428326952C`

c. **The MD5 Checksum of vlc.exe**
   - `5416BE1B8B04B1681CB39CF0E2CAAD9F`



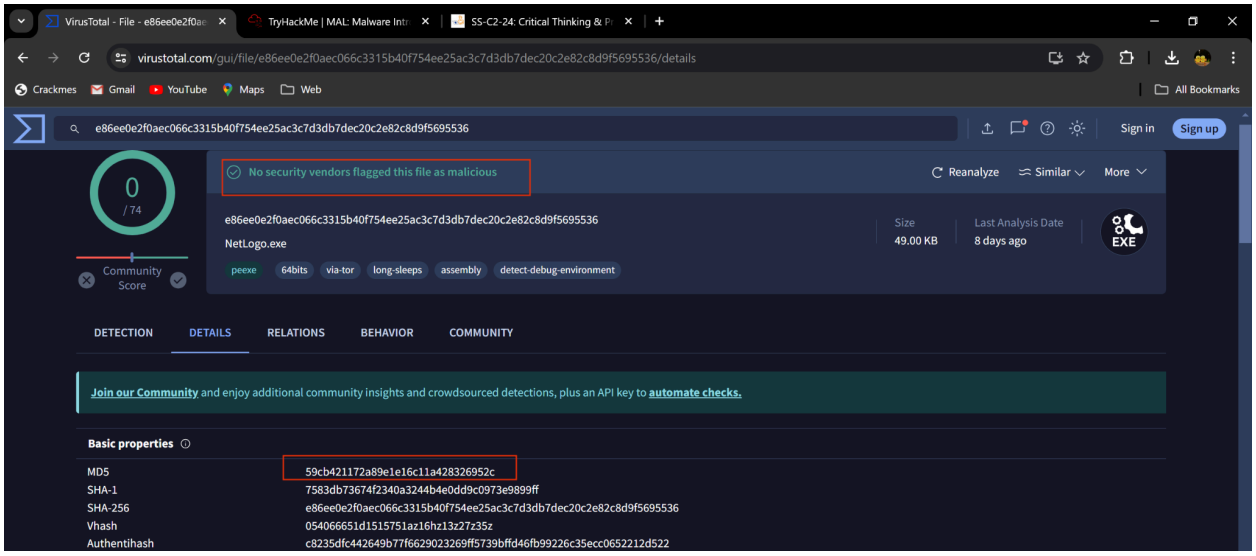
Now let's see if the MD5 checksums have been analyzed before

a. **Does Virustotal report this MD5 Checksum / file aws.exe as malicious? (Yay/Nay)**
   - `Nay`



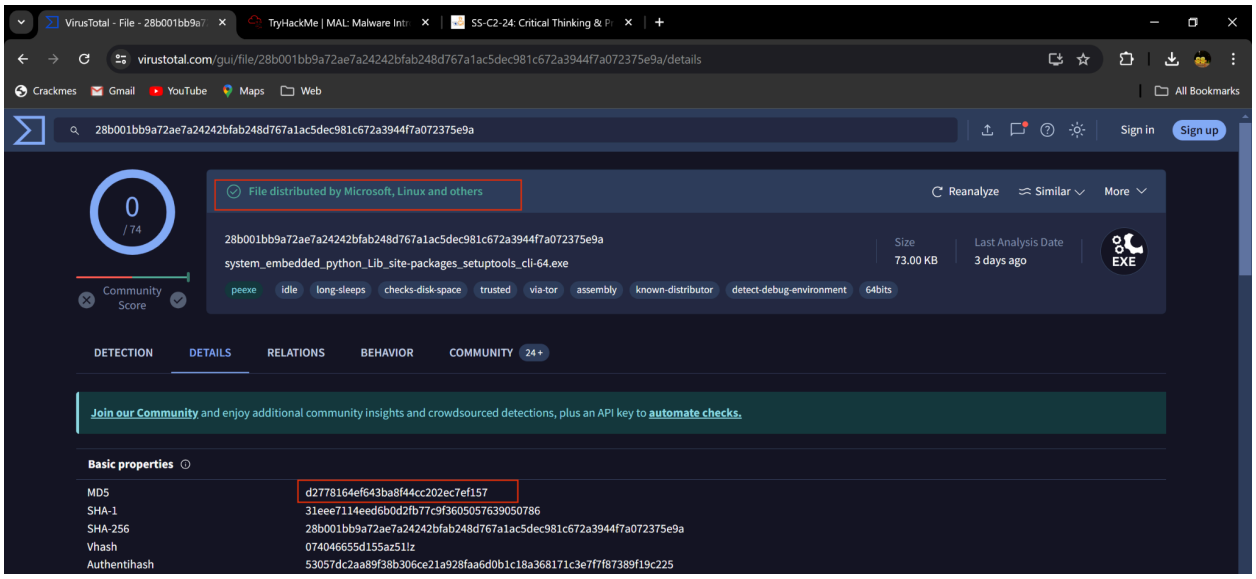
b. Does Virustotal report this MD5 Checksum / file Netlogo.exe as malicious? (Yay/Nay)

