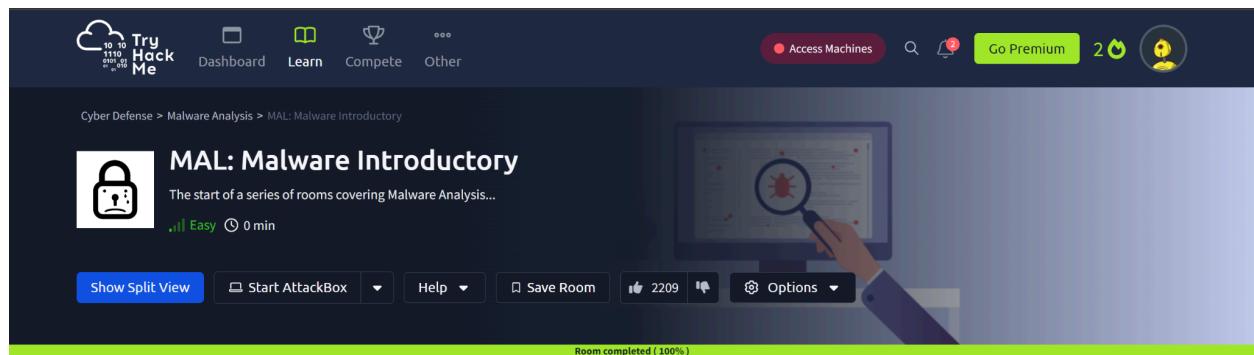


MAL: MALWARE INTRODUCTORY

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

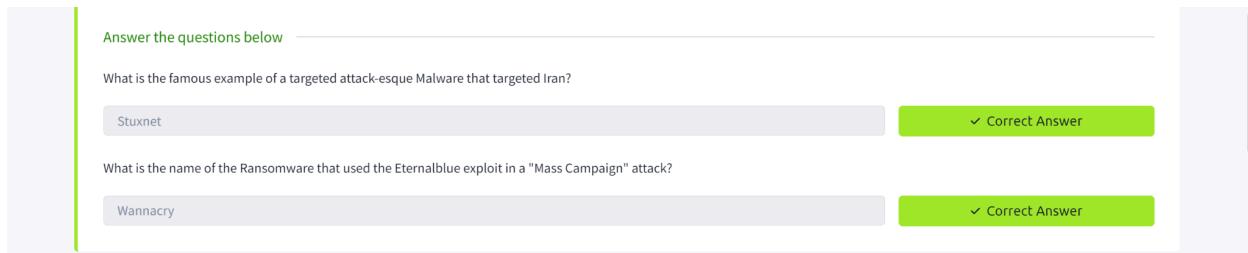
Answer the questions below

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

Stuxnet ✓ Correct Answer

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

Wannacry ✓ Correct Answer



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

Answer the questions below

Name the first essential step of a Malware Attack?

Delivery ✓ Correct Answer

Now name the second essential step of a Malware Attack?

Execution ✓ Correct Answer

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

Host-Based Signatures ✓ Correct Answer 💡 Hint

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

Network-Based Signatures ✓ Correct Answer 💡 Hint



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

Answer the questions below

The MD5 Checksum of aws.exe

D2778164EF643BA8F44CC202EC7EF157 ✓ Correct Answer

The MD5 Checksum of Netlogo.exe

59CB421172A89E1E16C11A428326952C ✓ Correct Answer

The MD5 Checksum of vlc.exe

5416BE1B8B04B1681CB39CF0E2CAAD9F ✓ Correct Answer



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

No security vendors flagged this file as malicious

900021691973aafe47b125d51e1bae5192760e91552dda0c7051226640c0a248
vlc.exe

Size: 962.70 KB | Last Analysis Date: 21 hours ago | EXE

Community Score: 0 / 74

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 3

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

Basic properties

MD5	5416be1bb04b1681cb39c0e02caad9f
SHA-1	f29c26d6210ae7d271f6eeed3f5fd8e8e5b89db
SHA-256	900021691973aafe47b125d51e1bae5192760e91552dda0c7051226640c0a248
Vhash	0950e76d1551555c051058z4553f2321zbaz1
Authentihash	fg9432591a65d64e9a04a3204e28421ad25736c3b92e5848e331e1c733146e9a