- Nay



c. Does Virustotal report this MD5 Checksum / file vlc.exe as malicious? (Yay/Nay)

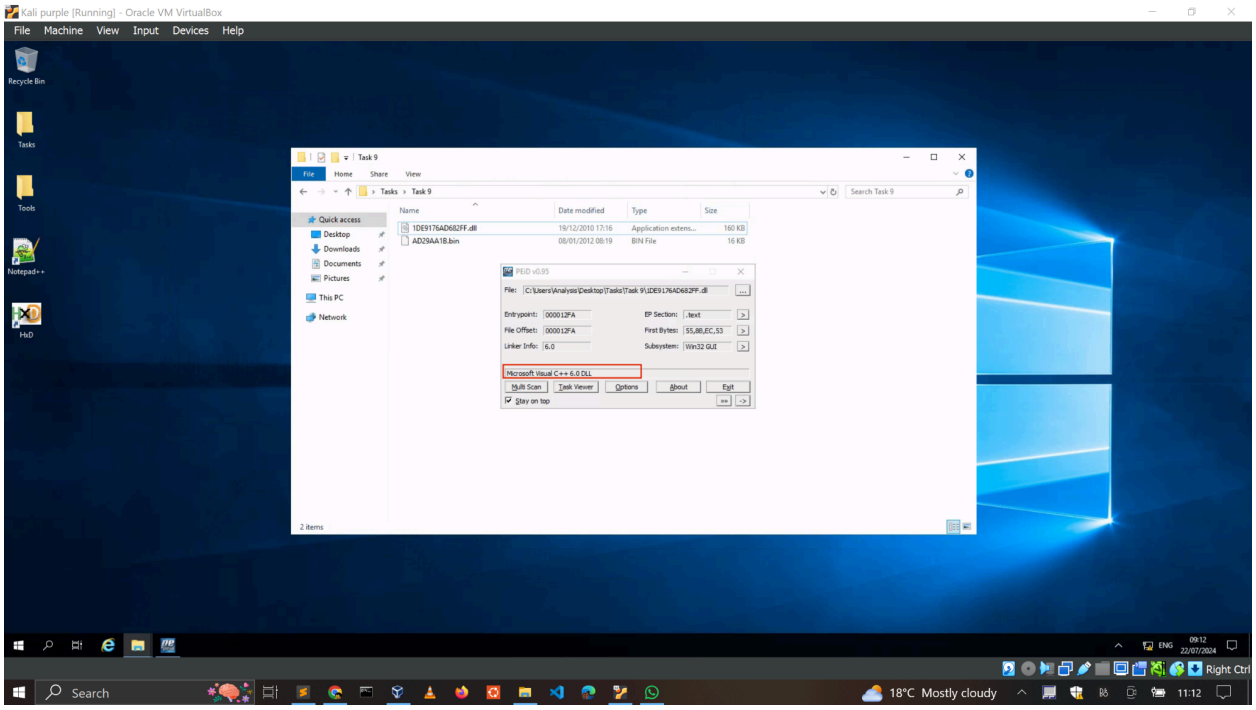
- Nay



Identifying if executables are obfuscated or packed

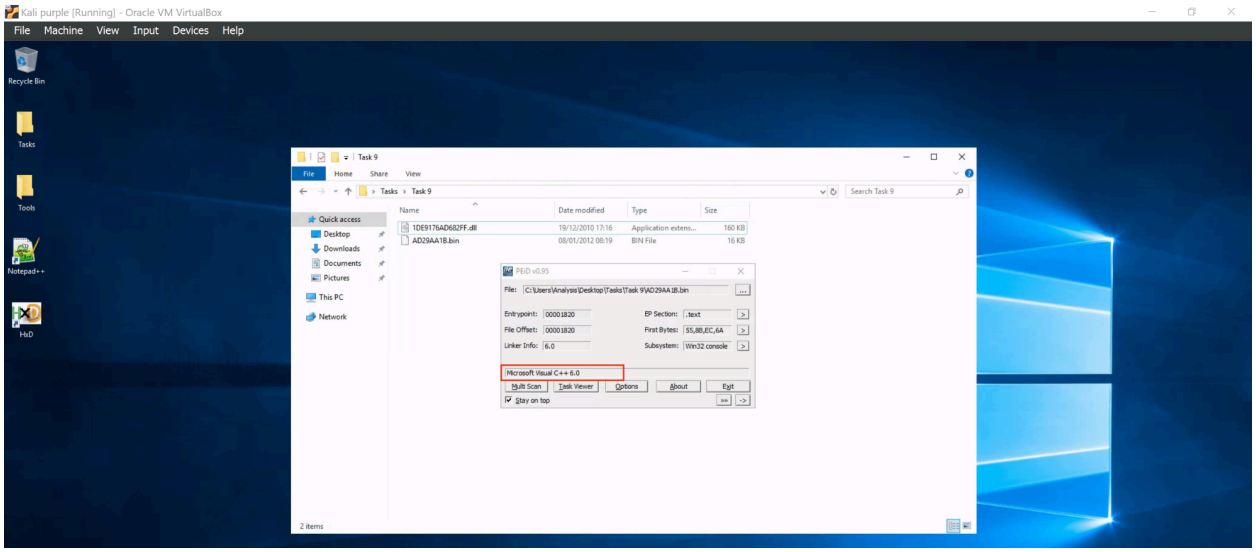
a. **What does PeID propose 1DE9176AD682FF.dll being packed with?**

- `Microsoft Visual C++ 6.0 DLL`



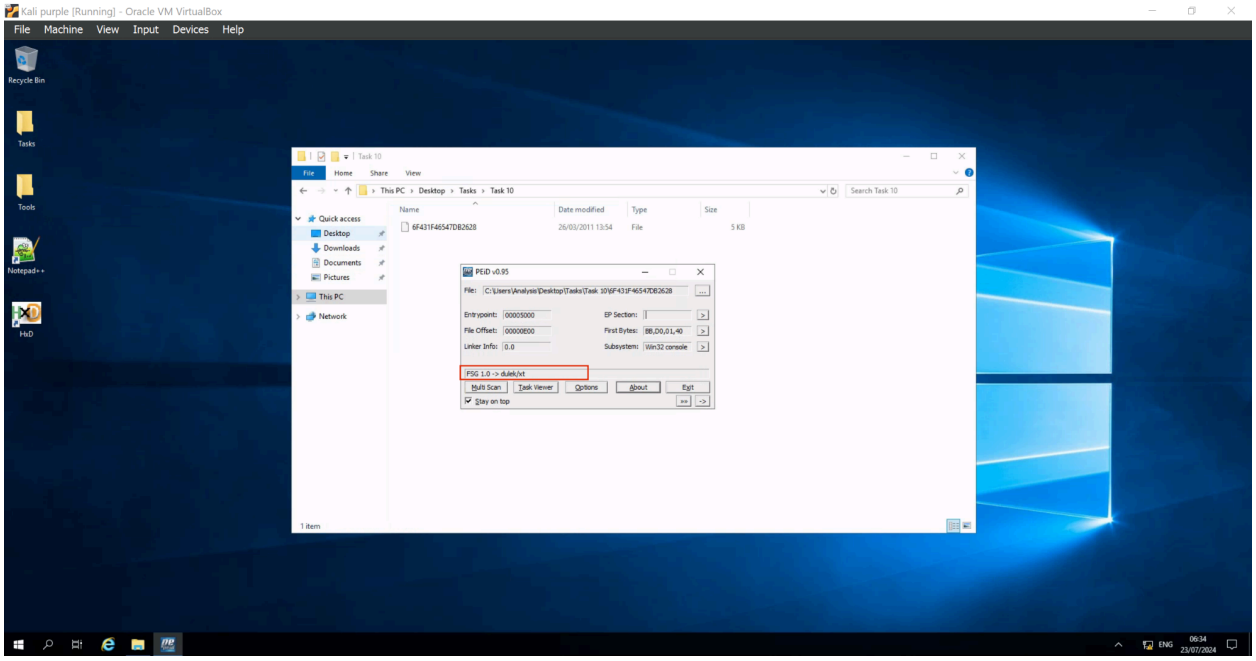
b. **What does PeID propose AD29AA1B.bin being packed with?**