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

• Nay

No security vendors flagged this file as malicious

e86ee0e20aec066c3315b40f754ee25ac3c7d3db7dec20c2e82c8d9f5695536
NetLogo.exe

Size: 49.00 KB | Last Analysis Date: 8 days ago | EXE

Community Score: 0 / 74

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

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

Basic properties

MD5	59cb421172a89e1e16c11a428326952c
SHA-1	7583db73674f2340a3244b4e0dd9c0973e989ff
SHA-256	e86ee0e20aec066c3315b40f754ee25ac3c7d3db7dec20c2e82c8d9f5695536
Vhash	054066651d1515751a16hz13z27z35z
Authentihash	c8235dfc44269b77f6629023269ff5739bffd46fb99226c35ecc0652212d522

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

• Nay

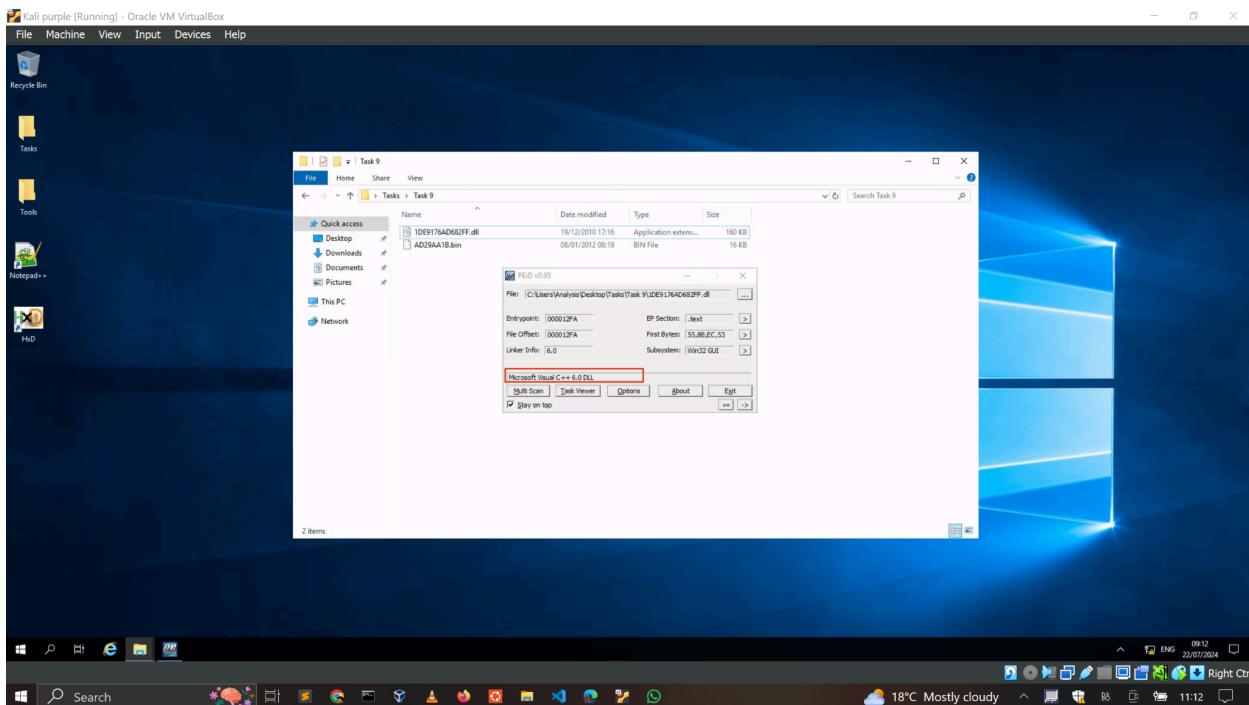
The screenshot shows the VirusTotal analysis interface for a file identified by hash 28b001bb9a72ae7a24242bfab248d767a1ac5dec981c672a3944f7a072375e9a. The main header includes tabs for VirusTotal, TryHackMe | MAL: Malware Intro, and SS-C2-24: Critical Thinking & Puzzles. The URL in the address bar is virustotal.com/gui/file/28b001bb9a72ae7a24242bfab248d767a1ac5dec981c672a3944f7a072375e9a/details. Below the header, there are links for Crackmes, Gmail, YouTube, Maps, and Web, along with an All Bookmarks button. The search bar contains the file hash. On the right side, there are buttons for Reanalyze, Similar, More, and a Sign in/Sign up link. The main content area displays the following information:

- File distributed by Microsoft, Linux and others**
- Community Score**: 0 / 74
- File Details**:
 - File Hash: 28b001bb9a72ae7a24242bfab248d767a1ac5dec981c672a3944f7a072375e9a
 - Type: system_embedded_python_Lib_site-packages_Setuptools_cli-64.exe
 - Format: peexe
 - Size: 73.00 KB
 - Last Analysis Date: 3 days ago
 - File Extension: EXE
- Detection**, **Details** (selected), **Relations**, **Behavior**, **Community** (24+)
- Basic properties**:
 - MD5: d2778164ef643ba8f44cc202ec7ef157
 - SHA-1: 31eeee7114eed680d2fb77c9f36f05057639050786
 - SHA-256: 28b001bb9a72ae7a24242bfab248d767a1ac5dec981c672a3944f7a072375e9a
 - Vhash: 074046655d155a2511
 - Authenticodehash: 53057dc2aa89f38b306ce21a928faa6d0b1c18a368171c3e7ff87389f19c25
- A green banner at the bottom encourages users to "Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks."

Identifying if executables are obfuscated or packed

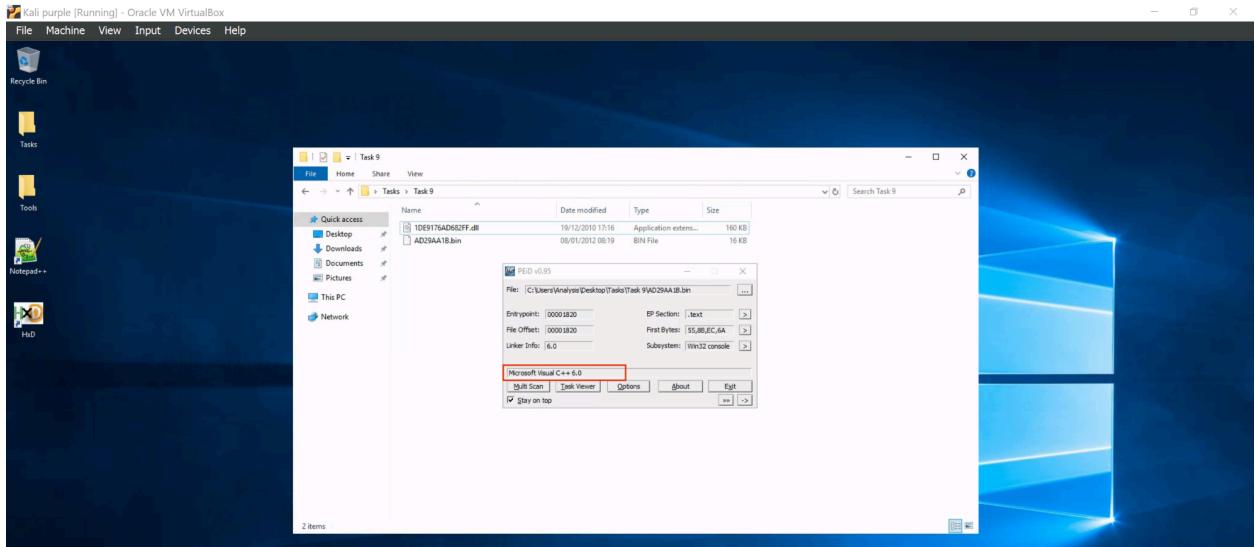
- a. What does PeID propose 1DE9176AD682FF.dll being packed with?