- `Microsoft Visual C++ 6.0`



c. **What packer does PeID report file "6F431F46547DB2628" to be packed with?**

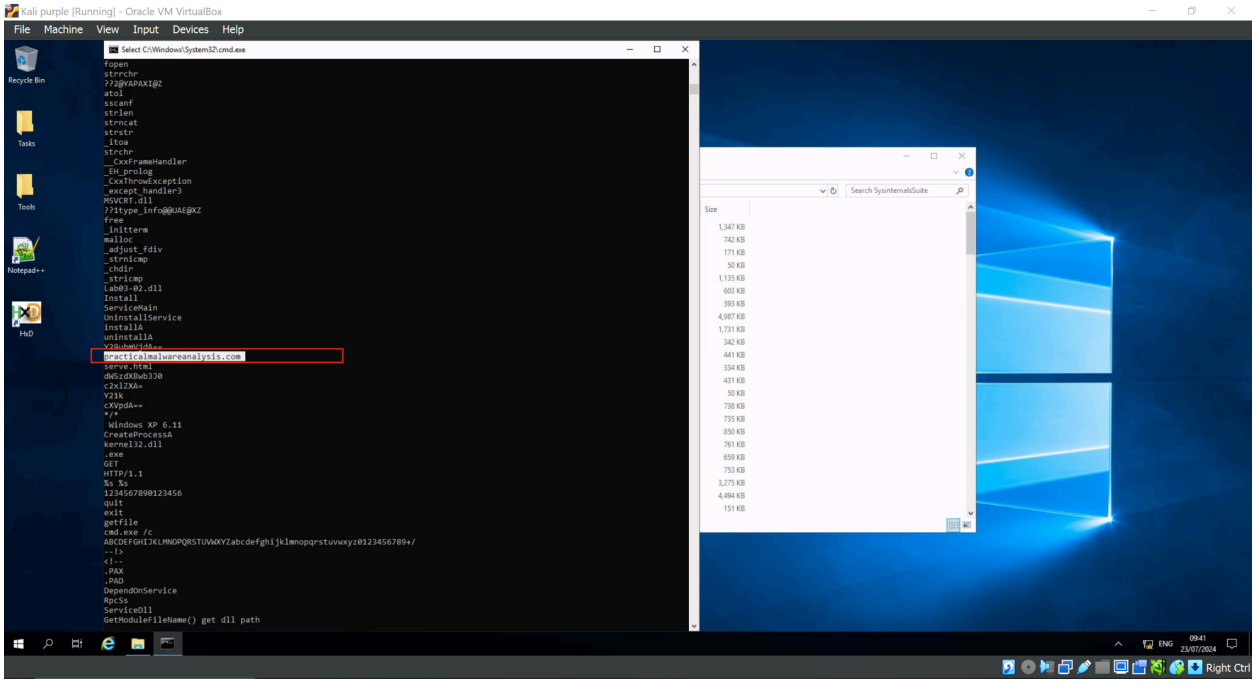
- `FSG 1.0 -> dulek/xt`



Introduction to strings

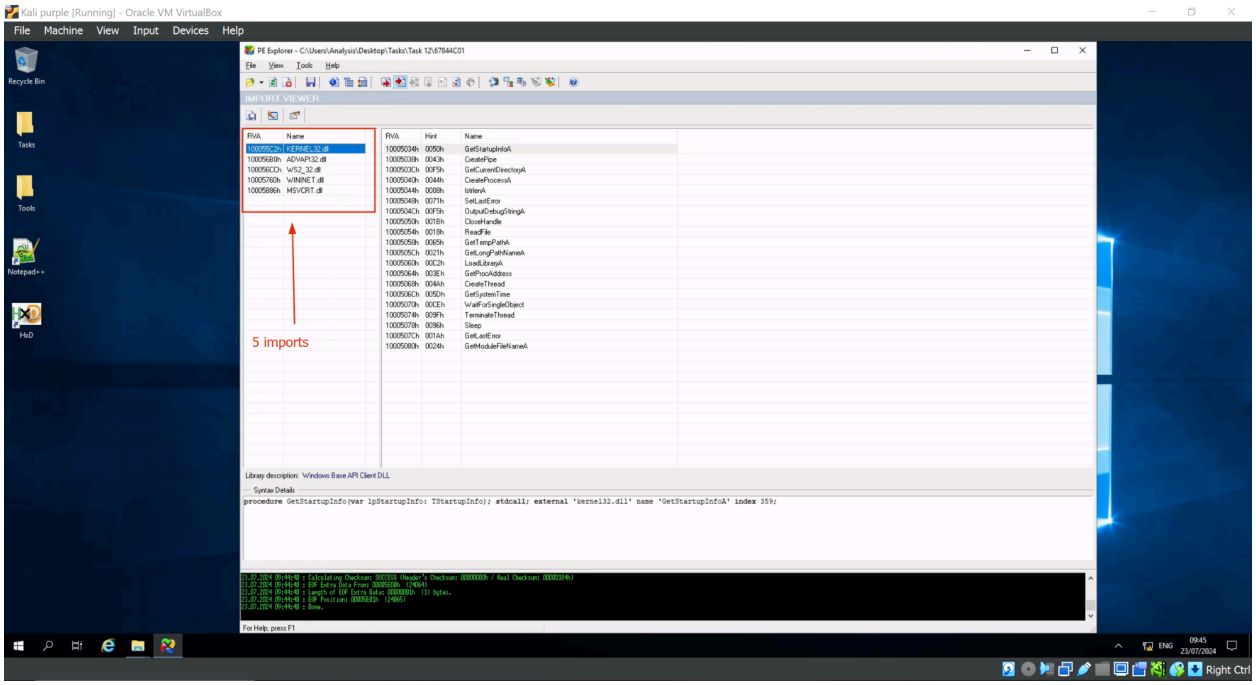
a. **What is the URL that is outputted after using "strings"**

- `practicalmalwareanalysis.com`



b. How many unique "Imports" are there?

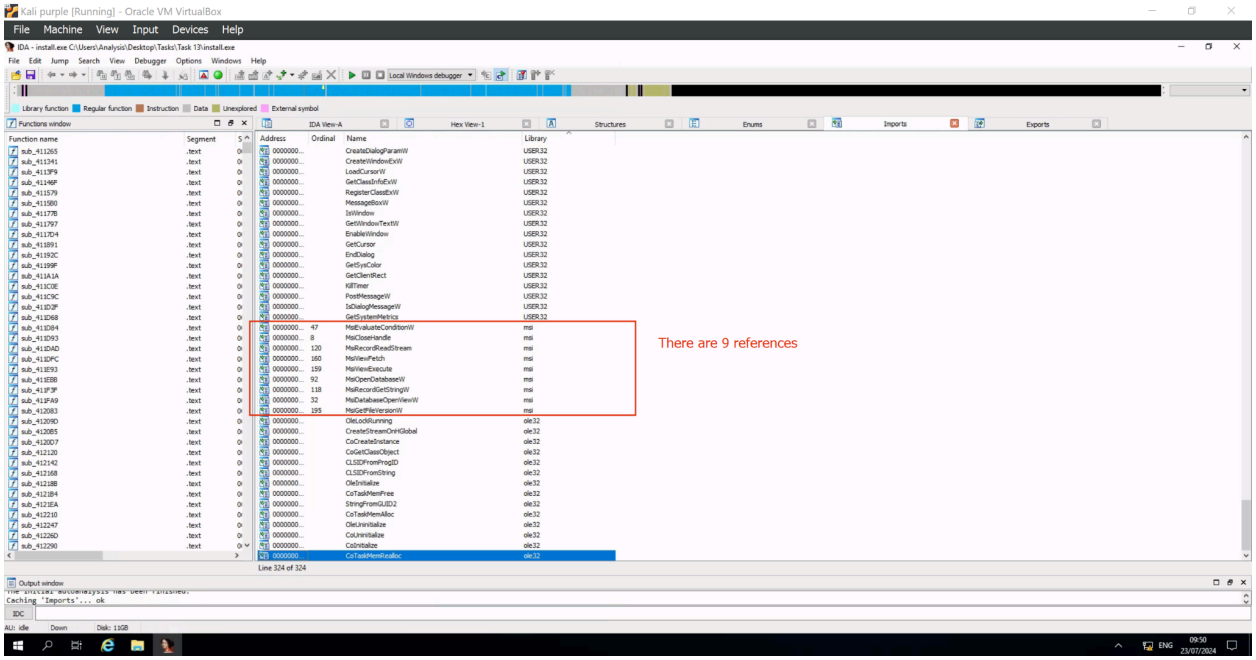
- 5



Introduction to strings

a. How many references are there to the library "msi" in the "Imports" tab of IDA Freeware for "install.exe"