- Microsoft Visual C++ 6.0 DLL



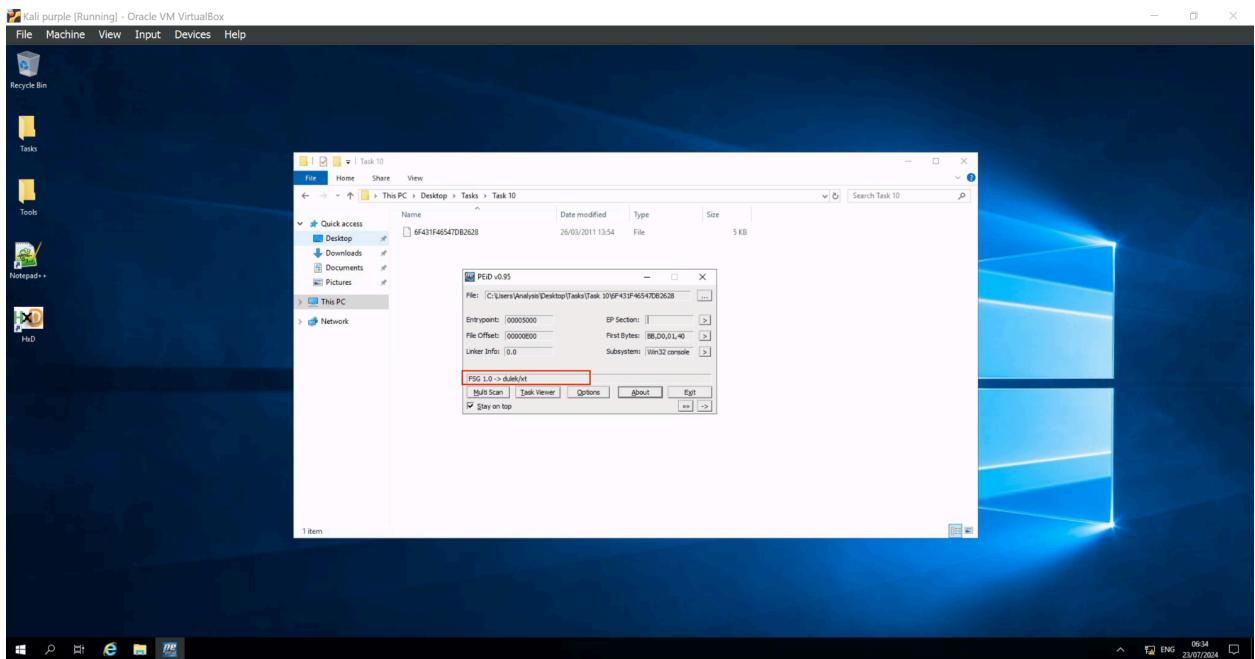
- b. What does PeID propose AD29AA1B.bin being packed with?

- 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

Kali purple [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Select C:\Windows\System32\cmd.exe

```

Fopen
StrCpy
?22@vxD!@I@Z
_atol
_sscanf
_strlen
_strncat
_strerror
_itowl
 strchr
_CxxFrameHandler
_EvtCreate
_CxxThrowException
_except_handler3
_kernel32.dll
?_tprintf@_Info@@IAE@XZ
free
_intlrcm
_malloc
_Adjust_FDiv
_strcmp
_CrtSetErrMode
_strcmp
_Lab03-02.dll
InstallService
ServiceMain
UninstallService
InstallService
UninstallService
VxDLib!VxDLib
http://www.malwareanalysis.com
dw5z0dBeB330
_Cxx12A
_VxM
_CxxPdA==
Windows XP 6.11
CreateProcessA
kernel32.dll
exit
GET
HTTP/1.1
1234567890123456
quit
exit
GetFile
cmd.exe /c
ABCDEFIGHJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789/
;)
<!--
-->
_PAR
_PMO
DependOnService
RpcSs
Service011
GetModuleFileName() get dll path

```

Size

1,347 KB
742 KB

Search SysinternalsSuite

09:41 ENG 23/07/2024 Right Ctrl

b. How many unique "Imports" are there?

- 5

Kali purple [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

PE Explorer - C:\Users\Analysis\Desktop\Tasks\Task 12\67844C01

File View Tools Help

IMPORT VIEWER

PVA Name

1000505Ch - FEDDNE132.dll	0050h	GetCommandLineA
1000505Bh - ADVAPI32.dll	0043h	CreatePipe
1000505Ch - WS2_32.dll	0059h	GetCurrentDirectoryA
1000505Bh - WININET.dll	0044h	CreateProcessA
1000505Bh - MSVCR7.dll	0050h	GetCurrentProcess
	0071h	SetLastError
	0059h	OutputDebugStringA
	0018h	ReadFile
	0065h	GetTempPathA
	0021h	GetLongPathNameA
	003Ah	GetVolumeNameA
	0038h	GetVolumePathNameA
	0044h	CreateThread
	0050h	GetSystemTime
	0040h	TerminateThread
	0059h	Sleep
	0019h	GetExitCode
	0024h	GetModuleHandleA