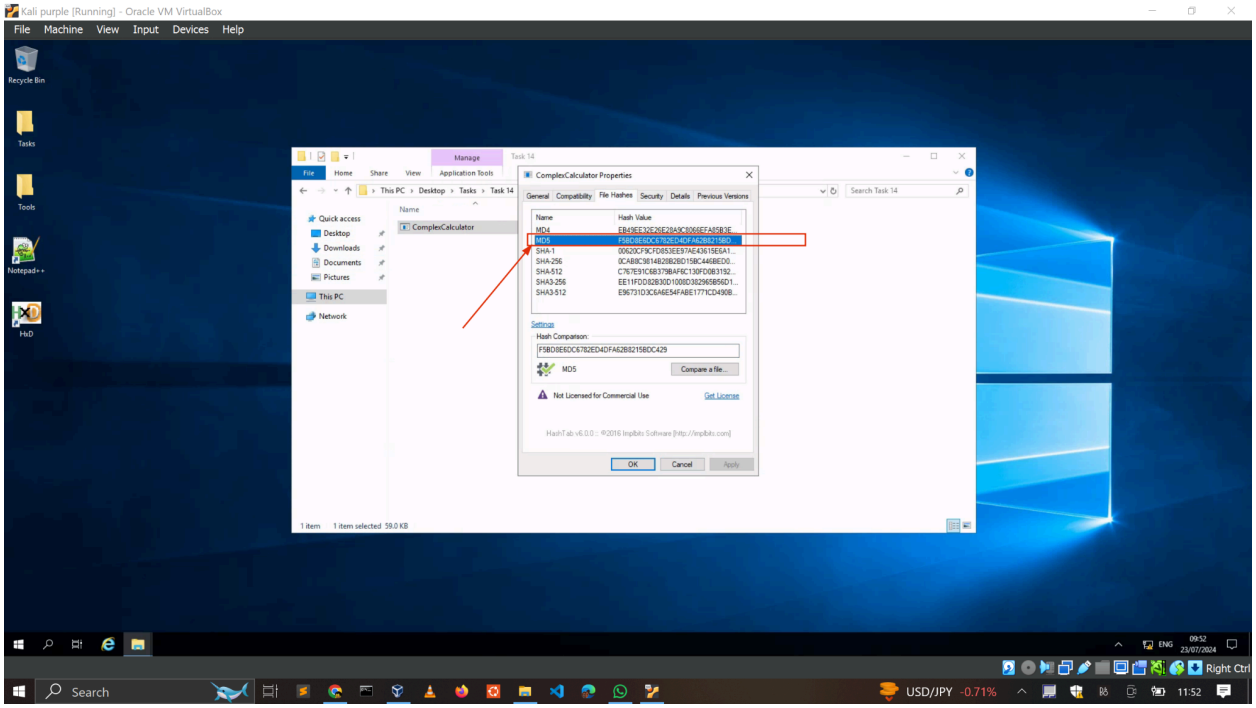
- 9



Introduction to strings

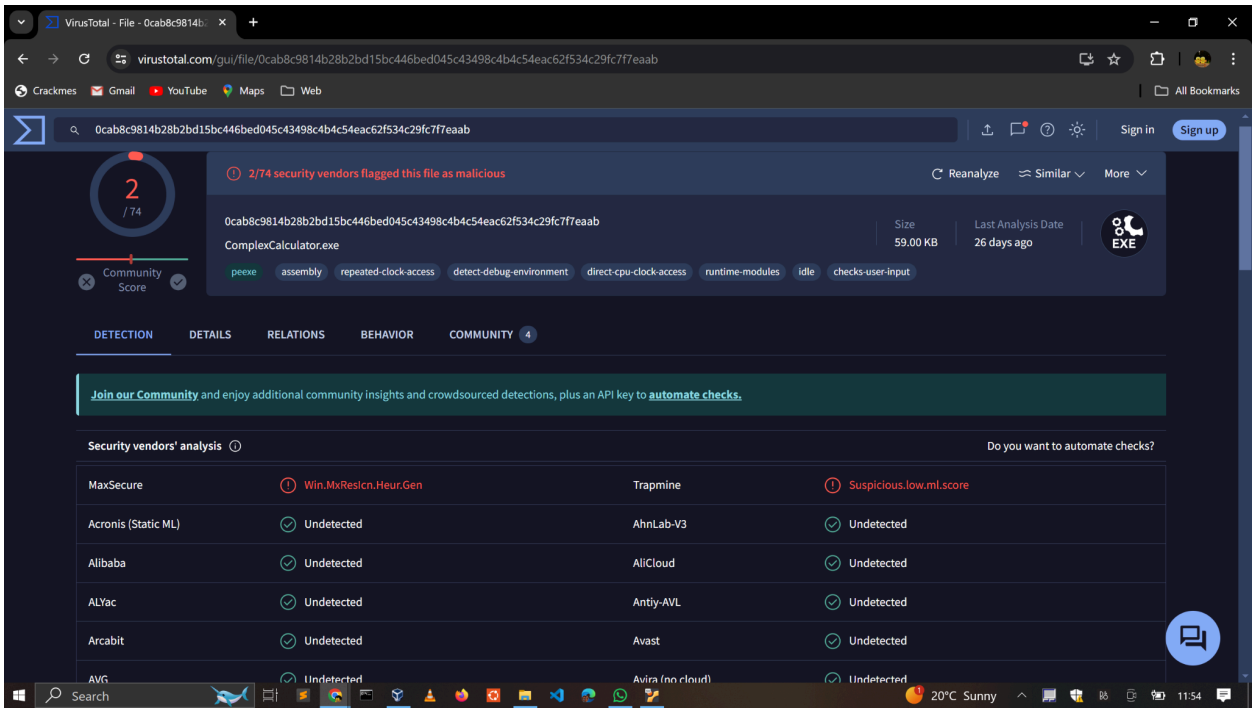
a. What is the MD5 Checksum of the file?

- f5bd8e6dc6782ed4dfa62b8215bdc429



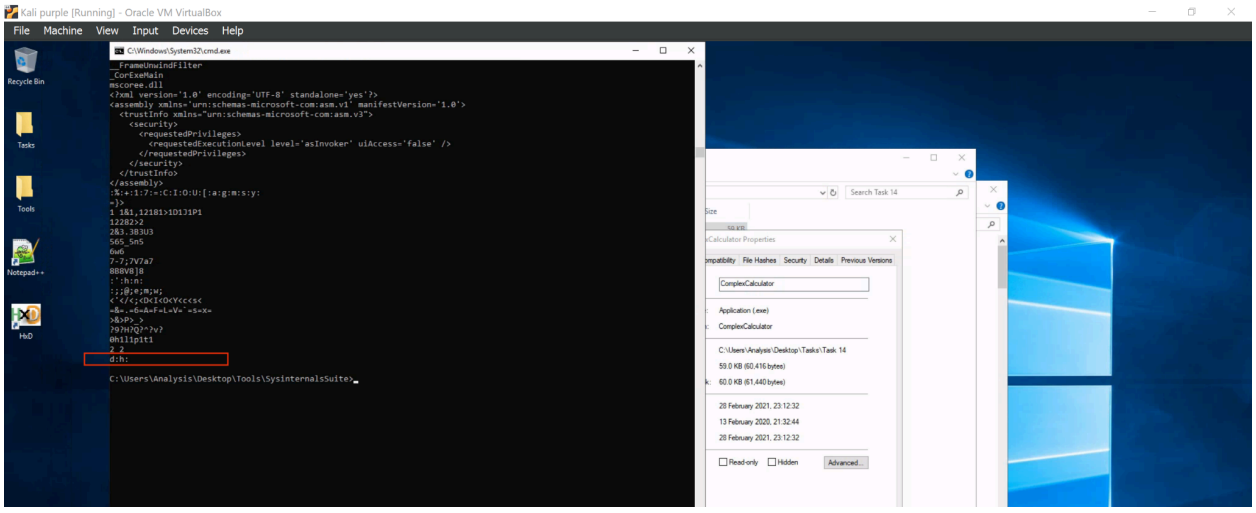
b. Does Virustotal report this file as malicious? (Yay/Nay)

- Yay



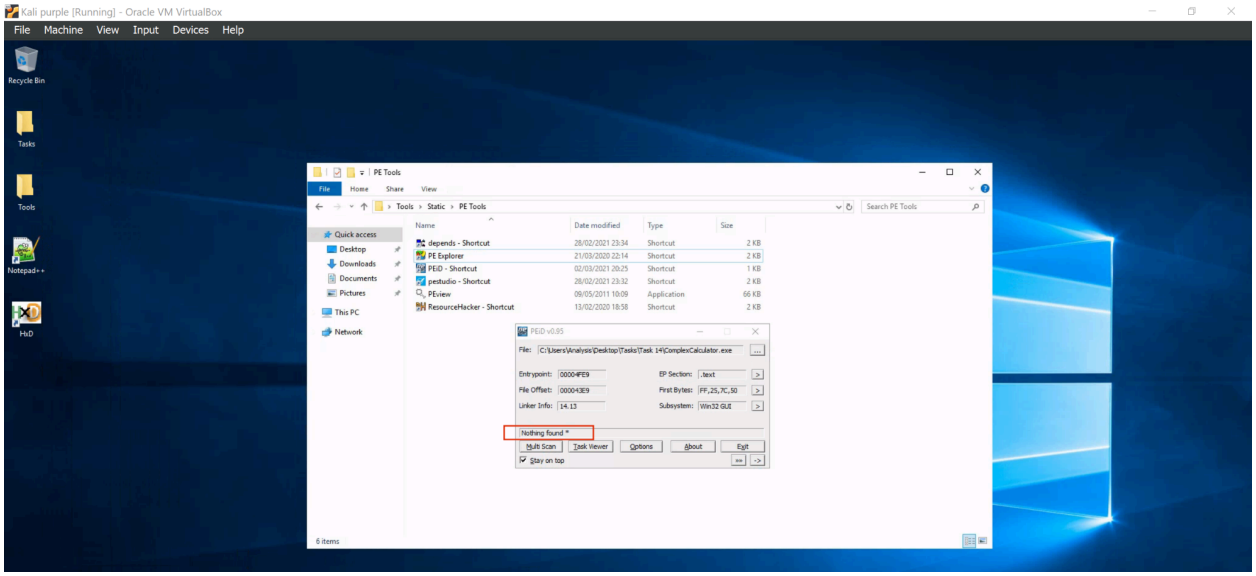
c. Output the strings using Sysinternals "strings" tool. What is the last string outputted?