5 imports

Library description: Windows Base API Client DLL

-- Syntax Details --

```

procedure GetStartupInfo(var lpStartupInfo: TStartupInfo); stdcall; external 'kernel32.dll' name 'GetStartupInfo' index 359;

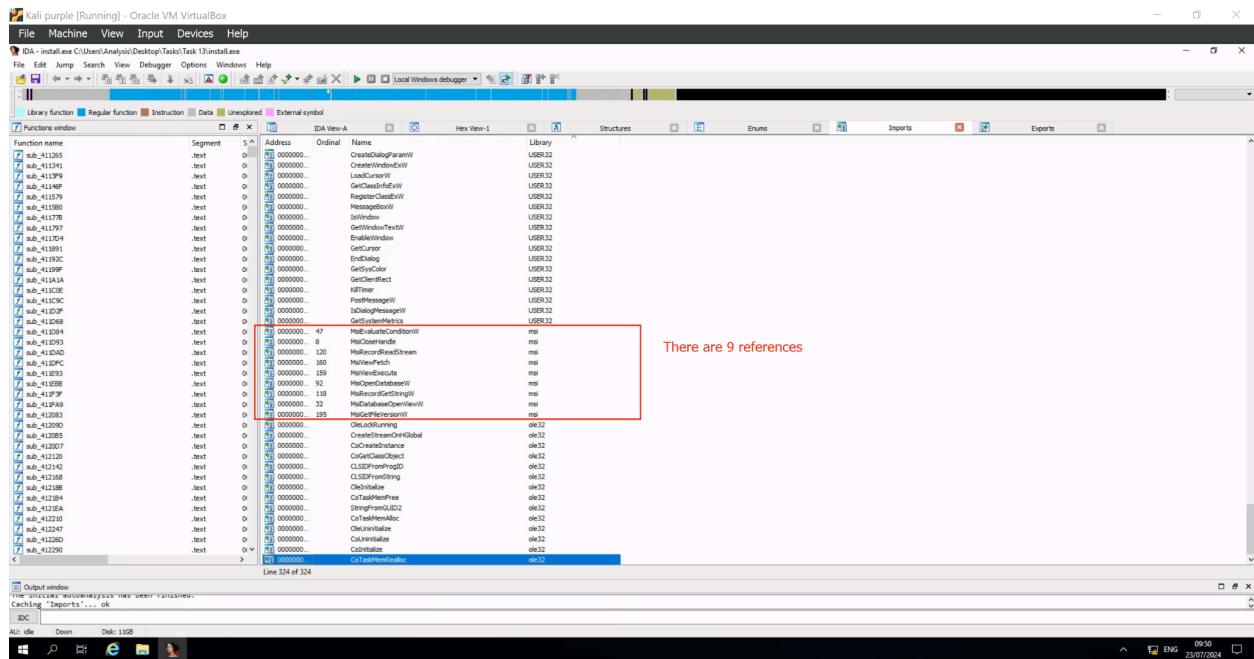
```

09:45 ENG 23/07/2024 Right Ctrl

Introduction to strings

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

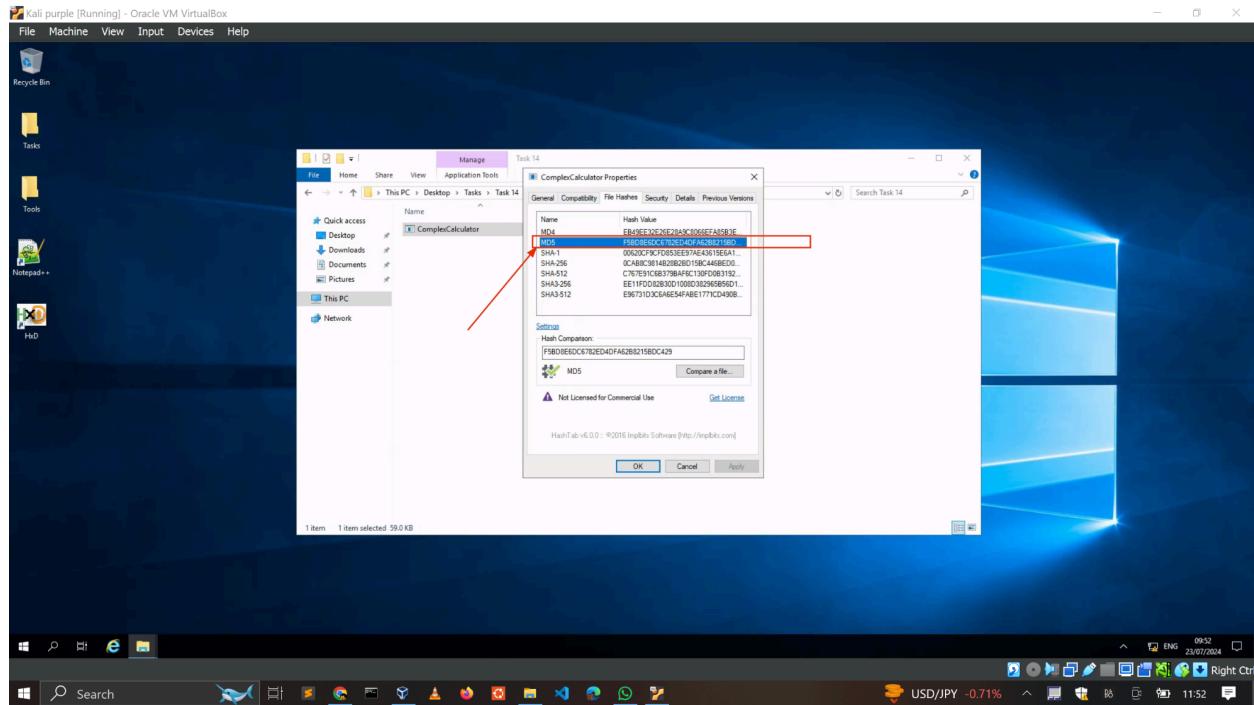
9



Introduction to strings

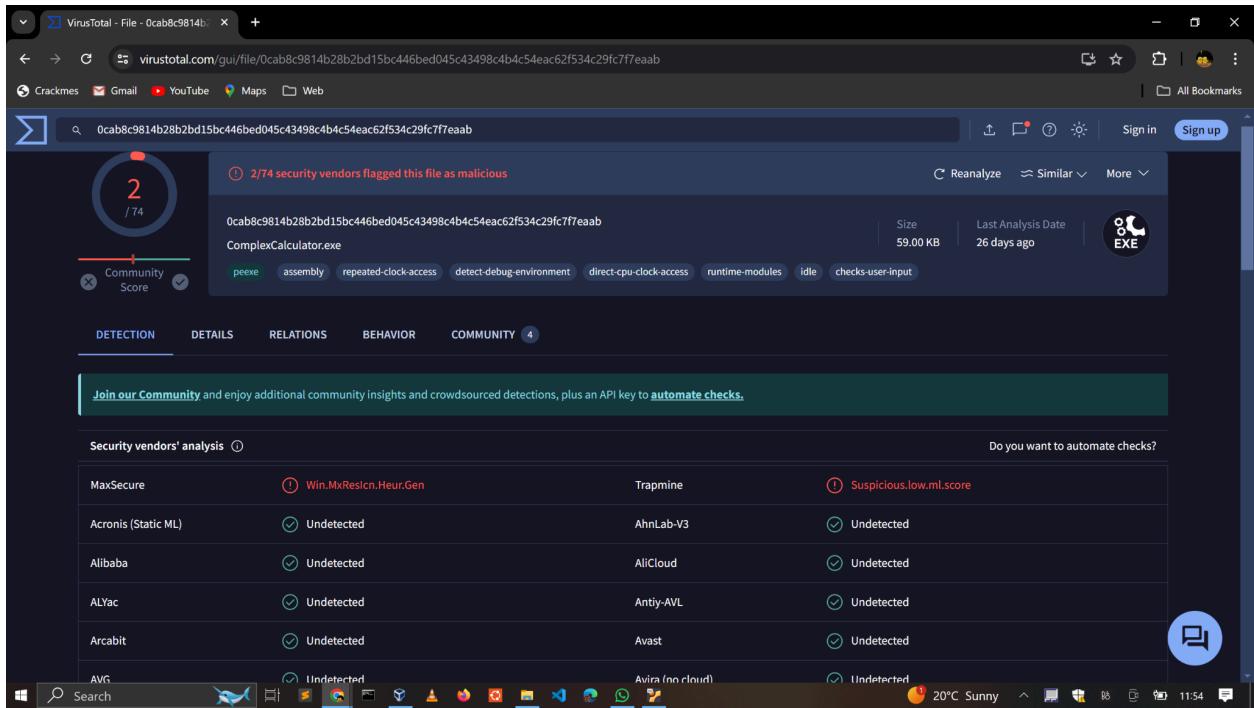
a. What is the MD5 Checksum of the file?