- d:h:



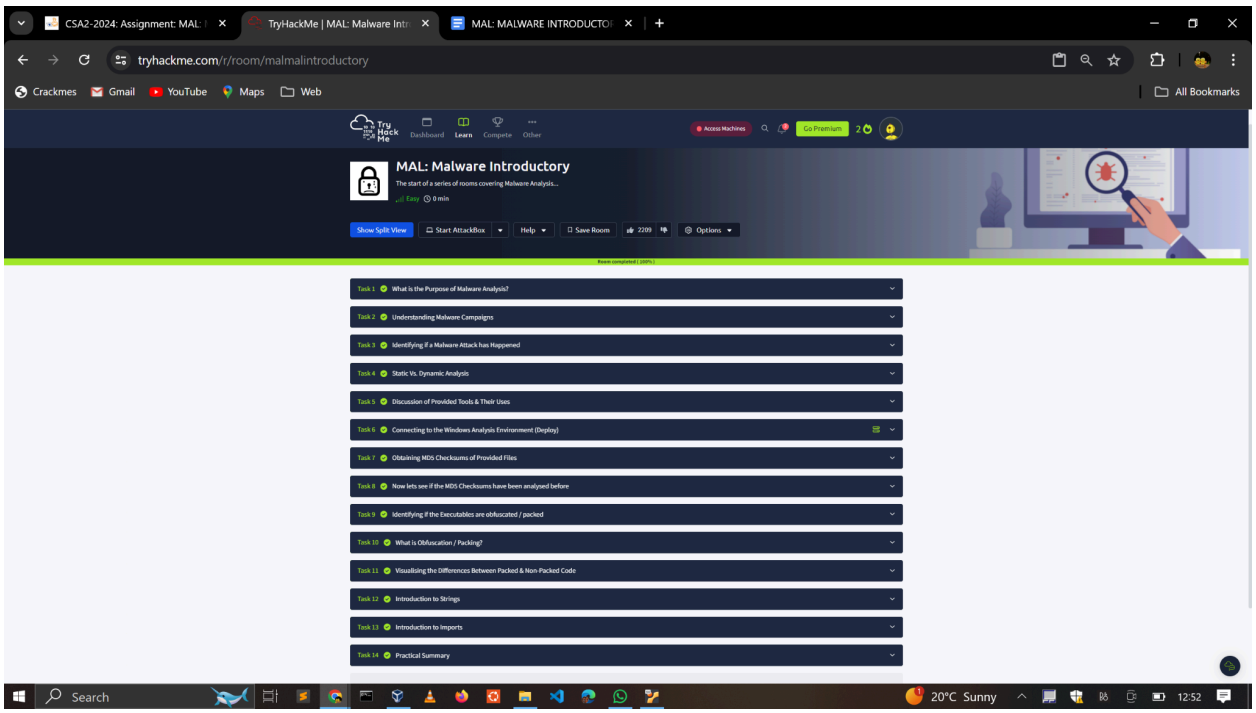
d. What is the output of PeID when trying to detect what packer is used by the file?

- Nothing Found


Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Tasks
Tools
Notepad++
HxD
PE Tools
File Home Share View
Tools › Static › PE Tools
Search PE Tools
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
Name
Date modified
Type
Size
depends - Shortcut 28/02/2021 23:34 Shortcut 2 KB
PE Explorer 21/03/2020 22:14 Shortcut 2 KB
PEiD - Shortcut 02/03/2021 20:25 Shortcut 1 KB
pestudio - Shortcut 28/02/2021 23:32 Shortcut 2 KB
PEview 09/05/2011 10:09 Application 66 KB
ResourceHacker - Shortcut 13/02/2020 18:58 Shortcut 2 KB
6 items
PEiD v0.95
File: C:\Users\Analysis\Desktop\Tasks\Task 14\ComplexCalculator.exe
Entrypoint: 00004FE9
EP Section: .text
File Offset: 000043E9
First Bytes: FF,25,7C,50
Linker Info: 14.13
Subsystem: Win32 GUI
Nothing found *
Multi Scan
Task Viewer
Options
About
Exit
Stay on top

3. MODULE COMPLETION

https://tryhackme.com/p/c1ph3rbnuk



4. CONCLUSION

This assignment has taught me how to to use tools like the **strings** utility to uncover interesting strings hardcoded within a binary like URLs, **PEid** to identify whether a malicious executable is packed or obfuscated, **Virustotal** to confrim the legitimacy of an executable by it's hash and **IDA pro** to view the libraries imported by a malicous binary respectively.