- [f5bd8e6dc6782ed4dfa62b8215bdc429](#)



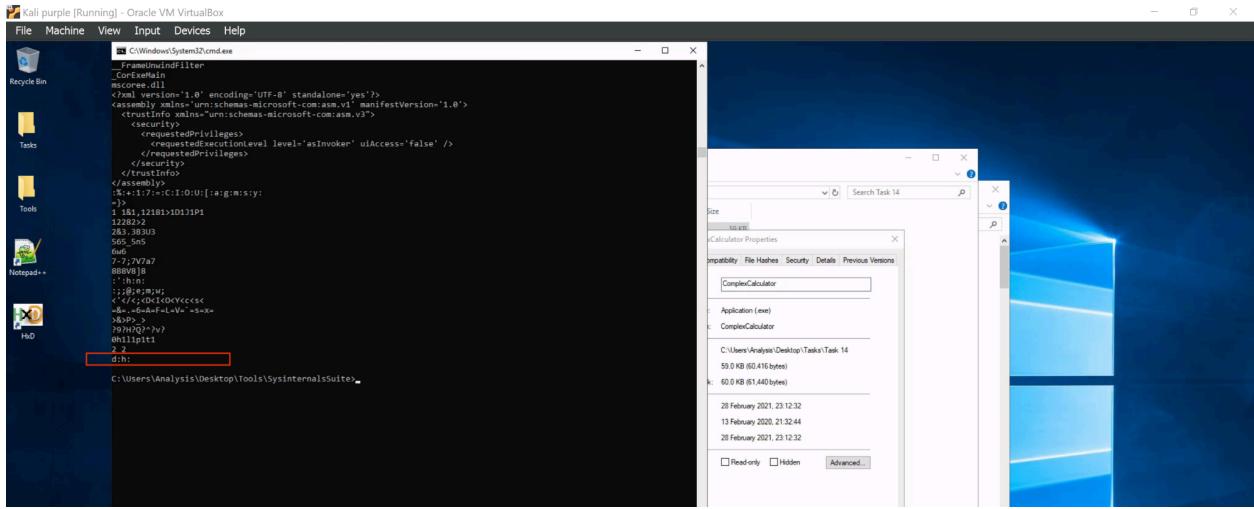
b. Does Virustotal report this file as malicious? (Yay/Nay)

- ## ● Yay



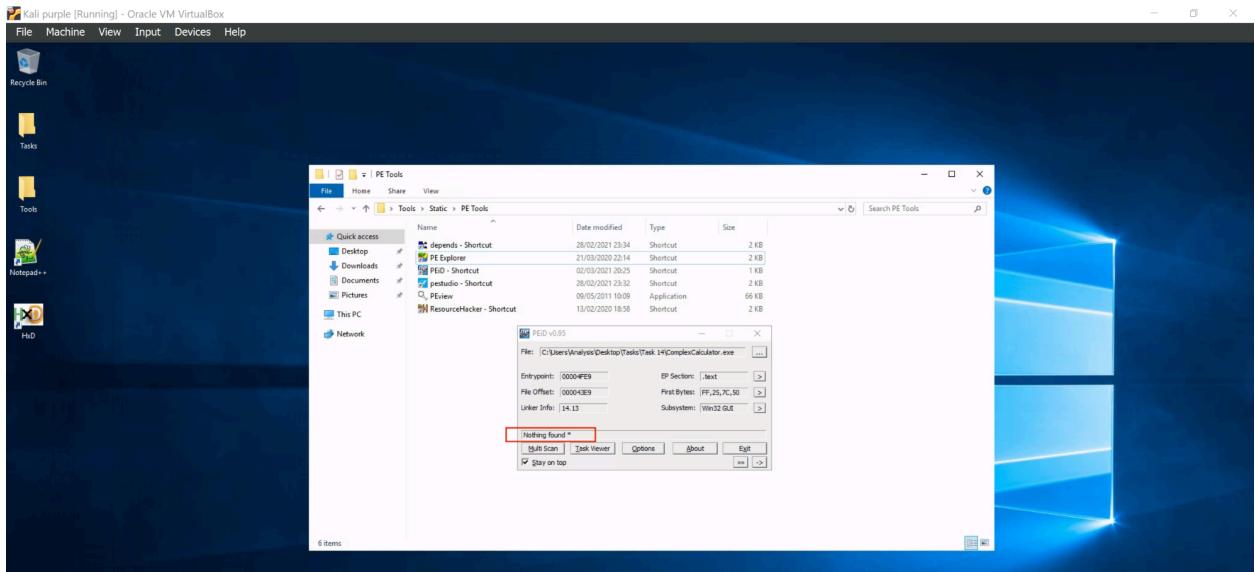
c. Output the strings using Sysinternals "strings" tool. What is the last string outputted?

- d:h:



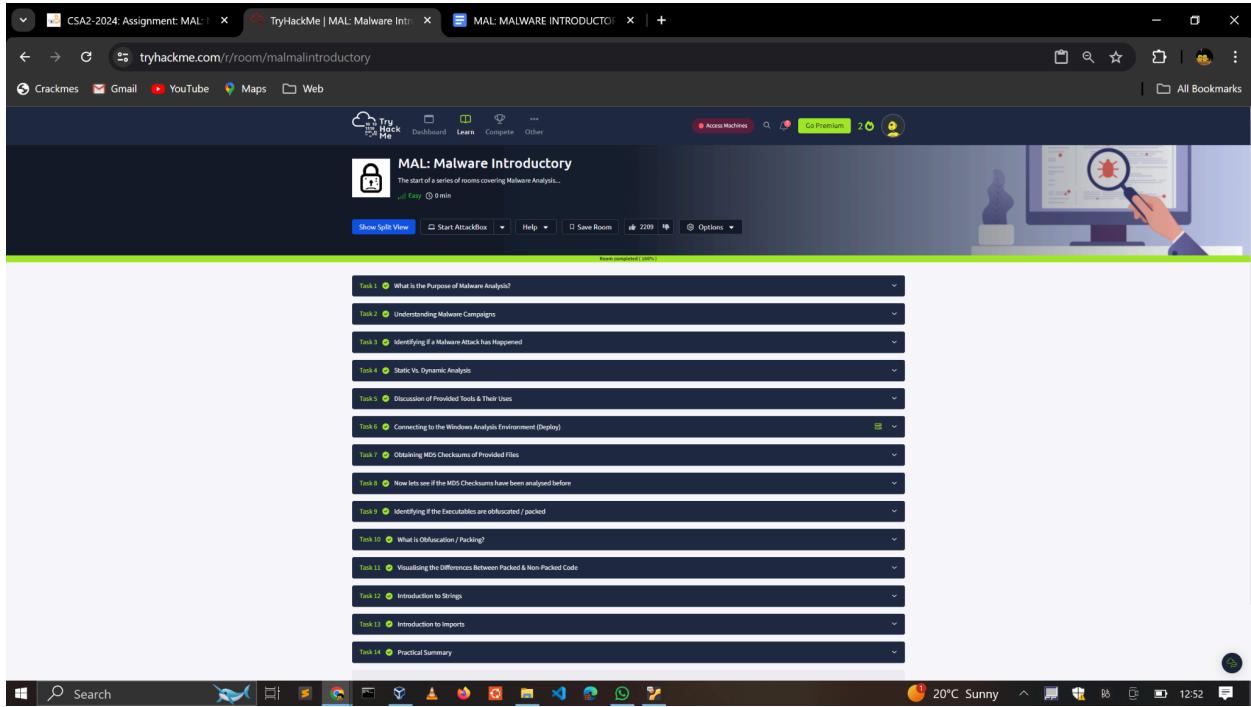
d. What is the output of PeID when trying to detect what packer is used by the file?

- ## ● Nothing Found



3. MODULE COMPLETION

<https://tryhackme.com/p/c1ph3rbnuk>



4. CONCLUSION

This assignment has taught me how 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 confirm the legitimacy of an executable by its hash and **IDA pro** to view the libraries imported by a malicious binary respectively.